29th NATIONAL RADIO SCIENCE CONFERENCE
(NRSC 2012)
April 10 - 12, 2012, Faculty of Engineering/Cairo University, Egypt

C11. An Efficient Fractional Fourier Transform Approach for Digital Image Watermarking

Ehab. H. Elshazly [1], Mahnoud A. Ashour [1], Elsayed M. Elrabaie [2], Alaaeldin M. Abbas [2]
[1] Eng. Dept., NCRRT, EAEA, 3 Ahmed Al-Zomar, 8th District, Nasr City, Cairo, Egypt,
eng_ehab_helmy@yahoo.com
[2] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt.

ABSTRACT

The paper presents an efficient approach for digital image watermarking based on the Fractional Fourier Transform (FRFT). In this approach, a watermark in the form of a PN sequence is embedded in the coefficients of the FRFT implemented on the image in the spatial domain or in transform domain. The FRFT is used in this paper as a means of security. The objective of using other transform domains prior to the FRFT is to make use of the details in these transforms domains. Before extraction of the watermark image, we intentionally attack the watermarked image with different common image processing attacks to test the robustness of the proposed algorithms. The proposed Discrete Wavelet Transform Fractional Fourier Transform (DWT-FRFT) algorithm gives best robustness over the other algorithms under these attacks.

Keywords: Watermarking, DWT, FRFT, joint transforms.

I. INTRODUCTION

The fast development of Internet in recent years has made it possible to easily create, copy, transmit, and distribute digital data. Consequently, this has led to a strong demand for reliable and secure copyright protection techniques for digital data. Digital watermarking has been proposed as a valid solution for this problem. The purpose of the watermarking is to embed some additional information about the digital data without visibly modifying it. In order to be successful, the watermark should be invisible and robust to premeditated or spontaneous modifications of the image. It should be robust against common image processing operations such as filtering, additive noise, cropping and common image compression techniques. Watermarking techniques can be categorized in different ways. They can be classified according to the type of watermark being used, i.e., the watermark may be a visually recognizable logo or a sequence of random numbers. Another classification is based on the domain in which the watermark is applied i.e., the spatial domain or a transform domain. The earlier watermarking techniques were almost in spatial domain. Spatial domain techniques are not resistant enough to image processing. Transform domain watermarking schemes like those based on the Discrete Cosine Transform (DCT) [1],[2],[3],[4],[5], and the Discrete Wavelet Transform (DWT) [6],[7],[8],[9] typically provide higher image imperceptibility and robustness. In DWT-based image watermarking, the input image is passed through a series of low and high pass filters producing low, middle and high frequency sub-bands each possessing unique characteristics. In general, embedding watermarks in the middle frequency sub bands demonstrated effective watermarking compared to embedding in the other sub-bands. Further performance improvements in the DWT-based digital image watermarking algorithms could be obtained by jointing DWT with other transforms [10]. The reason of applying two transforms is based on the fact that jointed transforms could make up for the disadvantages of each other, so that effective watermarking approaches could be acquired. Digital image watermarking based on the fractional Fourier transform have also been proposed [11],[12]. In this approach, the original image is transformed by the discrete fractional Fourier transform, and the transformed coefficients are modified by the information of the watermark. The transform order of the 2D-FRFT is used as the encryption key in the algorithm. A watermarking scheme based on the FRFT and Singular Value Decomposition (SVD) was presented in [13].

In this paper, we test jointing FRFT with DWT, DCT and Discrete Sine Transform (DST) and compare our results with the application of the FRFT on the image without any transforms (in spatial domain). In DWT–FRFT, watermark is embedded by altering the FRFT coefficients of middle frequency sub-bands of the 2-levels DWT transformed host image. Before extraction of the watermark, pre-processing operations are used to examine the performance of the algorithm. The rest of this paper is organized as follows; Section 2 describes the combined DWT-DCT digital image watermarking. Section 3 describes briefly the concept of FRFT. Section 4 describes the embedding algorithm in detail. The extraction algorithm is described in Section 5. The performance evaluation

978-1-4673-1887-7/12/$31.00 ©2012 IEEE

and evaluation metrics are presented in Section 6. Section 7 presents the experimental results. The conclusion is drawn in Section 8.

2. COMBINED DWT-DCT DIGITAL IMAGE WATERMARKING

In [10], the author presented the idea of using two transform domains in cascade for image watermarking; the DWT and the DCT. This idea is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. First he applied two levels DWT, and then he divided the chosen mid sub bands into 4 x 4 blocks applying DCT to each block. In the embedding stage, he used two PN sequences one for embedding the zero bit of the watermark and the other sequence to embed the one bit. In the extraction stage, two PN sequences generated with the same key used in embedding step and correlation factors between them and the chosen mid band coefficients are calculated and based on which correlation factor is greater than the other, he decide whether the extracted bit is zero or one. His results showed that the combined DWT-DCT watermarking algorithm outperforms the conventional DWT-Only approach with respect to robustness against the Gaussian noise and cropping attacks. The results are better regardless of whether the watermark was embedded in HL2 or HH2; however, HH2 gave better robustness against cropping compared with HL2. but in the same time the robustness of the DWT-Only approach against the JPEG compression attack is better than that of the combined DWT-DCT algorithm. The main focus on that work was to present robust watermarking technique ignoring the security aspect, so we will try to present robust and secured watermarking technique based on joint transforms and fractional Fourier transform.

3. FRACTIONAL FOURIER TRANSFORM

The fractional Fourier transform, which is a generalized form of the Fourier transform, has become a powerful and potential tool for time-varying and non-stationary signal processing. As the classical Fourier transform corresponds to a rotation in the time-frequency plane over an angle ($\frac{\pi}{2}$*)*, the FRFT can be considered as a generalized form that corresponds to a rotation over some arbitrary angle.

The FRFT has one more degree of freedom, when it is compared to the conventional FT, which is the angles in both x & y directions.

The pth order FRFT of a signal is defined as [11]

$$F^{p}\left[f(x)\right]=\int_{-\infty}^{\infty}K_{p}(x,u)f(x)dx\,, \qquad 0\leq|p|\leq 2 \tag{1}$$

$$K_{p}(x,u)=\begin{cases}\sqrt{\dfrac{1-j\cot\alpha}{2\pi}}\exp\left(j\dfrac{x^{2}+u^{2}}{2}\cot\alpha-j\dfrac{xu}{\sin\alpha}\right) & if\quad \alpha\neq n\pi\,,\\ \delta(u-x) & if\quad \alpha=2n\pi\,,\\ \delta(u-x) & if\quad \alpha=(2n+1)\pi\,,\end{cases} \tag{2}$$

Where p is the order of the FRFT and α is the rotation angle.

The relationship between p and α is $\alpha=\frac{p\pi}{2}$

$K_{p}(x,u)$ Is the kernel function of the FRFT.

The inverse of an FRFT with an order p is the FRFT with order $-p$ according to the following relation:

$$f(x) = F^{-p}\left[F^{p}(f(x))\right] \tag{3}$$

The Discrete Fractional Fourier Transform DFRFT:

Let $f(x)$ be a sampled periodic signal with a period Δ_0, the pth order discrete fractional Fourier transform (DFRFT) of $f(x)$ can be obtained by using Eq.(1), giving [12]:

$$f_p = \sum_{k=-\frac{N}{2}}^{\frac{N}{2}-1} f\left(k\frac{\Delta_0}{N}\right)\sum_{n=-\infty}^{\infty} k_p\left(x,\left(n+\frac{k}{N}\right)\Delta_0\right) \tag{4}$$

Two Dimensional Discrete Fractional Fourier Transform 2DFRFT:

The forward and inverse two-dimensional discrete fractional Fourier transform (2D-DFRFT) of the image signal are computed as [13]:

$$F_{\alpha,\beta}(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} f(p,q)K_{\alpha,\beta}(p,q,m,n) \tag{5}$$

$$f_{\alpha,\beta}(p,q) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} F_{\alpha,\beta}(m,n)K_{-\alpha,-\beta}(p,q,m,n) \tag{6}$$

Where (α,β) is the order of 2D-DFRFT, $K_{\alpha,\beta}(p,q,m,n) = K_\alpha \otimes K_\beta$ is the transform kernel, K_α, K_β are the one dimensional discrete fractional Fourier transform kernels.

4. Proposed Watermark Embedding

We start the watermarking process by applying the first transform which could be DCT, DST or DWT to the host image, and afterwards performing the FRFT to the transformed image. In case of DWT, The agreement adopted by many DWT-based watermarking methods, is to embed the watermark in the middle frequency sub-bands HL_X and LH_X , which is better in perspective of imperceptibility and robustness. Consequently, the sub-bands HL_2 and LH_2 are chosen to be transformed to FRFT domain. The watermark embedding and extraction procedure is illustrated in Fig. 1 followed by a detailed explanation. For simplicity, the DWT-FRFT watermarking procedure is considered in the next steps.

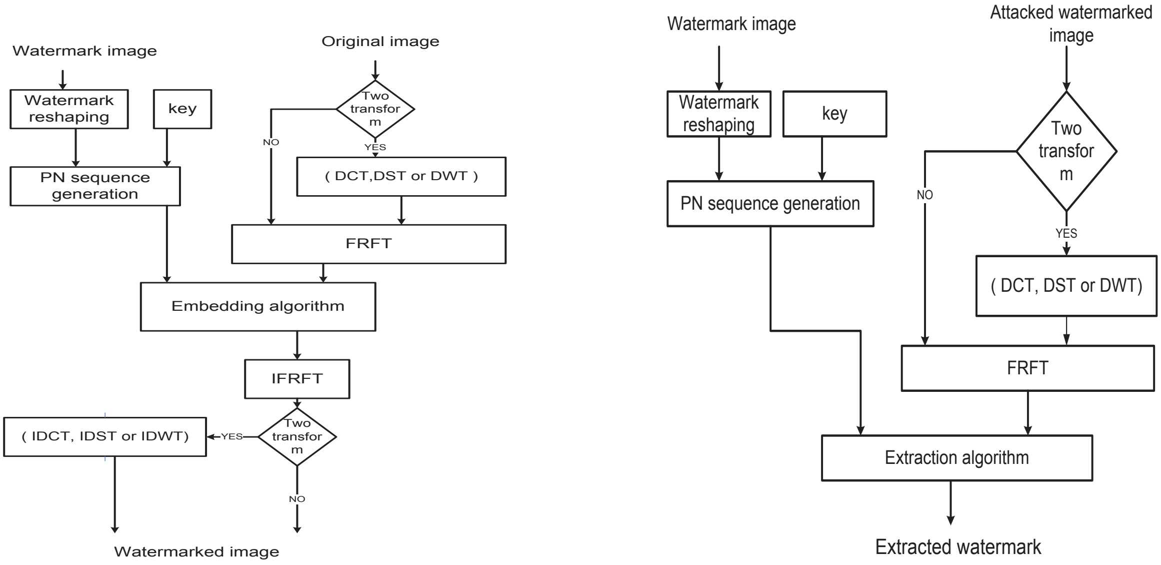

Fig. 1: Watermarking process. (a) Embedding procedure and (b) Extraction procedure.

Step 1: The host image is transformed to Two Dimensional Discrete Wavelet Transform (2D-DWT) domain to obtain four non-overlapping multi resolution coefficient sets: LL_1, HL_1, LH_1 and HH_1.

Step 2: The HL_1 sub-band is transformed to DWT to obtain four smaller sub-bands and HL_2 and LH_2 are chosen.

Step 3: The selected sub-bands are transformed to Two Dimensional Fractional Fourier (2D-FRFT) with angles α_1 and α_2 in both x & y directions.

Step 4: Re-formulate the grey-scale watermark image into a vector of zeros and ones.

Step 5: generate two PN sequences of size equal to that of HL_2 and LH_2 and for each pixel of the watermark we check if it was one we don't modify HL_2 and LH_2, and if it was zero we add these PN sequences multiplied by a factor K to HL_2 and LH_2 .where K is the gain factor.

Step 6: we repeat step 5 till the entire watermark pixels finished.

Step 7: Inverse the FRFT with angles $-\alpha_1$ and $-\alpha_2$. Then, inverse DWT.

Step 8: Compute the correlation and PSNR between the original image and watermarked one.

To test the algorithm robustness, we intentionally attack the watermarked image with noise, cropping, compression etc.

5. Watermark Extraction

The watermark extraction procedure is described in the following steps. The joint DWT-FRFT algorithm is a semi blind watermarking algorithm as the original host image is not required to extract the watermark but we need the watermark size and the same key to generate the PN sequences.

Step 1: The attacked watermarked image is transformed to two level 2D-DWT and HL_2, LH_2 are chosen.

Step 2: The selected sub-bands are transformed to 2D-FRFT with the same angles α_1 and α_2 in both x & y directions.

Step 3: Initialize message vector of the same length as original watermark to ones.

Step 4: Regenerate the two pseudorandom sequences ($PN\ 1$ and $PN\ 2$) using the same key which is used in the embedding process.

Step 5: for each pixel of the watermark calculate the correlation factor between the generated two PN sequences and HL_2 & LH_2 .

Step 6: If the average correlation is greater than a certain value, then the corresponding watermark bit is zero, otherwise it remains one.

Step 7: repeat steps 4,5 and 6 for each pixel in the watermark vector.

Step 8: The watermark is reconstructed using the extracted watermark bits, and compute the similarity and PSNR between the original and extracted watermarks.

The same procedure can be carried out for either DCT or DST transformed images.

The results for DWT-FRFT, DCT-FRFT, DST-FRFT and that of applying FRFT directly on the spatial domain image to results in [10] to demonstrate the robustness of the proposed algorithm.

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of the spatial domain or to support additional features.

6. PERFORMANCE EVALUATION

In this section, the proposed algorithms are evaluated. Several experiments are performed to evaluate the effectiveness of the presented watermarking algorithms. The proposed hybrid algorithms and the traditional FRFT algorithm are compared to the method in [10]. The LENA image of size 512×512 with 256 gray levels is used in these experiments as the host image and the binary COPYRIGHT image of size 20×50 as a watermark image. Figure 2 shows original image and watermark image which are used in the experiments.

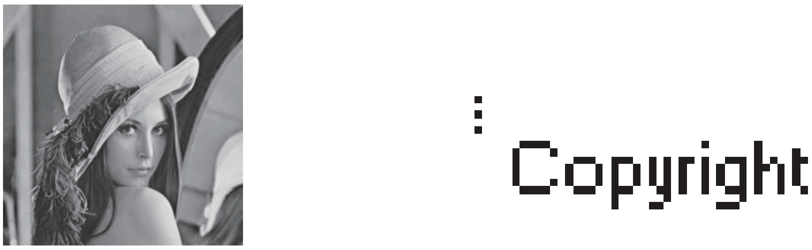

Fig. 2 Test images. (a) Original image and (b) Watermark image

In the proposed DWT-FRFT algorithm, the selected sub-bands are HL_2 and LH_2 . Then, we perform FRFT. For DCT, DST and spatial domain, the whole image is subjected to FRFT and the watermark is embedded in the whole image.

A. Performance Evaluation Metrics:

Watermarking algorithms are usually evaluated with respect to two metrics; imperceptibility and robustness [14]. The two metrics are described below.

Imperceptibility: Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked image, the Peak Signal-to-Noise Ratio (PSNR) is typically used. PSNR in decibels (dB) is given below in Eq. 8 [15].

$$PSNR = 20.\log_{10}\left(\frac{255}{RMS}\right) \tag{8}$$

Robustness: Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, intentionally or unintentionally, by different types of digital signal processing attacks [16]. In this paper, we will report on robustness results which we obtained for major digital signal processing operations (attacks); Gaussian noise, image compression, rotation, salt and pepper noise and image cropping. These attacks are a few; however, they are good representatives of the more general attacks. That is the Gaussian noise is a watermark degrading attack, JPEG compression is a watermark removal attack and cropping is a watermark geometrical attack. We measured the similarity between the original watermark and the watermark extracted from the attacked image using the correlation factor ρ given below in Eq. 9.

$$\rho\left(w, w'\right) = \frac{\sum_{i=1}^{N} w_i w'_i}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} w_i'^2}} \tag{9}$$

Where N is the number of pixels in the watermark, w and w' are the original and extracted watermarks, respectively. The correlation factor ρ may take values between 0 (random relationship) to 1 (perfect linear relationship). In general, a correlation coefficient of about 0.75 or above is considered acceptable.

In the beginning, we optimize each algorithm to get the best imperceptibility and highest similarity between original and extracted watermark at ideal case (no attack) by choosing the best embedding factor and these results are presented in figure 3.

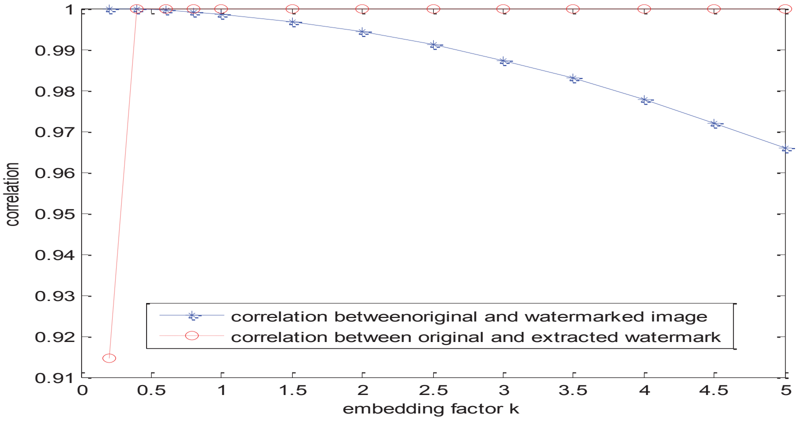

Fig.3 (a)

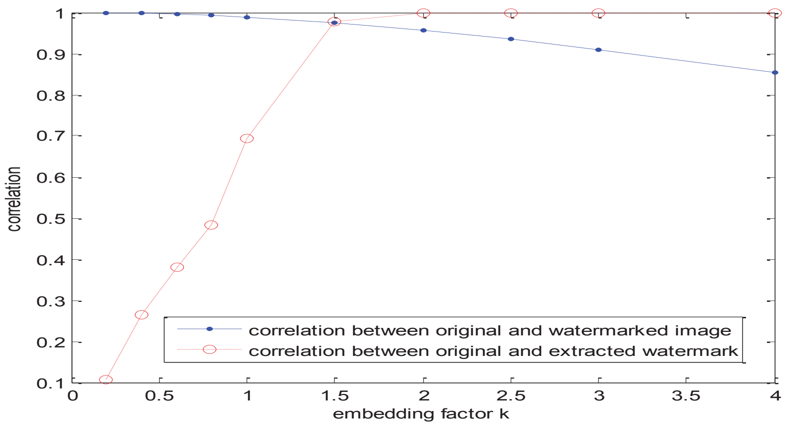

Fig.3 (b)

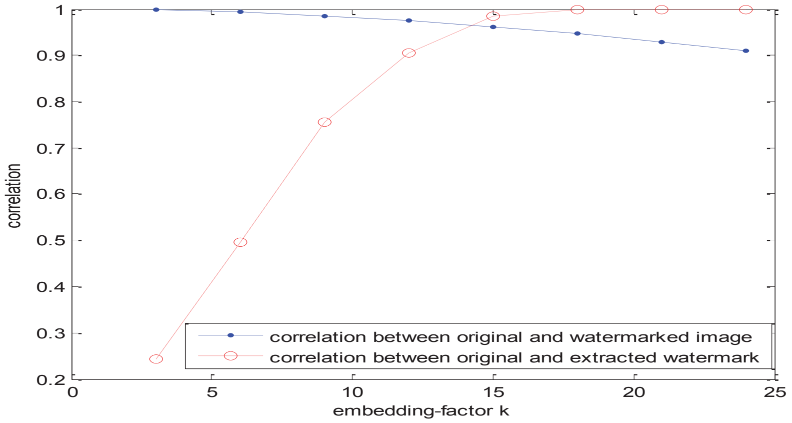

Fig.3 (c)

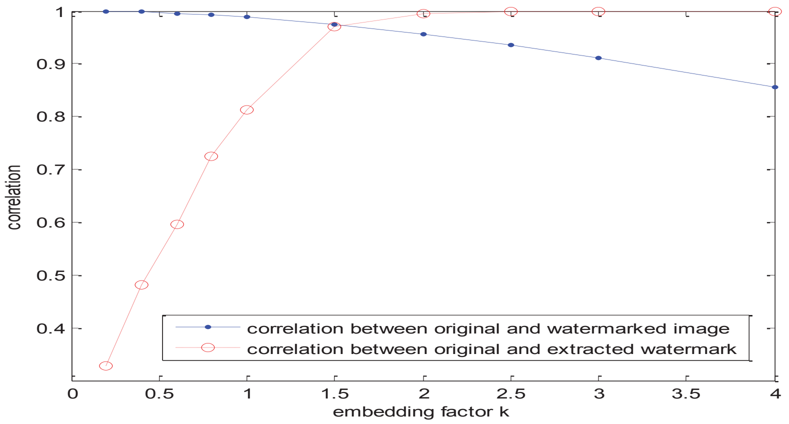

Fig.3 (d)

Fig.3 Relation between embedding factor and correlation factor. (a) In DWT FRFT, (b) In DCT FRFT, (c) in DST FRFT and (d) In FRFT.

In Fig. 3, the down going curve represents the imperceptibility, which represents the correlation factor between original host image and watermarked image while the up going curve represents the correlation factor between original and extracted watermark. We chose k=4.5 for DWT-FRFT, k=1.5 for DCT-FRFT and FRFT and chose k=15 for DST-FRFT where the two curves intercept, these values give good imperceptibility and robustness against attacks.

7. Results and discussion

In order to measure the robustness of the proposed algorithm, the watermarked image is extracted in the presence of common attacks. Figure 4 depicts the extracted watermark under different attacks in the DWT-FRFT for example. The performance analysis results are cited in Tables 1 and 2.

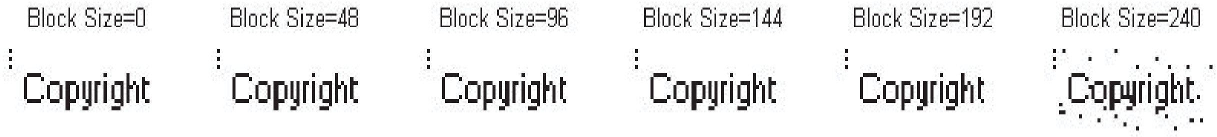

Fig.4 (a)

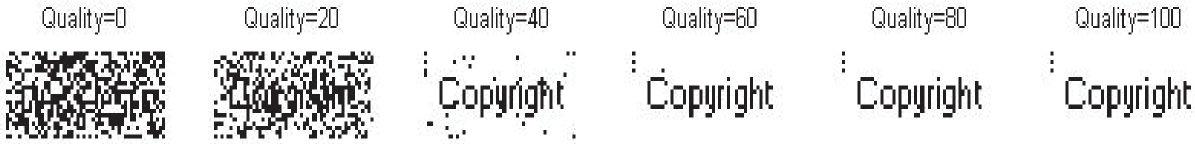

Fig.4 (b)

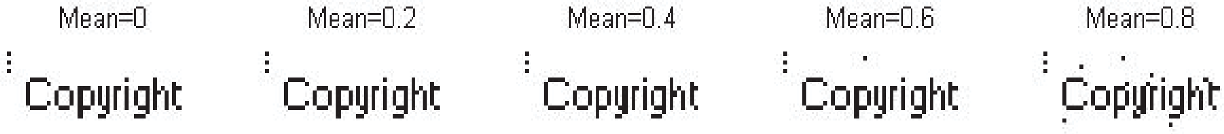

Fig.4 (c)

Fig.4 extracted image. (a) Under cropping attack, (b) Under J-PEG compression attack and (c) Under adding Gaussian with different mean.

Table.1 Experimental results using PSNR metric for imperceptibility.

Metric	DWT FRFT	DCT FRFT	DST FRFT	FRFT	Method in [10]
PSNR (dB)	+26.88	+27.39	+24.06	+27.39	+41.39

Table.2 Experimental results using correlation factor metrics for robustness.

Attack		**DWT FRFT**	**DCT FRFT**	**DST FRFT**	**FRFT**	**Method in [10]**
No attack		1	0.9787	0.9844	0.9693	0.9738
Gaussian noise with variance 10%		0.8940	0.7716	0.6003	0.6872	0.1680
Gaussian noise with mean of 0. 4		1	0.3578	0.4873	0.9146	0.8360
Salt & pepper noise with variance 10%		0.9947	0.9024	0.8725	0.8489	0.2702
JPEG compression	***QF=60***	0.9947	0.4528	0.4460	0.0.6959	0.9583
	QF=80	1	0.9165	0.7750	0.9104	0.9589
cropping	***Block size =96***	1	0.9423	0.9638	0.7907	0.9051
	Block size =192	1	0.6742	0.8197	0.5122	0.6110
Motion blurring Len=9 Theta=10		0.9895	0.0936	0.1309	-0.0290	0.8989
Gaussian Low pass Filter		1	0.6044	0.7872	-0.0270	0.9583
Sharpening		1	1	1	-0.0284	0.9895
Median filter		-0.7562	0.1188	0.1637	-0.0060	0.8532

Rotation 60 degree	0.0325	-0.0672	0.0264	-0.1008	0.0342

In Table 1, PSNR refers to the peak signal to noise ratio between the original host image and the watermarked one. And in Table 2 the correlation factor between the original and extracted watermark is used. The proposed hybrid algorithm gives more security over the traditional single transform algorithms by using FRFT angles in both directions as extra keys. As a result, it is impossible to inverse the FRFT without prior information about these angles. From Table 1, we find that in normal case (no attack) each algorithm is adjusted to give best imperceptibility and robustness. We notice that DWT FRFT gives highest correlation between original and extracted watermark, also its imperceptibility is still high. After pre processing with different common image processing attacks, from table 2 we find that DWT FRFT gives the best robustness under most attacks (cropping, JPEG compression, Gaussian noise addition and salt & pepper noise, Gaussian low pass filtering, motion blurring and sharpening) this robustness arises from the idea that the larger the magnitude of the wavelet coefficient the more significant it is to embed stronger watermarks. All the proposed algorithms and the one in [10] can not defense against rotation attack as it rearrange the image pixels. also it's clear that the proposed algorithms are not robust against median filtering as it make reordering of the pixels and that is the same problem we face with rotation attack and we work to avoid this problem in next work employing defensive techniques against geometrical attack in general such as template based watermarking [16],[17] and invariance-domain-based watermarking methods [18].

8. CONCLUSION

In this paper, joint DWT- FRFT, DCT-FRFT, DST-FRFT and FRFT digital image watermarking algorithms are presented. In DWT-FRFT, two middle sub-bands are subjected to FRFT and in the last algorithms the whole transformed image is subjected to FRFT. Implementation results show that the presented watermarking schemes provide enhanced security. The DWT-FRFT algorithm provides a good watermarked image quality and improved robustness over single transform algorithms. In the extraction procedure, common attacks are used to test the robustness of the presented algorithms. DWT-FRFT showed better robustness against most attacks than the other algorithms.

Acknowlegement

We would like to thank Dr. Fathi E. Abd El-Samie from the Faculty of Electronic Engineering, Menoufia University for his participation in this work.

REFERENCES

[1] S. Lin, and C. Chin, “A Robust DCT-based Watermarking for Copyright Protection,” IEEE Trans. Consumer Electronics, 46(3): 415-421, 2000.

[2] C. Wu, and W. Hsieh, “Digital watermarking using zero tree of DCT,” IEEE Trans. Consumer Electronics, vol. 46,no. 1, pp: 87-94, 2000.

[3] A. Nikolaidis, and I. Pitas, “Asymptotically optimal detection for additive watermarking in the DCT and DWT domains,” IEEE Trans. Image Processing, 2(10): 563-571, 2003.

[4] W. Chu, “DCT-Based Image Watermarking Using Sub sampling,” IEEE Trans. Multimedia, 5(1): 34-38, 2003.

[5] F.Deng, and B. Wang, “A novel technique for robust image watermarking in the DCT domain,” in Proc. of the IEEE Int. Conf. on Neural Networks and Signal Processing, vol. 2, pp: 1525-1528, 2003.

[6] M.S. Hsieh, and D.C. Tseng , “Hiding digital watermarks using multi-resolution wavelet transform”, IEEE Transactions on industrial electronics, vol. 48, No. 5, pp 875- 882, Oct, 2001.

[7] H. Guo, and N. Georganas, “Multi-resolution Image Watermarking Scheme in the Spectrum Domain,” Proceeding of IEEE Canadian Conference on Electrical and Computer Engineering, pp. 873-878, May, 2002.

[8] A. Reddy, and B. Chatterji, “A New Wavelet Based Logo-watermarking Scheme,” Pattern Recognition Letters, 26(7): 1019-1027, 2005.

[9] S. Wang, and Y. Lin, “Wavelet Tree Quantization for Copyright Protection Watermarking,” IEEE Trans. Image Processing, vol. 13, no. 2, pp: 154-164, 2004.

[10] Ali Al-Haj, “Combined DWT-DCT Digital Image Watermarking” Journal of Computer Science 3 (9): 740-746, 2007.

[11] M. Hadun Ozaktas, Orhan Arikan, “Digital Computation of the Fractional Fourier Transform,” IEEE Transactions on signal processing, vol. 9, 1996, pp. 2141-2149.

[12] S.C.Pei, M.H.Yeh, “Two dimensional discrete fractional Fourier transform,” Signal Processing , vol. 67, 1998, pp. 99- 108.

[13] Gaurav Bhatnagar and Balasubramanian Raman" A New SVD Based Watermarking Framework in Fractional Fourier Domain" ICCIT, IEEE2008, pp:539-544

[14] M. Ejima, and A. Myazaki, 2001." On the evaluation of performance of digital watermarking in the frequency domain," in Proc. of the IEEE Int. Conf. on Image Processing, 2: 546-549.

[15] Ashraf Aboshosha, M. Hassan, M. Ashour, and M. El Mashade, “Image Denoising based on Spatial Filters, an Analytical Study” ICCES09, Cairo, Egypt 2009.

[16] S.Voloshynovskiy, , S. Pereira and T. Pun, 2001. "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks,"Comm. Magazine, 39(8): 118-126

[17] S. Pereira, J.J.K. O’Ruanaidh, F. Deguillaume, G. Csurka, T. Pun, Template based recovery of Fourier-based watermarks using log-polar and log-log maps, in: Proceedings of the IEEE International Conference Multimedia Computing Systems, vol. 1, Florence, Italy, June 1999, pp. 870–874.

[18] S. Pereira, T. Pun, Robust template matching for affine resistant image watermarks, IEEE Trans. Image Process. 9 (6) (2000) 1123–1129.

[19] J.J.K. O’Ruanaidh, T. Pun, Rotation, scale, and translation invariant digital image watermarking, in: Proceedings IEEE International Conference Image Processing, Santa Barbara, CA, 1997, pp. 536–539.