Robust and secure fractional wavelet image watermarking

Ehab H. Elshazly, Osama S. Faragallah, Alaa M. Abbas, Mahmoud A. Ashour, El-Sayed M. El-Rabaie, Hassan Kazemian, Saleh A. Alshebeili, et al.

Signal, Image and Video Processing

ISSN 1863-1703

SIViP
DOI 10.1007/s11760-014-0684-x

Springer

SIViP
DOI 10.1007/s11760-014-0684-x

ORIGINAL PAPER

Robust and secure fractional wavelet image watermarking

Ehab H. Elshazly · Osama S. Faragallah · Alaa M. Abbas · Mahmoud A. Ashour · El-Sayed M. El-Rabaie · Hassan Kazemian · Saleh A. Alshebeili · Fathi E. Abd El-Samie · Hala S. El-sayed

Received: 11 July 2013 / Revised: 17 June 2014 / Accepted: 19 June 2014

Abstract This paper presents an efficient fractional wavelet transform (FWT) image watermarking technique based on combining the discrete wavelet transform (DWT) and the fractional Fourier transform (FRFT). In the proposed technique, the host image is wavelet transformed with two resolution levels, and then, the middle frequency sub-bands are FRFT transformed. The watermark is hidden by altering the selected FRFT coefficients of the middle frequency sub-bands of the 2-level DWT-transformed host image. Two pseudo-random noise (PN) sequences are used to modulate the selected FRFT coefficients with the watermark pixels, and inverse transforms are finally applied to get the watermarked image. In watermark extraction, we just need the same two PN sequences used in the embedding process and the watermark size. The correlation factor is used to determine whether the extracted pixel is one or zero. The proposed fractional wavelet transform (FWT) image watermarking method is tested with different image processing attacks and under composite attacks to verify its robustness. Experimental results demonstrated improved robustness and security.

Keywords Watermarking · DWT · FRFT · Security and robustness

E. H. Elshazly · M. A. Ashour
Engineering Department, NCRRT, EAEA, 3 Ahmed Al-Zomar, 8th District, Nasr City, Cairo, Egypt

O. S. Faragallah (✉)
Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
e-mail: osam_sal@yahoo.com

A. M. Abbas · E.-S. M. El-Rabaie · F. E. Abd El-Samie
Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

H. Kazemian
Intelligent Systems Research Centre, Faculty of Computing, London Metropolitan University, London, UK

S. A. Alshebeili
Electrical Engineering Department, KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICS), King Saud University, Riyadh, Saudi Arabia

F. E. Abd El-Samie
KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICS), King Saud University, Riyadh, Saudi Arabia

H. S. El-sayed
Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-kom, Egypt

1 Introduction

Watermarking has attracted researchers for many years, because through watermarking, we can embed data in digital media including audio, image and video. This technique gives a solution to overcome the illegal copy and reproduction problems. Watermarking is a strong way for ownership proof, and its robustness is measured by surviving attacks. Watermarking finds applications in various fields like data hiding, copyright protection and image authentication. In general, there are four challenges for good watermarking schemes, which are imperceptibility, robustness, capacity and security. Numerous watermarking algorithms have been proposed in literature depending on the DWT.

The DWT has proved to be suitable for watermarking applications. This transform allows the watermark embedding process in high frequencies, which leads to an unnoticeable change in the host data, by using the wavelet coefficients

Published online: 26 August 2014

in the detail sub-bands. However, the preferred wavelet is not carefully investigated in the literature. In [1], the author evaluated wavelet filter banks used in wavelet-based watermarking theoretically to find the best wavelet filter bank with the Daubechies wavelet. They deduced that db6 provides the best performance among the filter banks examined with respect to the quality of watermarked image and robustness of the watermark. In [2], authors tested eight families of wavelets, both orthogonal and biorthogonal wavelets have been compared, and they deduced that the Haar wavelet outperforms the other wavelet families.

Another transform domain that attracted attention of researchers in recent years for watermarking is the FRFT. In [3], the authors presented image watermarking in the fractional Fourier transformation (FRFT) domain. This approach uses a combination of the space and spatial/frequency domains. It offers two more degrees of freedom, resulting in the possibility to generate more watermarks than those in the FT and DCT domains. In [4], a digital watermark embedding/detection method for image was presented utilizing the chirp signal as a watermark and embedding in the FRFT domain of the image. The watermark position and the transform order are used as the encryption keys. It was shown that this algorithm is not only of good imperceptibility and security, very robust to JPEG compression and noise attacks, but also can provide protection under the cropping and filtering. In [5], the authors present a non-blind watermarking algorithm in the FRFT domain. Both the cover image and the watermark were transformed to FRFT domain, and the watermark coefficients were added in predefined positions to the FRFT coefficients of the cover image. Different watermarks with different sizes were tested to study the effect of watermark length on the visual quality of the watermarked image and the robustness of the algorithm. The author in that paper searched for security and capacity, but the robustness of the algorithm under different attack was not studied.

The main purpose of this paper was to take the advantages of jointing two transforms as a means to enhance robustness, imperceptibility and security of the watermarking method. The use of two transforms can gain the advantages of both domains, which gives the robustness requirements for watermarking. Jointing FRFT with another transform does not only improve robustness, but also enables using extra keys of security (transformation angles) in FRFT to enhance the overall security of the watermarking algorithm. First, each joint transform is adjusted to give its best performance under no attack using the controlling factors (embedding factor and threshold), and then the performance is measured under different common image processing attacks.

From the fact that DWT gives good robustness and FRFT insures security, we suggest to join the two transforms to derive a robust and secure watermarking algorithm. In [6], we have tried to test jointing FRFT with different transform domains (DWT, DCT and DST) to get a robust and secure algorithm, and we have deduced that DWT–FRFT gives the best robustness against attacks, but the capacity was limited as we were embedding the watermark in all the FRFT coefficients. The concept of using fractional wavelet transform was proposed in [7], and the authors had shown that scheme achieved better security due to the three-level security structure they provided by using two transform and a secret key, but there were not enough attacks to test their algorithm, and also capacity was not mentioned.

In this paper, we propose a secure and robust watermarking method that fulfills watermarking requirements. Security improvement in proposed fractional wavelet transform (FWT) watermarking method was achieved by embedding the watermark in a certain length of the FRFT coefficients. The start point and the length of modified coefficients in addition to the transformation angles in both x- and y-directions are used as extra secret keys. In the embedding stage, two PN sequences are used to be embedded in the FRFT coefficients of the selected DWT middle sub-bands. The embedding process is carried out according to the watermark pixel value (zero or one). At extraction, the same two PN sequences are generated and for each watermark pixel, the correlation factor between the FRFT coefficients and the corresponding PN sequence is calculated. The average correlation is compared to a threshold and upon that, a decision whether the extracted pixel was one or zero is taken. The proposed secure FWT watermarking method is tested under different attacks, and its security aspect was verified.

The rest of the paper is arranged as follows. Section 2 describes the DWT, the concept of FRFT and the FWT method for image watermarking. Section 3 gives in detail the watermarking process with FWT including embedding and the extraction algorithms. The performance evaluation and evaluation metrics are presented in Sect. 4. Section 5 presents the experimental results and discussion. Finally, the conclusion is given in Sect. 6.

2 Transform domain and digital watermarking

2.1 The discrete wavelet transform (DWT)

The DWT represents the approximation and detail of a signal in two separate signal sequences. The two-band decomposition–reconstruction wavelet filter bank is illustrated in Fig. 1. The $H_0(z)$ gives the approximation as a low-pass filtering of the signal, while $H_1(z)$ gives the details as a high-pass filtering of the signal. The main requirement of the wavelet basis function is that it achieves perfect reconstruction, by satisfying the following equations [8–10].

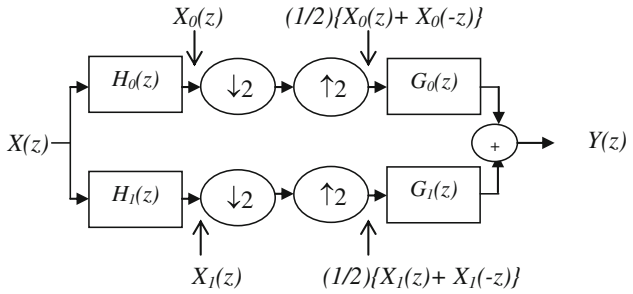


Fig. 1 The two-band decomposition-reconstruction wavelet filter bank

$$\{H_0(z)G_0(z) + H_1(z)G_1(z)\} = 2 \tag{1}$$

$$H_1(z) = z^{-k}G_0(-z) \quad \text{and} \quad G_1(z) = z^k H_0(-z) \tag{2}$$

For the Haar wavelet transform, the transfer functions of the filters are given by:

$$H_0(z) = \frac{1}{2}\left(1 + z^{-1}\right) \tag{3}$$

$$G_0(z) = (z + 1) \tag{4}$$

$$G_1(z) = \frac{1}{2}(z - 1) \tag{5}$$

$$H_1(z) = \left(z^{-1} - 1\right) \tag{6}$$

2.2 Fractional fourier transform

The FRFT is considered as the general form of the Fourier transform, which is an effective 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. When comparing between the FRFT and traditional FT, we find that the FRFT has a rotational angle in both the x- and y-directions, which means that the FRFT has one extra degree of freedom. The p[th] order FRFT of a signal is defined as [11,12]:

$$F^p[f(x)] = \int_{-\infty}^{\infty} K_p(x,u)\, f(x)\, \mathrm{d}x, \qquad 0 \le |p| \le 2 \tag{7}$$

$$K_p(x,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}} \exp\left(j\frac{x^2+u^2}{2}\cot\alpha - j\frac{xu}{\sin\alpha}\right) & \text{if} \quad \alpha \neq n\pi, \\ \delta(u-x) & \text{if} \quad \alpha = 2n\pi, \\ \delta(u-x) & \text{if} \quad \alpha = (2n+1)\pi, \end{cases} \tag{8}$$

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

$$f(x) = F^{-p}\left[F^p(f(x))\right] \tag{9}$$

2.2.1 The discrete fractional fourier transform (DFRFT)

Let $f(x)$ be a sampled periodic signal with a period Δ_0, the p[th] order discrete fractional Fourier transform (DFRFT) of $f(x)$ can be obtained as [13]:

$$f_p = \sum_{k=-\frac{N}{2}}^{\frac{N}{2}-1} f\left(k\frac{\Delta_0}{N}\right) \sum_{n=-\infty}^{\infty} k_p\left(x, \left(n + \frac{k}{N}\right)\Delta_0\right) \tag{10}$$

2.2.2 Two-dimensional discrete fractional fourier transform (2D-DFRFT)

The forward and inverse two-dimensional discrete fractional Fourier transform (2D-DFRFT) of an image is computed as [14]:

$$F_{\alpha,\beta}(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} f(p,q)\, K_{\alpha,\beta}(p,q,m,n) \tag{11}$$

$$f_{\alpha,\beta}(p,q) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} F_{\alpha,\beta}(m,n)\, K_{-\alpha,-\beta}(p,q,m,n) \tag{12}$$

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 1-D DFRFT kernels.

2.3 Secure watermarking in fractional wavelet domain

In [7], the authors presented the idea of using DWT combined with FRFT, which was simply mentioned as (FWT). They used only one- level 2-D DWT followed by 2-D FRFT carried out on the two middle sub-bands LH and HL. Their security issue depends only on the FRFT transformation angles in both directions, and the key image used to generate the PN sequence as secret keys. The robustness and security they introduced were not high. So, we try to improve the robustness by applying two levels 2-D DWT and change the controlling factors (embedding factor and threshold). We also improve the security by employing extra keys such as the length and the start point of FRFT coefficients used to embed the watermark in.

3 The proposed FWT watermarking method

The proposed algorithm has three levels of security represented in:

1. The image used to generate the two PN sequences.
2. The FRFT transformation angles in both x- and y-directions, and

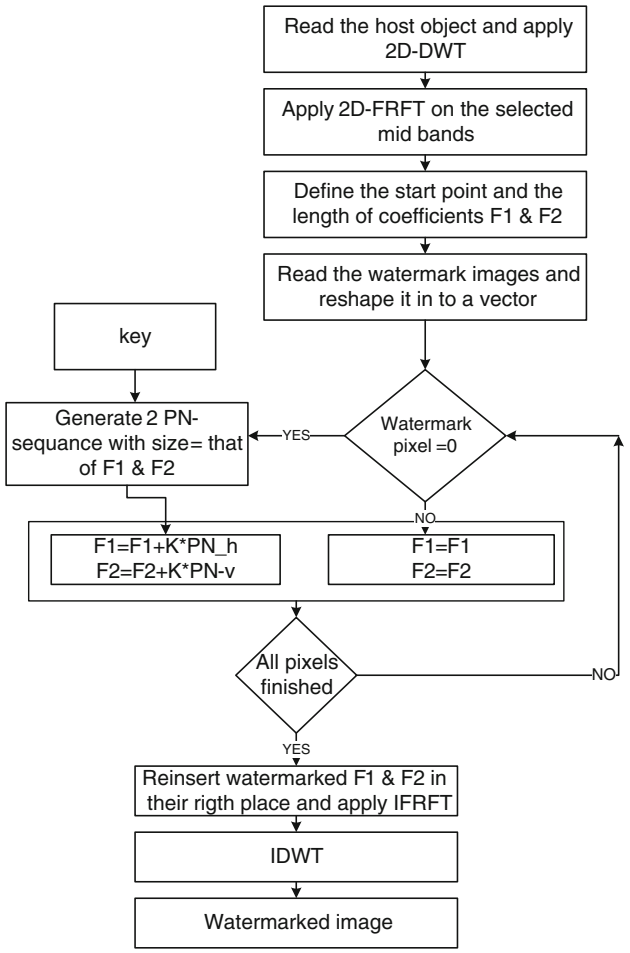


Fig. 2 Flowchart of the embedding procedure in the proposed FWT watermarking method

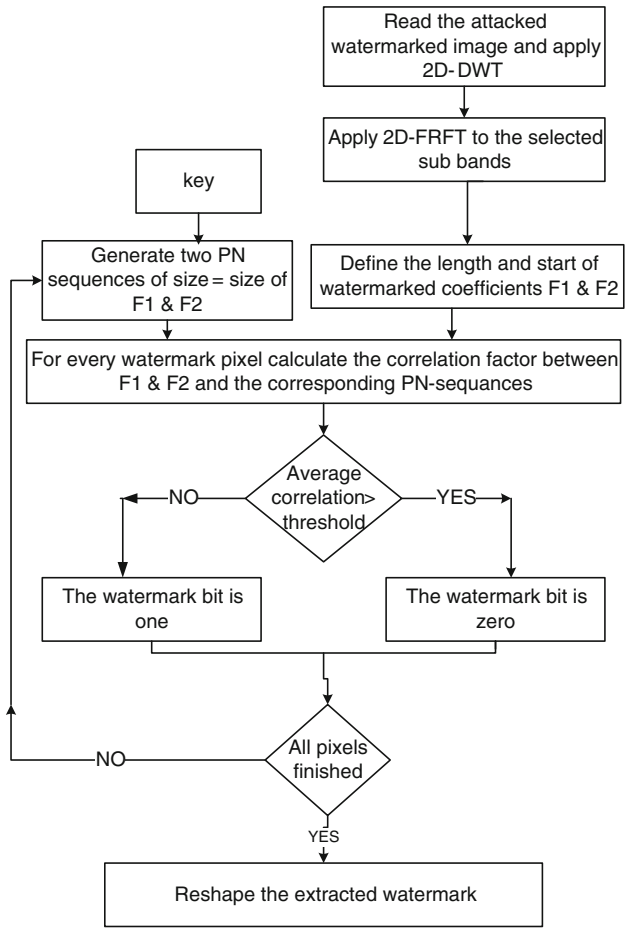


Fig. 3 Flowchart of the extraction procedure in the proposed FWT watermarking method

3. the length of FRFT coefficients to be watermarked, and their start point.

The proposed FWT image watermarking method embeds the watermark in a certain length of the FRFT coefficients and uses this length as a secret key. Embedding in a predetermined length not only improve security, but also enhances the capacity of the proposed FWT image watermarking method, as it enables to embed more than one watermark at different positions and with different lengths. Figures 2 and 3 show flowcharts of the embedding and extraction procedures in the proposed FWT watermarking method. There are three assumptions necessary for successful embedding and extraction of the watermark:

1. The watermark image to be embedded is a binary image.
2. The key used to initialize the PN sequence generator is available during embedding as well as extraction process.
3. The watermark size is known at the extraction phase.

The proposed FWT watermarking algorithm is semi-blind watermarking, and thus, the original host image is not required to extract the watermark, but the only needed are the watermark size and the same key to generate the PN sequences. To test the robustness of the algorithm, we intentionally attack the watermarked image with noise, cropping, compression, etc., and then try to extract the watermark from the attacked watermarked image.

4 Performance evaluation

Several experiments have been performed to evaluate the effectiveness of the proposed FWT watermarking method. The proposed method has been compared to the methods mentioned in [6] and [7]. We used MATLAB R2013a to perform simulation experiments. The 256 level 512×512 Lena image has been used in experiments as the cover image, and the COPYRIGHT image has been used as a watermark with size 20×50. Figure 4 illustrates the two images (original and cover).

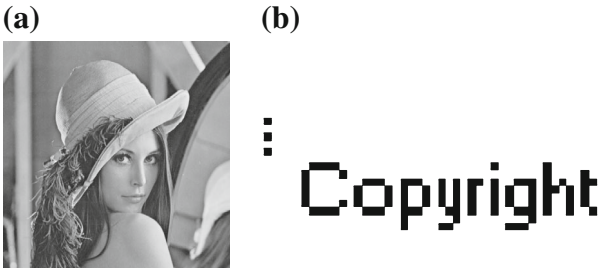


Fig. 4 The test images. **a** Original image **b** watermark image

In the proposed FWT watermarking method, the selected sub-bands are $CH2$ and $CV2$. We perform FRFT with angle 80 in both directions. The same angles used in [6] for comparison. The robustness and imperceptibility are generally used for evaluation [15]. The two metrics are explained below. Imperceptibility denotes that the host image still has the same quality even after watermark embedding. The quality of the host image is measured with the peak signal-to-noise Ratio (PSNR) in dB as follows [16]:

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{RMSE}\right) \tag{13}$$

where $RMSE$ is the root-mean-square error between the original and watermarked images.

Attacks attempt to remove or destroy the embedded watermark, intentionally or unintentionally. By calculating the robustness, we can measure the immunity of the watermark to attacks [17]. In this work, we use the robustness results for traditional attacks like image cropping, Gaussian noise, salt and pepper noise, rotation, and compression. These attacks are a good representation of the more general attacks. For example, cropping is a geometrical attack, noise is a degrading attack, and compression is a removal attack. The similarity between the original watermark and the recovered watermark is measured using the correlation factor ρ as follows:

$$\rho\left(w, w'\right) = \frac{\sum_{i=1}^{N} w_i w_i'}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} w_i'^2}} \tag{14}$$

where N is the number of pixels in the watermark, and w and w' are the original and extracted watermarks, respectively. The correlation factor ρ may take values between 0 (random relationship) and 1 (perfect linear relationship).

Firstly, we optimize the watermarking algorithm to get the best imperceptibility (low image degradation) under normal conditions (no attack) and good robustness (highest similarity between original and extracted watermark) by choosing the best embedding factor K. Figure 5a–e shows two curves, and the down-going curve represent the imperceptibility, which is the correlation factor between original host image and watermarked image. The up-going curve represents the robustness through the correlation factor between original and extracted watermarks.

In Fig. 5, we choose $k = 4.5$ for DWT–FRFT, $k = 1.5$ for DCT- FRFT and FRFT, $k = 15$ for DST–FRFT and $k = 4.5$ for the proposed FWT as these values give both good imperceptibility and robustness to attacks. The point where the two curves intercept is not necessarily the best choice for the embedding factor as this value should be chosen depending on the performance under attacks. For example, the curve on Fig. 5a shows that at $k = 0.55$, the correlation factor between original and extracted watermarks is 1. This means that $k = 0.5$ gives the required robustness under no attacks, but if the watermarking algorithm with $k = 0.5$ is tested under attacks; the robustness will not be perfect any more. So, $k = 1.5$ is chosen, and it is noticed that for larger values of k than 1.5, the improvement in robustness under attacks will be small, and at the same time, the watermarked image will have more degradation. So, the chosen values give good imperceptibility and robustness against attacks. In all the algorithms, the FRFT with transformation angle of 80° in both x- and y-directions, corresponding to transformation order of 0.8889 in both x- and y- directions, is used. These values are used as secret keys. The PSNR values for the watermarked images and the correlation factor between original and extracted watermarks are given in Table 1.

5 Results and discussion

We have fixed the embedding factor to the value used in [6] ($k = 4.5$) to study the effect of the length of coefficients to be watermarked and their position. We have changed the length from 1,000 coefficients to 9,000 coefficients and tried their position once at the beginning and once in the middle or at the end. The results for PSNR and correlation are listed in Table 2. It is clear from the Table 2 that increasing the length of coefficients to be watermarked decreases similarity between the original and watermarked image, and at the same time, it improves similarity between the original and extracted watermarks.

After choosing the length and position of the watermarking coefficients, we have chosen a new embedding factor k that ensures good robustness with the proposed algorithm. We have also changed the transformation angles in both x- and y-directions to enhance the performance of the proposed algorithm. The new value of the embedding factor is $k = 7.5$, and the transformation angles are 75.6° and 74.7° in both x- and y-directions corresponding to transformation orders of 0.84 and 0.83. These values were chosen after several trials to get the best evaluation metrics values of PSNR = 31.15 dB and correlation factor of 1 under no attack. Let us study the improved security in two cases.

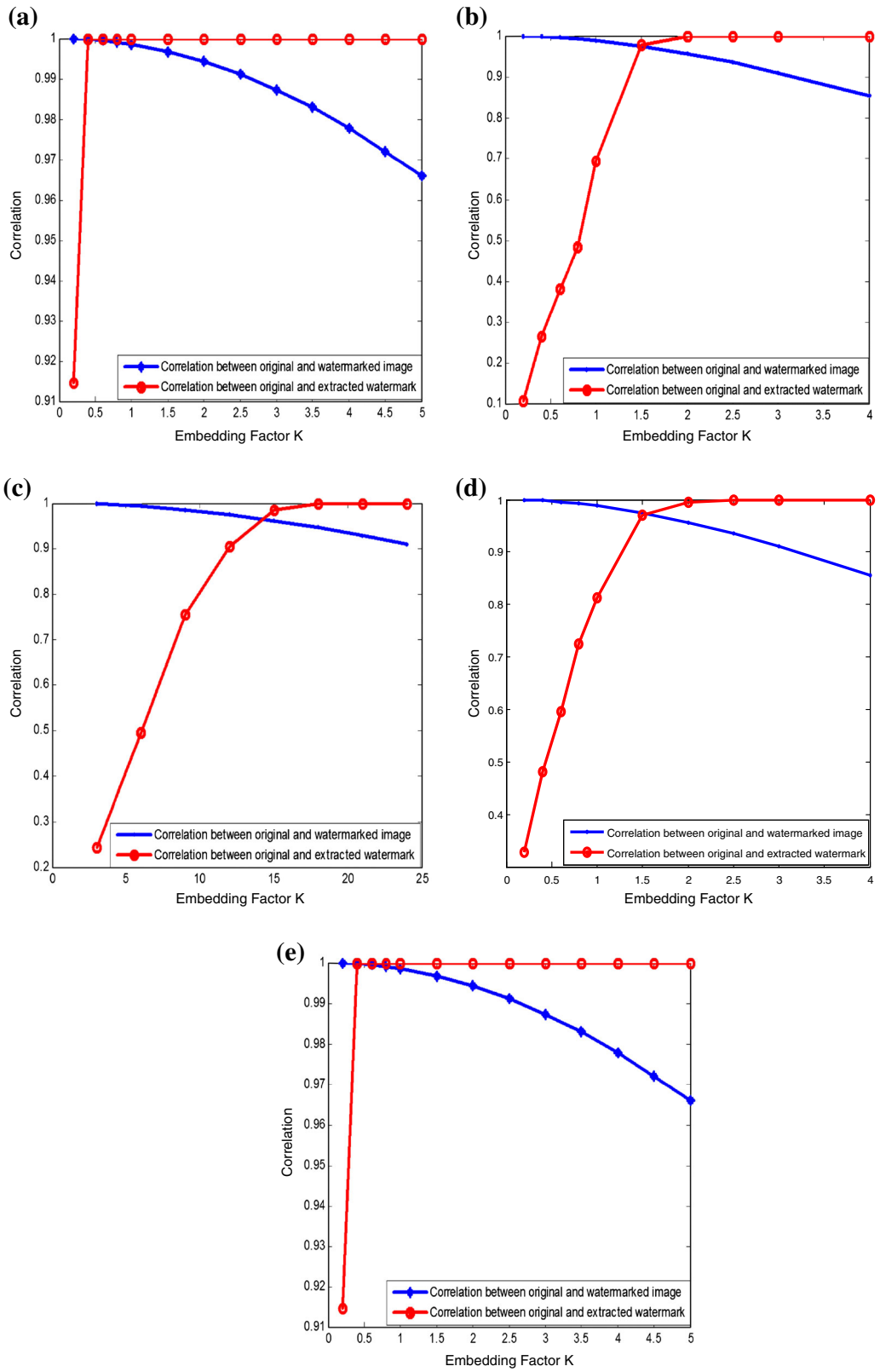


Fig. 5 The relation between the embedding factor K and the correlation factor **a** in DWT–FRFT, **b** DCT-FRFT, **c** DST–FRFT, **d** FRFT and **e** proposed FWT

Table 1 The PSNR and correlation factor for different watermarking methods

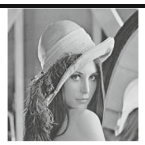
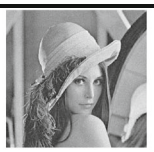
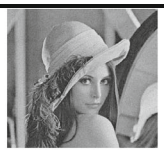
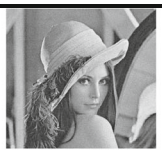
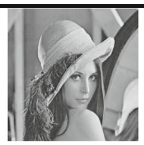
Metric	DWT-FRFT [6]	DCT-FRFT	DST-FRFT	FRFT [7]	Proposed FWT
Watermarked image					
PSNR (dB)	+26.88	+27.39	+24.06	+27.39	+26.87
Extracted watermark					
Correlation	1	0.9787	0.9844	0.9693	1

Table 2 Effect of length and position of watermarked coefficients

Number of coefficients	Metrics	Beginning	Middle	End
1,000	PSNR (dB)	39.15	38.80	39.74
	correlation	0.7095	0.7455	0.6970
3,000	PSNR (dB)	34.47	34.35	34.64
	correlation	0.9410	0.9455	0.9320
5,000	PSNR (dB)	32.10	32.05	32.22
	correlation	1	1	0.9895
9,000	PSNR (dB)	29.63	29.59	29.70
	correlation	1	1	1

Case 1: Assume any one knows the embedding and extraction steps, but does not know either the length or the start point. He will generate a PN sequence of length equal to the whole FRFT coefficients of the selected sub-band. In this case, the correlation factor between original and the extracted watermark will be −0.0023.

Case 2: Assume any one knows the embedding and extraction steps and the length of coefficients to be watermarked, but does not know the start point, and assume also just one coefficient shift from the true start. This gives a correlation factor between original and extracted watermarks of −0.0132.

After verifying security enhancement, the performance of the proposed FWT watermarking method under common image processing attacks has been tested and compared to that of [6]. As security and capacity are not affected by attacks, the robustness and imperceptibility only have been studied under these attacks.

The watermarked image has been cropped with different percentages. The performance results under cropping attack of ratios 25, 50 and 75 % are listed in Table 3. From this table, it is clear that all the watermarking algorithms give accepted performance under cropping attack except FRFT [7]. The DWT–FRFT and the proposed FWT watermarking methods can survive severe cropping attacks.

We have added Gaussian noise to the watermarked image and fixed the noise variance to 0.01 with different mean values. The correlation factor results are tabulated in Table 4. It is clear that both the DWT–FRFT and the proposed FWT watermarking methods give best performance.

The extracted watermark with both DWT–FRFT and the proposed FWT watermarking methods under Gaussian noise attack are shown in Fig. 6.

The performance of the DWT–FRFT and the proposed FWT watermarking methods has been evaluated under different types of noise (Gaussian noise, speckle noise, salt and pepper noise and Poisson noise), and the results are summarized in Table 5. It is clear that DWT–FRFT method gives the best performance.

We have compressed the watermarked image using a lossy compression technique with different quality values. The obtained results are summarized in Table 6, and the extracted watermarks under this attack are shown in Fig. 7.

It is clear that the DWT–FRFT and the proposed FWT watermarking methods give the best correlation between original and extracted watermarks even at low quality factors. This is attributed to the fact that embedding is carried out in the middle frequency sub-band, which is less affected by the compression attack.

Table 3 Correlation factor for all watermarking methods under cropping attack

Cropping percentage (%)	DWT–FRFT [6]	DCT–FRFT	DST–FRFT	FRFT [7]	Proposed FWT
25	1	0.9633	0.9743	0.9062	1
50	1	0.8354	0.9221	0.6214	0.9947
75	0.9743	0.6742	0.8197	0.5122	0.9320

Table 4 Correlation factor under Gaussian noise attack with different mean values and variance = 0.01

Mean value	DWT–FRFT [6]	DCT–FRFT	DST–FRFT	FRFT [7]	Proposed FWT
0	1	0.9626	0.9438	0.9320	1
0.2	1	0.7188	0.7082	0.9275	1
0.4	1	0.3600	0.4723	0.8670	1
0.6	0.9895	0.3403	0.3335	0.8154	0.9645
0.8	0.9104	0.1408	0.1408	0.7311	0.8317

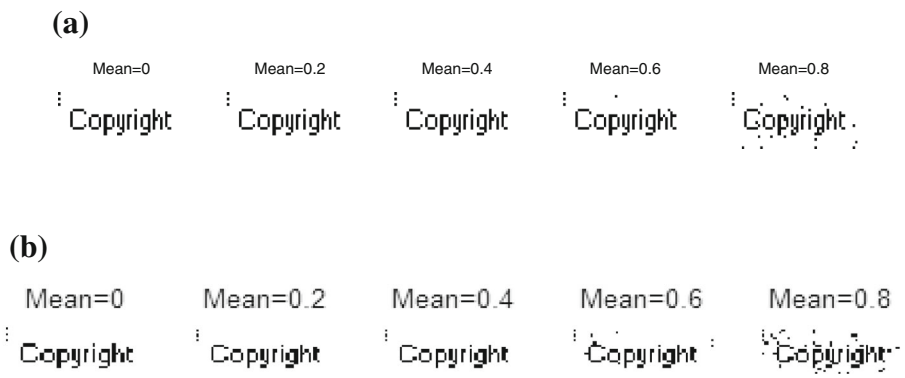


Fig. 6 Extracted watermark under Gaussian noise attack with different mean values and variance = 0.01. **a** Extracted watermarks with DWT–FRFT method. **b** Extracted watermarks with FWT method

Table 5 Correlation factor for different types of noise attacks

Noise type	DWT–FRFT [6]	Proposed FWT
Gaussian noise of variance 10 %	0.9275	0.8186
Salt and pepper noise of density 10 %	0.9947	0.9743
Poisson noise	1	1
Speckle noise of variance 10 %	0.9947	0.9645

Table 6 Correlation factor under JPEG compression attack with different quality levels

Quality factor	DWT–FRFT [6]	DCT-FRFT	DST–FRFT	FRFT [7]	Proposed FWT
0	0.0469	−0.0205	0.0140	0.0585	0.0331
20	0.3329	0.2004	0.1250	0.4141	0.2688
40	0.8822	0.3381	0.3067	0.5632	0.7437
60	0.9947	0.4528	0.4460	0.6959	0.9793
80	1	0.9165	0.7750	0.9104	1
100	1	0.9787	0.9844	0.9645	1

Table 7 gives the values of the correlation factor for the different watermarking methods under other attacks such as low-pass filtering, median filtering, motion blurring and sharpening.

The obtained results revealed that jointing the FRFT with other transforms gives extra keys in both directions, which increases the security level over the classical transform algorithms. Hence, it is impossible to invert the FRFT without knowing the correct transformation angles. Table 1 revealed that in normal case (no attack), each algorithm is adjusted to give the best imperceptibility and robustness. It was noticed that both DWT–FRFT and the proposed FWT watermarking

Fig. 7 Extracted watermarks under JPEG Compression attack with different quality factors. **a** DWT–FRFT watermarking method. **b** Proposed FWT watermarking method

Table 7 Correlation factor for the watermarking methods under different attacks

Attack	DWT–FRFT [6]	DCT–FRFT	DST–FRFT	FRFT [7]	Proposed FWT
Gaussian low-pass filtering	1	0.6044	0.7872	−0.0270	1
Median filtering	−0.7562	0.1188	0.1637	−0.0060	−0.6468
Motion blurring	0.9895	0.0936	0.1309	−0.0290	0.8525
Sharpening	1	1	1	−0.0284	1

methods give the highest correlation between the original and extracted watermarks with high imperceptibility. The imperceptibility has been enhanced by about four dBs as shown in Table 2 due to embedding in certain length of coefficients not in all coefficients. It is possible to embed more than one watermark at different positions.

The robustness of the proposed FWT watermarking method was tested under different attacks as shown in Tables 3, 4, 5, 6 and 7. It was found that the robustness of the proposed FWT watermarking method is comparable with that in [6] with good security. This robustness arises from the fact that the larger the magnitude of the wavelet coefficient, the more significant it is to embed stronger watermarks. From Table 7, we can notice that all watermarking methods were not robust against median filtering as it makes reordering of the pixels. Because watermarking techniques are pixel-oriented, any re-ordering of the pixels destroys the watermark [18].

It is necessary to test the performance of the proposed FWT watermarking method under real-time transmission conditions. In a step to simulate real-time conditions for image transmission, we have considered a transmission medium affecting the transmitted watermarked image with more than one attack. Some modifications in the proposed FWT watermarking method have been performed. The length of watermarked FRFT coefficients was increased from 9,000 to 13,000, and the embedding factor k was increased to 10.5. The transformation angles stayed the same.

It is well known that increasing the value of the embedding factor as well as the length of FRFT coefficients to be watermarked has its impact on the imperceptibility of the proposed FWT watermarking method. These factors were chosen to keep the PSNR between the original and watermarked images at the same level of that of watermarking algorithm presented in [6]. At the same time, these modifications ensure robustness of the watermarking scheme.

Table 8 The PSNR and correlation factor without attacks

Metric of evaluation	DWT–FRFT [6]	Proposed FWT
PSNR	+26.87 dB	+26.88 dB
Correlation	1	1

From Table 8, it is clear that both the proposed FWT watermarking method and the method in [6] give approximately the same results without attacks. Now, it is required to evaluate their performance under different combinations of attacks.

From Table 9, it is clear that the proposed FWT watermarking method gives better robustness due to the strong watermark inserted by choosing a large embedding factor. Besides the improved robustness, the imperceptibility, security and capacity of the proposed method are high.

6 Conclusion

This paper presented a robust and secure semi-blind FWT digital image watermarking method. In this method, the cover image is firstly subjected to two levels DWT, and then the two middle sub-bands are subjected to FRFT. Only, a certain length of these FRFT coefficients is used to embed two PN sequences according to the watermark bits. The length of those coefficients and their start position as well as the transformation angles in both x- and y-directions are

Table 9 Correlation factor under different combinations of attacks

Attack	DWT–FRFT [6]	Proposed FWT
Blurring + Gaussian low-pass filtering (GLPF)	0.9844	0.9021
Blurring + JPEG compression with $Q = 100$	0.9895	0.9320
Salt and pepper noise of density 10 % + GLPF	0.9895	1
Salt and pepper noise of density 10 % + Poisson noise	0.9947	1
Gaussian noise of variance 0.05 + Salt and pepper noise of density 10 %	0.9275	0.9693
Salt and pepper noise of density 10 % + Speckle noise of variance 0.1	0.9793	1
Salt and pepper noise of density 10 % + block size of (96 × 96) cropping	0.9793	1
Gaussian noise of variance 0.05 + block size of (96 × 96) cropping	0.9693	0.9895
GLPF + block size of (96 × 96) cropping + Poisson noise	1	0.9895
Salt and pepper noise of density 5 % + Gaussian noise of variance 0.05 + Poisson noise	0.9549	0.9947

used as extra secret keys for ensuring good security. In the recovery process, the robustness of the proposed method has been tested under attacks. The proposed FWT watermarking method showed improved security compared with other watermarking methods. Capacity has also been improved, as it became possible to embed more than one watermark of different size at different positions. The effect of changing the fractional power was taken into consideration, and after several trials, the transformation angles that achieve good watermarking requirements were found out. To simulate real-time transmission conditions by applying composite attacks, some modifications in the proposed FWT watermarking method were done, and the performance was evaluated under these attacks.

References

1. Miyazaki, A.: A study on the best wavelet filter bank problem in the wavelet-based image watermarking. In: 18th European Conference on Circuit Theory and Design, ECCTD, pp. 184–187 (2007)
2. Brannock, E., Weeks, M., Harrison, R.: Watermarking with wavelets: simplicity leads to robustness. In: Proceedings of the IEEE Southeast Conference 2008, Huntsville, Alabama, April 3–6, pp. 587–592 (2008)
3. Djurovic, I., Stankovic, S., Pitas, I.: Digital watermarking in the fractional Fourier transformation domain. J. Netw. Comput. Appl. **24**(2), 167–173 (2001)
4. Yu, F.Q., Zhang, Z. K., Xu, M.H.: A digital watermarking algorithm for image based on fractional Fourier transform. In: 2006 1ST IEEE Conference on Industrial Electronics and Applications, IEEE (2006)
5. Hussain, F., Khan, E., Farooq, O.: Embedding and non-blind extraction of watermark data in images in FRFT domain. In: International Conference on Multimedia, Signal Processing, and Communication Technologies 14–16 March, pp. 280–283 (2009)
6. Elshazly, Ehab H., Ashour, Mahmoud A., El-Rabaie, El-sayed M., Abbas, Alaa M., Kazemian, H.: An efficient fractional fourier transform approach for digital image watermarking. In: Proceeding of National Radio Science Conference NRSC (2012)
7. Pujara, Chirag, Bhardwaj, Ashok, Gadre, Vikram M.: Secured watermarking in fractional wavelet domains. IETE J. Res. **53**(6), 573–580 (2007)
8. Dietze, M., Jassim, S.: Filters ranking for DWT domain robust digital watermarking. EURASIP J. Appl. Signal Process. **2004**, 2093–2101 (2004)
9. Tao, P., Eskicioglu, A.M.: A robust multiple watermarking scheme in the DWT Domain. In: Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, pp. 133–144, October 25–28 (2004)
10. Tcheslavski, G.V.: Wavelets Fundamentals. http://ee.lamar.edu/gleb/dip/index.htm, April (2008)
11. Ozaktas, M.H., Arikan, O.: Digital computation of the fractional fourier transform. IEEE Transactions on Signal Processing **9**, 2141–2149 (1996)
12. Elhoseny, H.M., Ahmed, H.E.H., Abbas, A.M., Kazemian, H.B., Faragallah, O.S., El-Rabaie, S.M., Abd El-Samie, F.E.: Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation. Signal Image Video Process. J. (2013). doi:10.1007/s11760-013-0490-x. Springer
13. Pei, S.C., Yeh, M.H.: Two dimensional discrete fractional fourier transform. Signal Process. **67**, 99–108 (1998)
14. Bhatnagar, G., Raman, B.: A new SVD based watermarking framework in fractional Fourier domain. Contemp. Comput. **IC3**(1), 107–118 (2010)
15. Ejima, M., Myazaki, A.: On the evaluation of performance of digital watermarking in the frequency domain. In: Proceedings of the IEEE International Conference on Image Processing, pp. 546–549 (2001)
16. Aboshosha, A., Hassan, M., Ashour, M., El Mashade, M.: Image denoising based on spatial filters, an analytical study. In: ICCES09, Cairo, Egypt (2009)
17. Voloshynovskiy, S., Pereira, S., Pun, T.: Attacks on digital watermarks: classification, estimation-based attacks, and benchmarks. Comm. Mag. **39**(8), 118–126 (2001)
18. Sheng Xie, R., Zhou, M., Huang, C., Li, Y.: Anti-geometrical attacks image watermarking scheme based on template watermark. In: Proceedings of Computer Network and Multimedia Technology, CNMT, pp. 1–4 (2009)