# Secure Watermarking in Fractional Wavelet Domains

Chirag Pujara, Ashok Bhardwaj, Vikram M Gadre & Sourabh Khire

IETE Journal of Research
Vol 53, No. 6, November-December 2007, pp 573-580

# Secure Watermarking in Fractional Wavelet Domains

CHIRAG PUJARA, ASHOK BHARDWAJ, VIKRAM M GADRE
Department of Electrical Engineering, Indian Institute of Technology Bombay, Mumbai 400 076, India.
e-mail: pchirag@gmail.com

AND

SOURABH KHIRE
Department of Electronics and Telecommunication Engineering, Don Bosco Institute of Technology, Mumbai 400 070, India.

**This paper proposes a novel technique for securing and preventing the misuse of images by digital image watermarking. The technique is based on a hybrid approach employing the Wavelet Transform (WT), and the Fractional Fourier transform (FRT) termed as the Fractional Wavelet Transform (FWT). We present experimental evidence to establish the advantages of this scheme over other watermarking schemes when subject to attacks such as noise and compression.**

*Indexing terms: Watermarking, Fractional fourier transform, Wavelet transform, Security.*

## 1. INTRODUCTION

With the immense growth of the Internet, the need for securing the sensitive data available over the web has grown manifold. The situation has particularly worsened for the images available over the Internet, and there have been instances where images have been stolen and misused. Watermarking is a method in which a particular bit sequence, known as the watermark, is embedded in the original data to make it authentic. Any attempt to remove the watermark, ideally results in complete degradation of the original data and hence renders the image useless. In image watermarking, one image is hidden in another image. The image to be protected is known as the source image or a cover image, while the image that is embedded in the source image is termed as a watermark image or simply, a watermark. The watermarking algorithm should be secure enough to prevent an unauthorized person from extracting the watermark from the watermarked image.

On the basis of watermark strength or perceptibility, watermarking can be classified as, (l) visible water-marking (2) Invisible watermarking (3) Visible watermarking is like stamping a watermark on the paper. It is useful to immediately convey the claim of ownership. Invisible watermarking is rather complex, and is more of an aid in catching a thief, than for discouraging theft as in the case of visible watermarking.

Three challenges for a good watermarking scheme are

1. Security
2. Invisibility
3. Robustness

Watermarking finds applications in various fields like data hiding, image authentication, and covert communication.

Numerous watermarking algorithms have been proposed in the literature, so far. The concept of using Code Division Multiple Access (CDMA) based watermarking scheme in the wavelet domain is considered in [2]. The authors have shown that in the wavelet domain, adding a watermark in LH and HL sub-bands will be less perceptible, and more robust against compression and noise attacks. The security aspect of spread spectrum based watermarking is discussed in [3]. The security is due to a secret key, which is used for random number generation. This same key is required for both the embedding and recovery of watermark. The concept of watermarking in the Fractional Fourier Transform domain has been discussed in [4,5]. They have shown that instead of using the Discrete Fourier Transform (DFT) or the Discrete Cosine Transform (DCT), the Fractional

Paper No 75-A; Copyright © 2007 by the IETE.

Fourier Transform (FRT) will provide greater freedom to embed the watermark in the desired Fractional Fourier domain. This also enhances the security of the method because the parameter (angle) of FRT is hidden, even if the watermarking scheme is known.

In this paper, we propose a method for digital image watermarking which falls in the category of invisible watermarking. Here, the main focus is on security. In this method we apply a wavelet operator on the source image, followed by a Fractional Fourier operator. Our method has an additional degree of freedom, compared to the method based on the Discrete Wavelet Transform (DWT) [6] or FRT alone. We use the spread spectrum technique to embed a watermark in the transform domain coefficients. To generate the pseudo random sequence, we use a special 8-bit key image which consists of 35 pixels. This key is needed to recover the watermark from the watermarked image. This feature also adds to the security of the method.

## 2. BASIC THEORY

The Fractional Fourier Transform is a generalization of the conventional Fourier Transform. It has one more degree of freedom as compared to the conventional FT which is the angle [7,8]. It is useful for the localization of linear frequency modulated signals. The 2D FRT is simply an extension of the FRT having 2 degrees of freedom i.e., angles in both the directions '*x*' and '*y*'. The 2D FRT can be computed using its kernel $K(u,v)$ which will map the 2D signal $f(x,y)$ to $F(u,v)$ which constitutes the 2D Fractional Fourier domain [7,9].

$$F^{\alpha_x,\alpha_y} f(x,y) = \iint K_{\alpha_x,\alpha_y}(u,v;x,y) f(x,y)\,dxdy$$

where

$$K_{\alpha_x,\alpha_y}(u,v;x,y) = K_{\alpha_x}(u,x) K_{\alpha_y}(v,y)$$

$$K_\alpha(u,x) = A_\phi exp^{i\pi(\cot(\phi u^2) - 2\operatorname{cosec}(\phi ux) + \cot(\phi x^2))}$$

$$A_\phi = \sqrt{1 - i\cot(\phi)}$$

$$\phi = \frac{\alpha\pi}{2}$$

The Fractional Wavelet Transform was first defined by Mendlovic and David [10]. The use of the FWT for optical image encryption was first proposed by Chen and Zhao [11]. In the above references, the authors have defined the FWT to be a cascade of the FRT and the WT. However in our paper, the manner, in which the Fractional Wavelet Transform has been used for the watermarking of digital images, slightly varies from the FWT explained in the references mentioned above.

Here, we have applied the Wavelet operator on the digital image, and then applied the Fractional Fourier operator only on the LH and the HL sub-bands, which are further used for embedding the watermark. The FRT has not been applied on the LL sub-band, because it causes a lot of distortion in the watermarked image.

Also, the HH sub-band is not used for the embedding purposes, to increase the robustness of the scheme against the lossy compression attacks.

## 3. WATERMARKING IN FWT DOMAIN

This section gives a detailed algorithm for the embedding and the extraction of the watermark. Also, the assumptions necessary for the successful embedding and recovery of the watermark have been presented.

### A. Assumptions

(1) The watermark image to be embedded is a binary image.

(2) The key used to initialize the Pseudo-random Noise (PN) sequence generator is available during embedding as well as recovery of the watermark.

(3) The watermark size is known at the recovery phase.

### B. Steps to embed the watermark

(1) Apply the 2D-DWT once on the source image, to give four bands of wavelet coefficients; namely LL, LH, HL and HH.

(2) Choose any two of these bands, and apply the 2D-FRT on them with a desired angle. (We chose the LH and the HL coefficients and 81° for the FRT on both the axes).

(3) Initialize the PN sequence generator with a secret key.

(4) Generate two PN sequences with length equal to the size of the LH and the HL sub-bands respectively.

(5) Scan the watermark pixel by pixel. For a black pixel, add the PN sequences scaled by an

appropriate factor to the LH and the HL coefficients respectively. For a white pixel, keep the LH and the HL coefficients unmodified.

(6) Repeat steps 4 and 5 till each pixel of the watermark is embedded.

(7) Apply the inverse transforms to obtain the watermarked image

Figure 1 shows the flowchart for the watermark embedding.

## C. Steps to recover the watermark

(1) Apply the 2D-DWT on the watermarked image.

(2) Apply the 2D-FRT on the two bands of wavelet coefficients chosen in the embedding stage (LH and HL sub-bands in our case).

(3) Initialize the PN sequence generator with the key used during the embedding stage.

(4) Generate two PN sequences with length equal to the size of the selected sub-bands, These two sequences will necessarily be the same as generated during the embedding stage.

(5) Compute the cross-correlation of both the selected sub-bands with the corresponding PN sequence, for each pixel of the watermark image. This gives a correlation vector with its length equal to the number of pixels in the watermark image. The elements of this correlation vector contain the cross-correlation values.

(6) Compare every element of this correlation vector with a threshold (which is the mean of correlation vector in our case) to obtain a vector containing

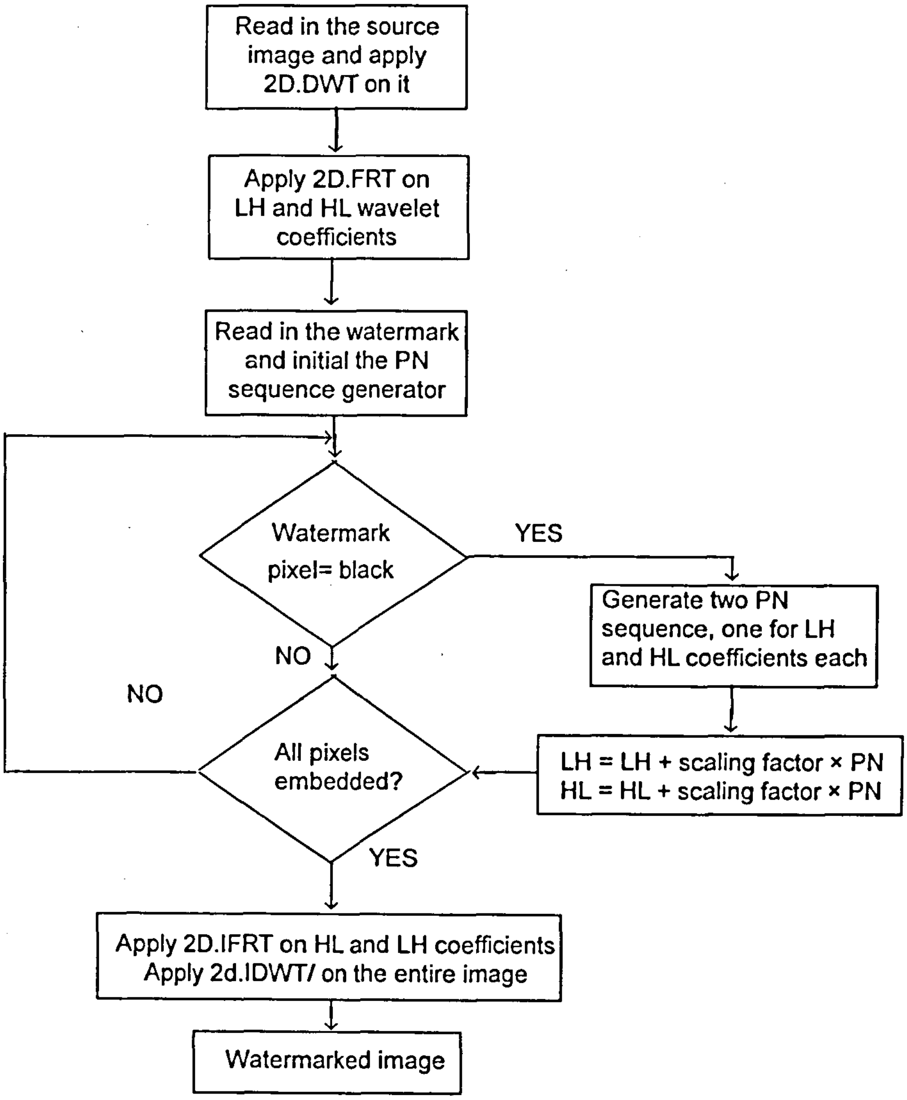

Read in the source image and apply 2D.DWT on it
Apply 2D.FRT on LH and HL wavelet coefficients
Read in the watermark and initial the PN sequence generator
Watermark pixel= black
YES
Generate two PN sequence, one for LH and HL coefficients each
NO
NO
All pixels embedded?
LH = LH + scaling factor × PN
HL = HL + scaling factor × PN
YES
Apply 2D.IFRT on HL and LH coefficients
Apply 2d.IDWT/ on the entire image
Watermarked image

Fig 1 Flowchart for embedding the watermark

the pixels of the extracted watermark by the following rule.

IF, the value of correlation > the threshold then,

the watermark pixel is identified as black.

ELSE, the watermark pixel is identified as white.

(7) Reshape the obtained vector to recover the watermark image.

Figure 2 shows the flowchart for the watermark extraction.

## 4. FEATURES OF THE PROPOSED WATERMARKING SCHEME

### A. Security Aspect

The main aim of this algorithm is to provide enhanced security. The key idea behind the proposed scheme is to use two different transforms which are independent of each other, and have their own degrees of freedom. The proposed algorithm has three levels of security. Since we apply both the DWT and the FRT, we get two levels of security. The third level of

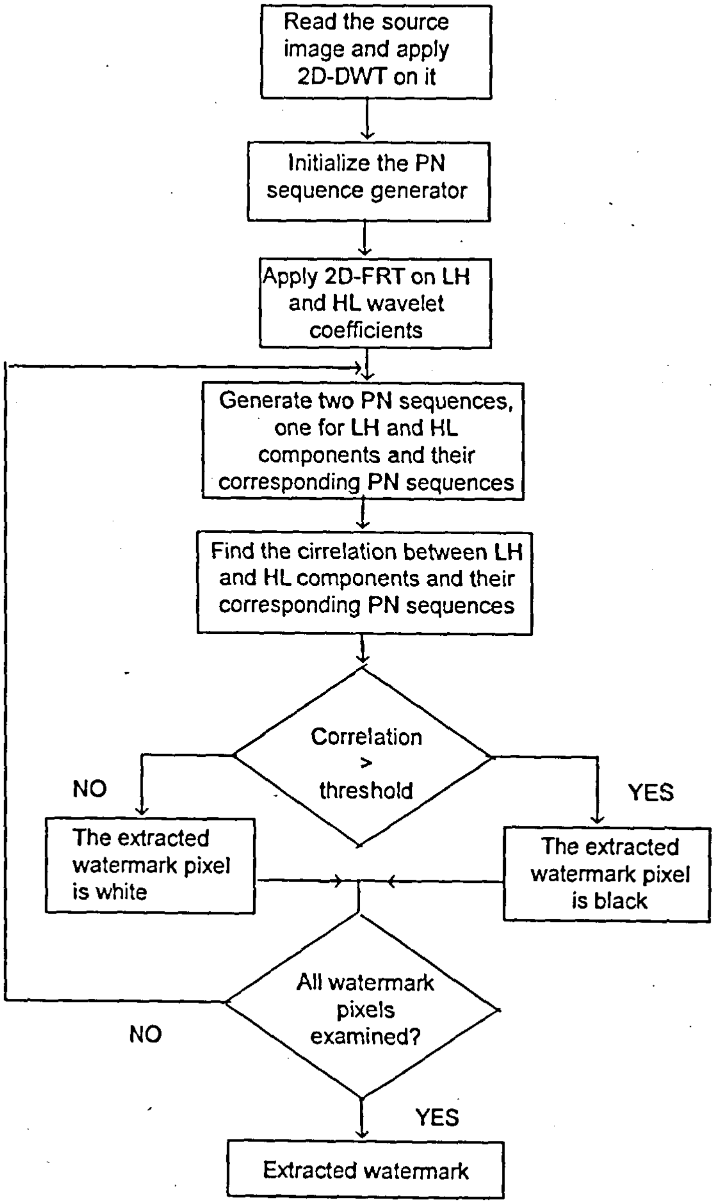

Read the source image and apply 2D-DWT on it
Initialize the PN sequence generator
Apply 2D-FRT on LH and HL wavelet coefficients
Generate two PN sequences, one for LH and HL components and their corresponding PN sequences
Find the cirrelation between LH and HL components and their corresponding PN sequences
Correlation > threshold
NO
YES
The extracted watermark pixel is white
The extracted watermark pixel is black
All watermark pixels examined?
NO
YES
Extracted watermark

Fig 2 Flowchart to recover the watermark

security is a secret key used for embedding the watermark.

The watermark is embedded in the transformed coefficients by a spread spectrum technique as defined below. We have used the "rand" function of MATLAB for generating the PN sequence. The seed for the PN sequence generator is a 'key' which, in our case, is a gray-scale image of 35 pixels. This unique key is needed at the time of embedding as well as at the time of extraction.

Thus, by construction, the proposed scheme employing a hybrid approach is more secure as compared to the watermarking algorithms employing only the WT or the FRT.

### B. Robustness

It has been observed that the effect of noise and compression is more in spatial domain techniques, like LSB based methods. LSB based methods alter the last bit of selected pixels, which generally gets chopped off in compression, or gets changed randomly due to addition of noise. Hence, generally transform based techniques are more robust against various attacks like noise, compression, lowpass filtering [1].

The dual-transform based scheme described has been found to be robust against the lossy compression and Additive White Gaussian Noise (AWGN) attacks. For testing robustness against compression attacks, we have used the popular JPEG technique, employing the 2D-DCT for compression. The watermark perceptibility is reduced because it has been embedded in the LH and HL coefficients and not in the coarse wavelet coefficients that have the highest energy concentration.

The correlation based method described in Section 3 is optimal for the additive watermarking scheme, provided that the source image has a Gaussian distribution.

## 5. SIMULATION RESULTS

The image that we used for watermarking is the standard' Lena' image as seen in Fig 3. Its size is 512 × 512 pixels. The watermark image is shown in Fig 4. Its size is 24 × 53 pixels. The images shown are not to scale. For measuring image quality, generally quantitative measures like Peak Signal to Noise Ratio (PSNR) and Percentage Absolute Error (%AERROR) are used. These are defined in eqn (2) and eqn (3) respectively [12].

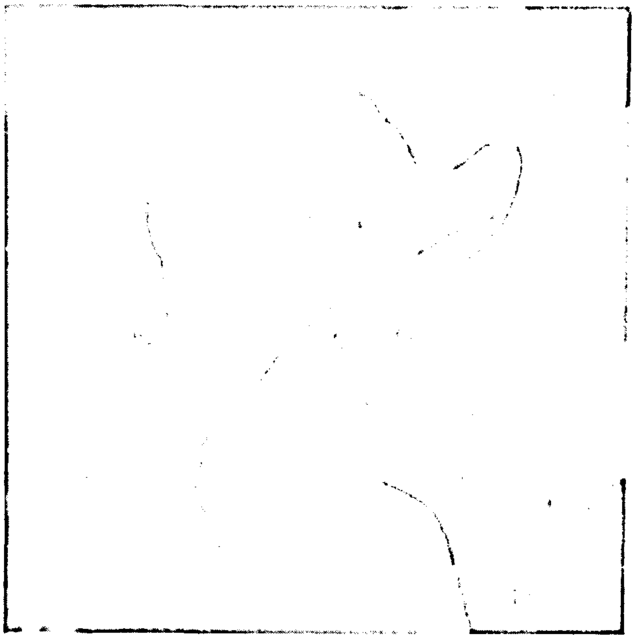


Fig 3 Image used for Water marking. Actual size 512 × 512

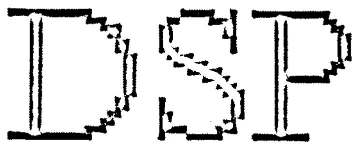


Fig 4 Watermark Image used for embedding Actual size 24 × 53

$$\mathrm{PSNR} = 10 \log \left[ \frac{\max(f(x,y)^2)}{\sum_{x=1}^{n} \sum_{y=1}^{n} \frac{(f(x,y)-g(x,y))^2}{mn}} \right] \quad (2)$$

where

$f(x,y)$ = pixel intensity of the source image. with $m$ rows and $n$ columns

$g(x,y)$ = pixel intensity of the image with watermark embedded in it

$$\%\mathrm{AERROR} = 100 \left[ \frac{\sum_{x=1}^{n} \sum_{y=1}^{n} |f(x,y)-g(x,y)|}{\sum_{x=1}^{n} \sum_{y=1}^{n} |f(x,y)|} \right] \quad (3)$$

As seen by the eqn (3), the % AERROR depicts the absolute value of the difference in the intensities of the original image and the watermarked image. The PSNR alone is not always a good measure for image quality. Our evaluation of the proposed scheme considers PSNR and %AERROR together as a measure of image quality. We have tested our watermarking scheme against compression (JPEG), and AWGN (N (0,0.01)) attacks.

We have compared the performance of our FWT-based scheme with other popular transform-based watermarking approaches such as, the DCT, the DWT and the FRT. The basic algorithm for embedding the watermark for all the above schemes is as follow

1. Apply the forward transformation kernel on the image to obtain the transformed image.
2. Select the appropriate transformed coefficients for embedding the watermark. For example, selecting one of the four sub-bands in DWT, or selecting the mid-frequency coefficients in case of DCT for embedding the watermark.
3. Embed the watermark using the spread spectrum approach explained in Section 3.
4. Apply the reverse transformation kernel to obtain the watermarked image.

Figure 5 shows the performance of the various watermarking schemes when subject to JPEG compression attack. The JPEG quality factor indicates the amount of compression of the image. For lower quality factors, the Compression Ratio (CR) is high and hence the compressed image is distorted. For higher quality factors, the C.R is low and hence the quality of the compressed image is good.

As seen in Fig 5, the PSNR is higher and the %AERROR is lesser for lower compression ratios for the FWT based scheme as compared to the schemes based on the DCT, the WT and the FRT. This indicates that our scheme is more robust against lossy compression as compared to the other schemes for quality factors upto about 60. It also indicates that the perceptibility of the watermark in the watermarked image is lesser in our scheme as compared to the FRT and the DWT based schemes for all the quality factors. However, for higher quality factors, the distortion in the watermarked image due to the addition of watermark is greater in our scheme as compared to the DCT based scheme. This may be attributed to the fact that the watermark is embedded in the mid-frequency coefficients of the DCT, thus reducing the perceptibility of the watermark in the watermarked image. However, in the FWT, the effect of the LH and the HL bands is perhaps not as insignificant.

Figure 6 shows the PSNR and the %AERROR curves for the recovered watermark. The watermark recovery is expected to be better for those schemes for which the strength of the embedded watermark is higher in the watermarked image. Thus, the watermark recovery can be improved at the cost of increased distortion in the watermarked image. Figure 5 and Fig 6 show that the watermark recovery for our scheme is comparable to the other schemes despite introducing lesser distortion in the watermarked image.

Figure 7 demonstrates the effect of a noise attack on the watermarked image. Here the watermark is embedded and then the watermarked image is subject to the noise attack in the form of the Additive White Gaussian noise with mean '0', and variance '0.01 '. The recovered watermark quality for all the schemes, drastically degrades when subject to noise. However, our scheme still performs better than the DCT and the FRT based schemes. Although the extracted

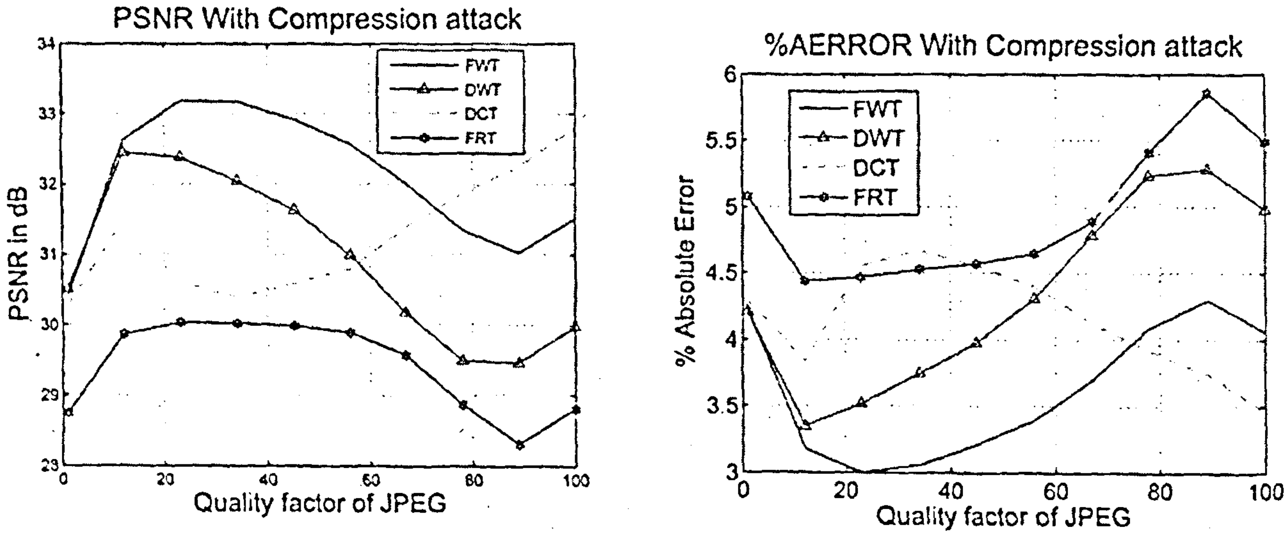


Fig 5 Comparison with compression attack for watermarked image

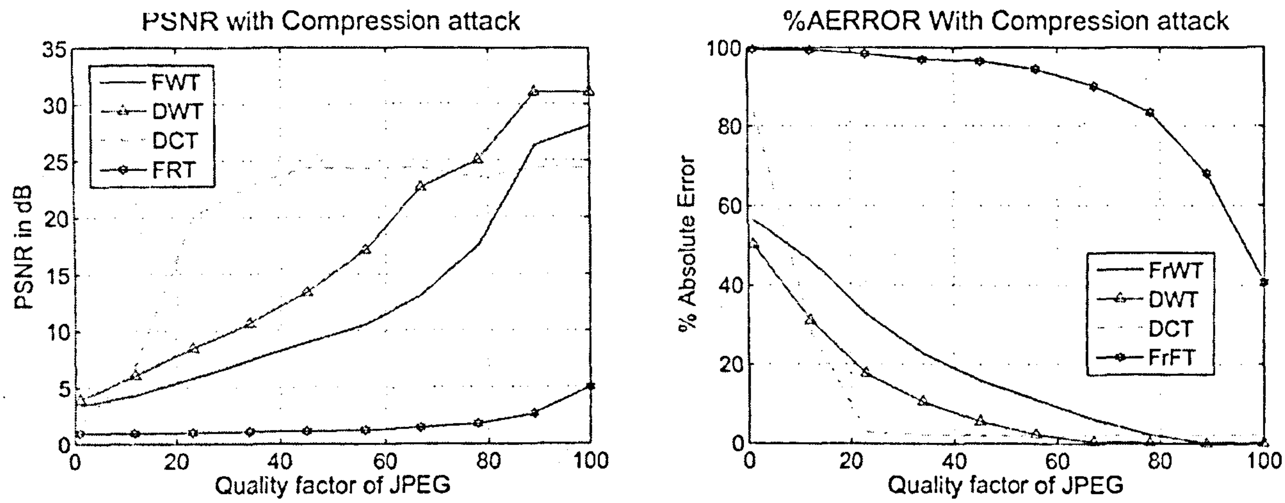
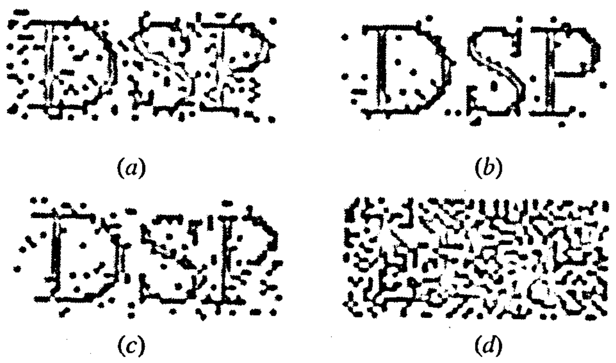


Fig 6 Comparison with compression attack for the recovered watermark


(*a*) (*b*)

(*c*) (*d*)

Fig 7 Extracted watermark after a noise attack (AWGN(N(0.0.1)), for watermarking schemes based on (*a*) FWT (*b*) DWT (*c*) DCT and (*d*) FRT

watermark is distorted, it is still recognizable, indicating that the scheme is fairly robust to the noise.

Thus from the simulated graphs and images, we can establish the following,

1. Our scheme uniformly shows a better PSNR and a smaller %AERROR for the watermarked image as compared to the other transform based schemes when subjected to compression attacks.
2. The recovered watermark's quality obtained using our scheme is comparable to that of other schemes despite introducing lesser distortion in the watermarked image. This indicates that our scheme is more suitable when invisible watermarking is required.
3. Although the noise attack leads to degradation in the recovered watermark's quality, it is still fairly recognizable, indicating the scheme's robustness towards the noise attacks.

## 6. CONCLUSION

The proposed scheme achieves better security due to the three level security structure provided by the use of dual transforms and a secret key. Also, the perceptibility of the watermark embedded using our scheme is less than the other transform based watermarking schemes. Although the quality of the recovered watermark image degrades considerably when subject to noise and compression attack, the recovered watermark images are still acceptable. Overall, the proposed watermarking scheme provides enhanced security, with a good watermarked image quality, and with improved robustness over other transform based watermarking schemes.

## REFERENCES

1. Chun-Shien Lu, Multimedia security: Steganography and digital watermarking techniques for protection of Intellectual Computer security, Multi-media systems-Security measures; Intellectual property, Hershey, Publishers: Idea Group Inc (IGI), Publication date: Jul 1, 2004, ISBN: 1591401925.
2. Maity Santi & Kundu Malay, A blind CDMA watermarking scheme in Wavelet Domain, International conference on Image processing, ICIP, pp 2633-2636, 2004.
3. Ingemar J Cox, Joe Kilian, Tom Leighton, & Talal Shamoon, Secure spread spectrum watermarking for images, audio and video, IEEE Transactions on Image Processing, vol 6, pp 1673-1687, Dec i997.
4. Xia-mu Niu, Sheng-he Sun, Digital Watermarking for Still Image Based on Discrete Fractional Fourier Transform, Journal of Harbin Institute of Technology, vol 8, no 3, pp 66-70, 2001.

5. Igor Djurovi, Srdjan Stankovi & Ioannis Pitas, Digital watermarking in the fractional Fourier transformation domain, Journal of Network and Computer Applications, pp 167-173, 2001.

6. Mallat S G, A Theory for Multiresolution Signal Decomposition: The Wavelet Representation, IEEE Transactions on Pattern analysis and Machine Intelligence, vol 11, no 7, pp 674-693, July 1989.

7. Ozaktas H M, Zalevsky Z & Kutay MA, The Fractional Fourier Transform, Series in Pure and Applied Optics, John Wiley and Sons, 2001.

8. Bultheel A & Martinez H, A shattered survey of the Fractional Fourier Transform, http://www.cs.kuleuven.ac.be/nalag/papers/ade/frft/frft.pdf

9. Ozaktas H, Arikan O, Kutay M & Bozdagi G, Digital Computation of the Fractional Fourier Transform, IEEE Transactions on Signal Processing, vol 4, no 9, pp 2141-2150, September 1996.

10. David Mendlovic, Zeev Zalevsky, David Mas, Javier Garca & Carlos Ferreira, Fractional wavelet transform, Applied Optics, vol 36, no 20, pp 4801-4806.

11. Linfei Chen & Daomu Zhao, Optical image encryption based on fractional wavelet transform, Optics Communications, 254 (2005), pp 361-367.

12. M Kutter & FAP Petitcolas, A fair benchmark for image watermarking system, Electronic Imaging '99,, Security and Watermarking of Multimedia Contents, vol 3657, Sans Jose, CA, USA.