Robust Invisible Watermarking Scheme Based on Random DFRFT

(IJCSNT) International Journal of Communication Systems and Network Technologies
ISSN Number: 2053-6283
Volume 12, Issue No. 1, 27–41

https://journals.mirlabs.in/index.php/ijcsnt
DOI-10.18486/ijcsnt/12.1.158
IJCSNT

Deepak Sharma[1]

Abstract

The copyright for content protection and authentication are the two main important criterion of any digital image watermarking. Any watermarking scheme are four major requirements of security, higher imperceptibility, robustness, and large capacity. Focussing on the requirements this paper presents a novel image watermarking scheme using random discrete fractional fourier transform (RDFRFT) with multiple parameter discrete fractional Fourier transform (MPDFRFT). The system uses the RDFRFT to convert original image into fractional fourier domain and embed the watermark image in the original image using MPDFRFT. The MPDFRFT is used to enhance security of the watermarked image by setting multiple parameters as a key. The multiple-parameter discrete fractional Fourier transform (MPDFRFT) is N order DFRFT parameters, where N refers to the number of the input data points. The MPDFRFT posses to have all of the desired properties for fractional transforms. The MPDFRFT reduces to the DFRFT when all of its order parameters are having the same value whereas RDFRFT is kernel matrix with random DFT eigenvectors and eigenvalues. The RDFRFT has key feature that the phase and magnitude of its transform output are both random so this feature has been utilized for enhancing the security. The proposed scheme is implemented by subdividing the cover image and RDFRFT is applied on each subdivided image to transformed coefficients then MPDFRFT is applied on watermark image with different parameters for enhancing the robustness. Similarly, during watermark extraction process the reverse order of MPDFRFT and inverse of RDFRFT is applied for reconstruction of original images and watermark image. The robustness of the watermark image is examined under various attacks such as rotation, additive noise, cropping and filtering operations. The analyzed and simulation results validates that the embedding scheme has good performance of major watermarking parameters robustness and perceptibility.

Keywords

Watermarking, Random Discrete Fractional Fourier Transform, Multiple Parameter Discrete Fractional Fourier Transform

Received: 10 December 2022; **Revised:** 16 April 2023; **Accepted:** 25 April 2023; **Published:** 30 April 2023;

[1]Department of Electronics and Communication, Jaypee University of Engineering and Technology, Noida, Uttar Pradesh, India.

Corresponding author:
Email: deepakforu23@rediffmail.com

Introduction

The rapid growth in emerging cyberspace technologies had raised the quality and quantity of multimedia content. This ample multimedia content require copyright protection, content authentication from different types of malicious activities like data alteration, piracy, legal issues and dissemination of data *etc*. To combat these illegal issues digital watermarking is a feasible solution to defend multimedia content from unauthorized access and tampering data from hostile. Digital watermarking is a an information hiding technique used to conceal proprietary information, copyright infringement issues and authorized certification of multimedia content.

Any watermarking system has two major requisites: imperceptibility and robustness. Imperceptibility is the basic requirement of the watermarking to hide the watermark in watermarked image and robustness is required to preserve the watermark originality against the various unintentional, intentional and geometric attacks. For higher security, the watermark should be invisible to the human eye to ensure that the hostile attackers cannot access the secured data todistort or alter it. In watermarking process system has to take care about the image quality after embedding the watermark and better quality signifies high watermark imperceptibility if the watermarking scheme is visible. The need of robustness is to protect the intellectual property rights of data owners against unauthorized copying, and redistributing it on the other networks. By increasing the capacity of the embedded watermark data leads to the system robustness but same time it also affects the media imperceptibility. Hence, a trade off always must be exists between the imperceptibility and the robustness in any watermarking scheme. Therefore, Currently the problem attracted researchers in the area of image watermarking application is to design and develop such type of novel algorithms those are capable to serve with sufficient resistance against various attacks along with sufficient level of imperceptibility.

According to the domains, watermarking can be classified as the spatial domain and the transformed domain watermarking. In spatial domain watermarking schemes, the watermark is embedded by directly modifying the pixel values of the image [1–3] and these schemes are less complex but are not robust against attacks due to their low-bit carrying capacity whereas, in the transform domain schemes, usually image is segmented into multiple frequency bands and have a capacity to embed more no. of bits of watermark inside it. These transforms domain watermarking schemes are such as the discrete cosine transform (DCT) [4–6], discrete wavelet transform (DWT) [7–9], Redundant Discrete Wavelet Transform (RDWT) [10], Finite Ridgelet Transform (FRIT) [11], singular value decomposition (SVD) [12–14], and fractional Fourier transform (FrFT) [15–18] are most commonly used transform used in watermarking schemes. Transform domain techniques are more renowed over spatial domain schemes due to an additional feature of robustness over the spatial domain watermarking scheme. Recently, few researchers have articulated fusion of transforms based watermarking schemes to improve the robustness and achieve high imperceptibility. These schemes are also called as hybrid watermarking schemes

In this paper, a novel image watermarking algorithm based on random discrete fractional Fourier transform and MPDFRFT has been proposed. In 2006 Pei [19] has given a newtype of generalized DFRFT with multiple parameter MPDFRFT derived from the eigen decomposition based DFRFT by taking the different fractional powers for different eigen values. The MPDFRFT has more versatility than the DFRFT because it has multiple order parameters. The MPDFRFT also follow all of the desired properties for fractional transforms. The multiple parameters of this MPDFRFT give a chance to enhance data security significantly, this extra order parameters of the MPDFRFT are used as an extra keys for security. Similarly, in 2009 Pei [20] derived RDFRFT from kernel matrix with random DFT eigenvectors and eigenvalues. RDFRFT has an unique feature that its magnitude and phase of its transformed output are both random in a nature. For the application in security these transforms may use in watermarking schemes to achieve higher security to make system more robust against attacks. This proposed novel watermarking scheme utilize both MPDFRFT and RDFRFT to enhance the security and produces the imperceptible watermarked image.

The organization of the paper is as follows. Following the introduction, the basic concept of fractional fourier transform along with RDFRFT and MPDFRFT are explained in section II. Section III discusses about the proposed watermarking scheme alsong with its algorithm. In section IV, experimental results has bee explained and compared. Finally, section V describes the concluding remarks.

BACKGROUND

In this section, the concepts of fractional Fourier transform, random discrete fractional Fourier transform and Multiple parameter discrete fractional Fourier transform, are briefly described.

2.1 Fractional Fourier Transform

The FRFT of the signal $x(t)$ can be given by with an angle α,

$$f_\alpha(u) = \int_{-\infty}^{+\infty} x(t)\, K_\alpha(t,u)\, dt \tag{1}$$

The signal $x(t)$ can be recovered back to its original domain by taking an FRFT with an angle $-\alpha$:

$$x(t) = \int_{-\infty}^{+\infty} f_\alpha(u)\, K_{-\alpha}(t,u)\, du \tag{2}$$

The FRFT transform kernel is given by [21,22]

$$K_\alpha(t,u) = \begin{cases} \sqrt{\dfrac{1-j\cot\alpha}{2\pi}}\; e^{\,j(t^2+u^2)/2\cot\alpha - jut\cos ec\,\alpha} & \text{if } \alpha \text{ is not a multiple of } \pi \\ \delta(t-u) & \text{if } \alpha \text{ is not a multiple of } 2\pi \\ \delta(t+u) & \text{if } \alpha+\pi \text{ is not a multiple of } 2\pi \end{cases} \tag{3}$$

Where $K_\alpha(t,u) = \sum_{n=0}^{\infty} e^{-j\alpha n} H_n(t) H_n(u)$ and $H_n(t) = \frac{1}{\sqrt{2^n n! \sqrt{\pi}}} h_n(t) e^{-t^2/2}$

Here the α indicates the rotation angle of the transformed signal in FRFT domain. $H_n(t)$ is the n-th order normalized Hermite Gaussian function. Where $h_n(t)$ is the n-th order Hermite polynomial.

The 2-D FRFT of the signal $x(s, t)$ by an angle parameter (α, β) can be given by [23],

$$f_{\alpha,\beta}(u,v) = \int_{-\infty}^{+\infty} x(s,t)\, K_{\alpha,\beta}(s,t,u,v)\, ds\, dt \tag{4}$$

The signal x(s, t) can be recoveredback in its original domain by taking its 2-D FRFT operation with an angles -α,-β given by:

$$x(s,t) = \int_{-\infty}^{+\infty} f_{\alpha,\beta}(u,v)\, K_{-\alpha,-\beta}(u,v,s,t)\, du\, dv \tag{5}$$

The 2-D FRFT transform kernel in two dimensions is defined as[23],

$$K_{\alpha,\beta}(s,t,u,v) = \frac{1}{2\pi}\sqrt{1-j\cot\alpha}\,\sqrt{1-j\cot\beta}\; e^{\left[j(s^2+u^2)/2\cot\alpha - jus\cos ec\,\alpha\right]} e^{\left[j(t^2+v^2)/2\cot\beta - jtv\cos ec\,\beta\right]} \tag{6}$$

The α and β indicate the rotation angles of the transformed signal for 2-D FRFT in fractional domain.

2.2 Multiple Parametr Discrete Fractional Fourier Transform

The MPDFRFT has been derived from the eigen decomposition based DFRFT by taking the different fractional powers for the different eigenvalues. The MPDFRFT has higher versatility than the DFRFT because it has *N* order parameters, where *N* indicates number of input data points.

The $p^{\text{-th}}$ order $N \times N$ DFRFT is derived using the eigen decomposition algorithm and its transform kernel is given on the basis of expression given below[24–26],

$$F^{2\alpha/\pi} = VD^{2\alpha/\pi}V^T \tag{7}$$

Where $\alpha = \pi p/2$ the DFRFT order of the parameter and α indicates the rotation angle of DFRFT. The Dickinson and Steiglitz[27] introduced a new commuting matrix ***S*** to compute the real eigenvectors of the DFT kernel matrix ***F***.

$$S = \begin{bmatrix} 2 & 1 & 0 & 0 & \cdots & 1 \\ 1 & 2Cos\,\omega & 1 & 0 & \cdots & 0 \\ 0 & 1 & 2Cos\,2\omega & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & 2Cos\,3\omega & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \cdots & 2Cos\,(N-1)\omega \end{bmatrix} \tag{8}$$

Where, $\omega = 2\pi/N$ and *N* indicates the size of the DFT kernel matrix. The matrix ***S*** commutes with matrix ***F***, The eigenvectors of matrix ***S*** are also the eigenvectors of matrix ***F***, but their eigen values are distinct values. The matrix ***S*** is a real symmetric matrix, the eigen values of ***S*** are all real and the eigenvectors of ***S*** are orthonormal to each other.

$V = [v_0\ v_1\ \ldots\ldots\ v_{N-2}\ v_{N-1}]$ For *N* is odd, $V = [v_0\ v_1\ \ldots\ldots\ v_{N-2}\ v_{N-1}]$ for *N* is even, and v_k is the *k*-th order DFT hermit eigen vector. $D^{2\alpha/\pi}$ is a diagonal matrix with eigen values of DFRFT in the diagonal entries. The methods used for finding the DFT Hermite eigenvectors v_k are given in[24] and[26].

Hence, The N DFT matrix F can be given by,

$$F_{kn} = \frac{1}{\sqrt{N}}\, e^{-j\frac{2\pi}{N}kn}, \qquad 0 \le k, n \le N-1 \tag{9}$$

The DFRFT kernels between even and odd length cases equation (1) can be written as follows:

$$F^{2\alpha/\pi} = \sum_{k=0}^{N-1} e^{-jk\alpha} v_k v_k^T \qquad \text{(For the odd values of } N\text{)} \tag{10}$$

$$F^{2\alpha/\pi} = \sum_{k=0}^{N-2} e^{-jk\alpha} v_k v_k^T + e^{-jN\alpha} v_N v_N^T \qquad \text{(For the even values of } N\text{)} \tag{11}$$

The DFRFT output is computed for even and odd values can be given by,

$$X_\alpha = \sum_{k=0}^{N-1} e^{-jk\alpha} v_k v_k^T x \qquad \text{(For the odd values of } N\text{)} \tag{12}$$

$$X_\alpha = \sum_{k=0}^{N-2} e^{-jk\alpha} v_k v_k^T x + e^{-jN\alpha} v_N v_N^T x \qquad \text{(For the even values of } N\text{)} \tag{13}$$

The generalization of the DFRFT on the basis of different fractional power for the eigen values $\lambda_k = \exp(-j\pi k/2)$ of the DFT matrix. The N point $N \times N$ MPDFRFT matrix can be formulated as,

$$F^{\overline{2\alpha/\pi}} = V \cdot diag\left(\left(e^{-j\frac{\pi}{2}0p_0}\right), \left(e^{-j\frac{\pi}{2}1p_1}\right) \ldots\ldots\ldots\ldots \left(e^{-j\frac{\pi}{2}(N-1)p_{N-1}}\right)\right) \cdot V^T \qquad \text{Odd values of } N \tag{14}$$

$$= V \cdot diag\left(\left(e^{-j\frac{\pi}{2}0p_0}\right), \left(e^{-j\frac{\pi}{2}1p_1}\right) \ldots\ldots \left(e^{-j\frac{\pi}{2}(N-2)p_{N-2}}\right) \left(e^{-j\frac{\pi}{2}(N)p_N}\right)\right) \cdot V^T \qquad \text{Even values of } N \tag{15}$$

When $diag(u_1, u_2, \ldots\ldots, u_n)$ represents the $N \times N$ diagonal matrix whose diagonal elements are$u_1, u_2, \ldots\ldots, u_n$. In equation (15), $\overline{p}$ is a $1 \times N$ parameter vector consisting of the N independent order parameters of the MPDFRFT,

$$\overline{p} = \begin{cases} (p_0, p_1, p_2, \ldots\ldots\ldots, p_{N-1}) & \text{for } N \text{ odd} \\ (p_0, p_1, p_2, \ldots\ldots\ldots, p_{N-2}, p_N) & \text{for } N \text{ even} \end{cases} \tag{16}$$

The diagonal matrix is simplified as

$$D^{\overline{2\alpha/\pi}} = \begin{cases} diag\left(\left(e^{-j\frac{\pi}{2}0p_0}\right), \left(e^{-j\frac{\pi}{2}1p_3}\right) \ldots\ldots\ldots\ldots \left(e^{-j\frac{\pi}{2}(N-1)p_{N-1}}\right)\right) \text{ for } N \text{ is odd} \\ diag\left(\left(e^{-j\frac{\pi}{2}0p_0}\right), \left(e^{-j\frac{\pi}{2}1p_2}\right) \ldots\ldots \left(e^{-j\frac{\pi}{2}(N-2)p_{N-2}}\right) \left(e^{-j\frac{\pi}{2}(N)p_N}\right)\right) \text{ For } N \text{ even} \end{cases} \tag{17}$$

The vector $\overline{a}$ is given in equation (16) and $D^{\overline{2\alpha/\pi}}$ is the $N \times N$ diagonal matrix of the DFT Eigen values

$$D^{2\alpha/\pi} = \begin{cases} diag\left(e^{-j\frac{\pi}{2}1}, e^{-j\frac{\pi}{2}3} \ldots\ldots\ldots\ldots e^{-j\frac{\pi}{2}(N-1)}\right) \text{ for } N \text{ is odd} \\ diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}2} \ldots\ldots\ldots\ldots e^{-j\frac{\pi}{2}(N-2)}, e^{-j\frac{\pi}{2}(N)}\right) \text{ For } N \text{ even} \end{cases} \tag{18}$$

Then equation (13) can be expressed in summarized form as,

$$F^{\overline{2\alpha/\pi}} = VD^{\overline{2\alpha/\pi}}V^T \tag{19}$$

The MPDFRFT of $X_{\overline{p}}$ of the$N \times 1$ data vector x with the parameter vector $\overline{p}$ can be given by,

$$X_p = F^{\overline{2\alpha/\pi}}x \tag{20}$$

2.3 Random Discrete Fractional Fourier Transform

A random discrete fractional Fourier transform (RDFRFT) is derived from the kernel matrix with random DFT eigenvectors and eigenvalues. The DFT is randomized by using the discrete random Fourier transform (DRFT) by taking the random powers for eigenvalues of the DFT matrix [28]. The eigenvectors received from the DRFT are not random because they are Hermite Gaussian type and are computed using the same method given by Pei [25]. Subsequently, the eigenvectors of the RDFRFT kernel matrix are random DFT eigenvectors because they are computed from eigenvectors of a random DFT-commuting matrix. The eigenvalues of the RDFRFT are taken as random fractional powers of the DFT eigenvalues so the transformed outputs of the RDFRFT israndom in both magnitude and phase.

To develop RDFRFT the $N \times N$ DFT matrix F can be given by,

$$F_{kn} = \frac{1}{\sqrt{N}} e^{-j\frac{2\pi}{N}kn}, \qquad 0 \le k, n \le N-1 \tag{21}$$

The eigen decomposition of the DFT commutating matrix F can be given as,

$$F_{\Phi}^{a} = \sum_{k=0}^{N-1} \gamma_k^{ak} \psi_k \psi_k^T \tag{22}$$

Here ψ_0, $\psi_1\psi_2$..... and ψ_{N-1} are orthonormal random eigen vector computed with the random DFT commutating matrix Φ. γ_k is the DFT eigen corresponding value of ψ_k and γ_k^{ak} has only 4 distinct eigen values based on Table-1.

Table 1. The eigen values assignment for DFRFT kernel

γ_k^{ak}	Random eigen Values
	$e^{-j2\pi a_k}$, if $\lambda_k = 1\ for\ k = 0, 1, 2 \ldots (4m-2), 4m$
	$e^{-j\pi a_k/2}$, if $\lambda_k = -j\ for\ k = 0, 1, 2 \ldots (4m-2), 4m$
	$e^{-j\pi a_k}$, if $\lambda_k = -1\ for\ k = 0, 1, 2 \ldots (4m-2), 4m$
	$e^{-j3\pi a_k/2}$, if $\lambda_k = je^{-jk\alpha}\ for\ k = 0, 1, 2 \ldots (4m-2), 4m$

The symmetric $N \times N$ DFT commutating matrix with a random generating matrix can be generated by following :

1. Formulate a $N \times N$ real random matrix Z whose $N \times N$ entries are independent and uniforly distribute in the interval [-4, 4].

2. Taking the K symmetric part $\exists$ of the random matrix Z so,

$$\exists = (Z + \mathrm{K}Z\mathrm{K})/2 \tag{23}$$

3. The random generating matrix G from the symmetric part of K, given as,

$$G = (\exists + \exists^{T})/2 \tag{24}$$

Here T indicates the transpose of matrix.

4. The random DFT commutating matrix Φ can be generated by,

$$\Phi = G + FGF^{-1} \tag{25}$$

Now with the random DFT commutating matrix Φ and MPDFRFT, the random DFRFT can be defined as,

$$F_{\Phi}^{a} = \sum_{k=0}^{N-1} \gamma_k^{ak} \psi_k \psi_k^{T} \tag{26}$$

PROPOSED SCHEME

In this segment, the proposed watermarking scheme described in detail with the help of block digram shown in figure-1along with embedding and extraction algorithm. The scheme process in three stages: where first stage is to apply RDFRFT on original image and in second stage 2D MPDFRFT is applied on watermark image to enhance security, the third stage watermark is added in cover image in fractional Fourier domain. The watermark embedding applied at the transmitter side invisible watermarked image is received. The watermark and original image is summed in fractional domain to binary domain.

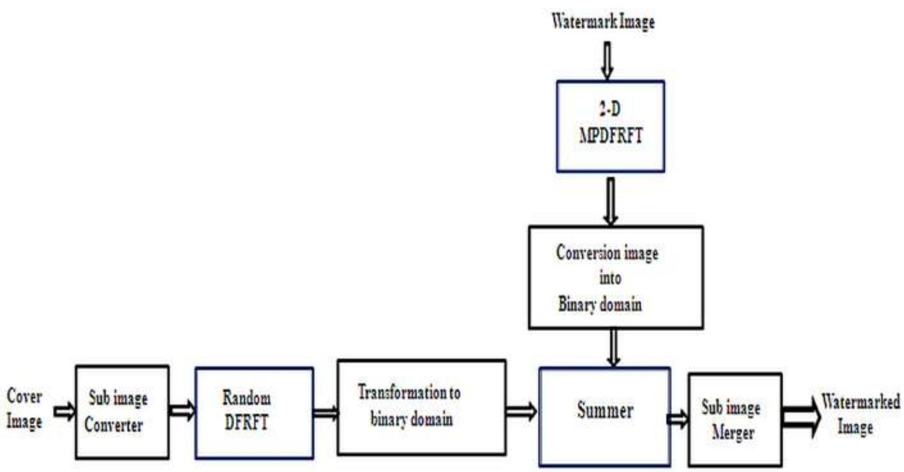


Figure 1. Proposed watermark embeddding model

The proposed watermark embedding algorithm is as follows:

Step-1: The original image of size 512×512 is divided into the sub image block size of 8×8.

Step-2: The 2-D random DFRFT is applied on each block by randomizing the eigen values and eigen vectors of the RDFRFT matrix which is random in both magnitude and phase.

Step-3: The watermark image of size 64×64 has been subdivided of size 8×8. On each block 2D-MPDFRFT is applied on watermark image with parameter vector *(r,s)* in the range of 0 to 4.

Step-4: The Selected 8 pixels form each transformed window randomly and then covert them into binary form. If the transformed value is negative, consider it as positive value and then convert it into binary form.

Step-5: The pixels of watermark in transform domain has been converted into the 8-bit binary form and this watermarks is embedded in the selected part of the 8 x 8 window of cover image in which the selected pixels for embedding,.

Step-6: The step 1 to 5 is repeated until all blocks of cover image are completed and watermark image is embedded all window of size 8×8.

Similarly to receive the original cover image from watermarked image watermark extraction process is applied at the receiver side. The watermark image is extracted from watermarked image along with original image. The watermark extraction process is implemented as shown in figure 2.

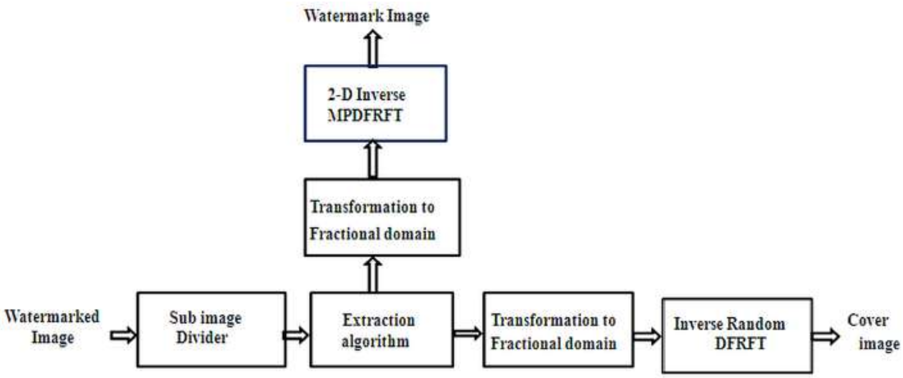


Figure 2. Proposed watermark extraction model

Proposed watermark extraction process is implemented as per following steps:

Step-1: The watermarked image is converted into the sub image size of 8 x 8 due to its highest correlation.

Step-2: Rearrange the same random pixels using circulry reversal matrix as randomized during the embedding process at transmitter side, from the each window.

Step-3: Convert those pixels into 8-bit binary form and extract the bit and filled with zero bits results there are fewer changes in it's the value in fractional domain.

Step-4: Perform 2D-MPDFRFT on each window with the same reverse parameter order with (*r, s*) chosen in the range from 0 to 4.

Step-5: Apply inverse of random DFRFT in a similar way as on each block by similarly randomizing the eigen values and eigen vectors of the RDFRFT matrix that was random using circularly reversal matrix.

Step-6: Place the positions extracted from the selected pixels and convert into its visual form to produce the pixels of original image.
Step-7: This process is repeated from steps 2 to 6 until all the pixels of watermark are produced.

Experimental Results and Comparison

In this segment, the testing of proposed scheme is carried out to verify the performance of the proposed model. The experiment is investigated on three set of test images comprises baboon, pepper and lena color images of size 512×512 are used as original images. The image of JUET logo size 64×64 is used as watermark image for embedding in original image. The proposed model based on RDFRFT-MPDFRFT based watermark scheme performance is evaluated and discussed based on performance parameter imperceptibility and robustness against different attacks. The imperceptibility of watermarked image refers that the human visual quality of the host image should not be affected much even after watermark embedding and not observable of watermark indicate higher imperceptibility. The quality of watermarked image is determined based on subjective and objective parameter and both the measure should be high. One of the objective criteria is peak signal-to-noise ratio (PSNR), which indicate thr imperceptibility degree whereas the subjective criteria can be easily determine by visually observing and comparing with original image. The other vital requirement for any watermarking system is the robustness. The robustness can be measured by evaluating the Normalized correlation coefficient (NCC).

$$\text{Peak Signal to Noise Ratio (PSNR)} = 10\log_{10}\left[\frac{MAX_I^2}{MSE_y + MSE_{cb} + MSE_{cr}}\right] dB$$

$$\text{Mean square Error (MSE)} = \frac{1}{R \times S}\sum_{i=1}^{R}\sum_{j=1}^{S}\left[W(i,j) - W'(i,j)\right]^2$$

Where $R{\times}S$ is the size of the original image. If the PSNR has value above 32dB indicates no significant difference between the extracted watermark image and original image.

The NCC is given as,

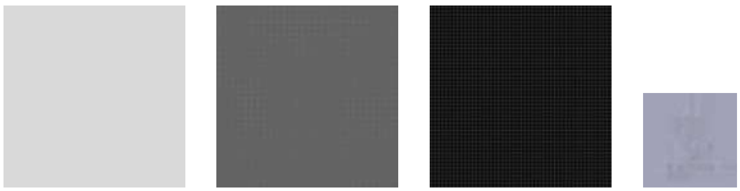
$$NCC = \frac{\sum_{i=1}^{R}\sum_{j=1}^{S} W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{R}\sum_{j=1}^{S}\left[W'(i,j)\right]^2}\sqrt{\sum_{i=1}^{R}\sum_{j=1}^{S}\left[W(i,j)\right]^2}}$$

Here W is the watermark image and W' is extracted watermark image. The normalized correlation coefficient lies between 0 to1. If NCC tends to unity received watermarked image is similar as extracted watermark image.

The figure 3 shows the original cover image of baboon, pepper and lena considered for experimental investigation purpose of having size 512×512. The watermark image which is to be embed is Juet logo of size 64×64. As per applied our proposed algorithm proposed model exhibit high imperceptibility shown in figure 4, for all test images with all test images and watermark can not be detected until you don't have correct order parameters. Baboon image (56.14dB), Pepper image (54.22dB) and Lena image (53.24dB) PSNR is received when extracted with correct order parameters as shown in figure 5. If the watermarked image is received just after watermark embedding the watermarked image can be received in invisible mode and can be used for secret transmission purpose as shown in figure 4 for all respectivewatermarked images.

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

Figure 3. Original cover image (a) Baboon (b) Pepper e (c) Lenna (f) Juet watermark



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

Figure 4. Watermarked Images (a) Baboon (b) Pepper (c) Lenna (d) Extracted Watermark Juet logo

(a) (b) (c) (d) Extracted watermark

Figure 5. Extracted images with correct order parameter (a) Baboon (b) Pepper (c) Lenna (f) Juet Watermark Image

This can be proven by extracting the watermark image and calculating the NC between the original watermark and the extracted watermark imagethe proposed scheme is robust. Moreover, when the watermarked image may be exposed to several attacks during transmission to make sure the robustness of the proposed scheme investigated to all test images.

The table 2 summarizes the robustness of the proposed scheme under various types of attacks for test images Aeroplane, frout, Baboon, Pepper and Lena. It summarizes the normalized correlation coefficient (NCC) with cover images.

Table 2. The NCC of watermarked image under various attacks

Types of Attacks	Images Parameter	Baboon	Pepper	Leena
Salt and pepper noise	Density 0.1	0.913	0.920	0.960
	Density 0.2	0.912	0.908	0.908
	Density 0.3	0.920	0.864	0.892
	Density 0.4	0.864	0.844	0.842
	Density 0.5	0.867	0.847	0.830
Speckle noise	Variance 0.1	0.920	0.936	0.921
	Variance 0.2	0.920	0.902	0.942
	Variance 0.3	0.828	0.869	0.910
	Variance 0.4	0.856	0.865	0.853
	Variance 0.5	0.850	0.835	0.862
Gaussian Noise	M=0 σ=0.1	0.922	0.975	0.970
	M=0 σ=0.2	0.960	0.94	0.940
	M=0 σ=0.3	0.92	0.930	0.922
	M=0 σ=0.5	0.910	0.899	0.910
JPEG Compression	Q =10	0.930	0.863	0.978
	Q =20	0.952	0.910	0.980
	Q =30	0.963	0.928	0.986
	Q =40	0.876	0.962	0.988
	Q =50	0.881	0.970	0.992
	Q =60	0.870	0.965	0.986
Rotation (angle in degree)	Clockwise 10^o	0.994	0.992	0.997
	Clockwise 20^o	0.993	0.989	0.992
	Clockwise 30^o	0.988	0.988	0.994
	Clockwise 90^o	0.984	0.982	0.997
	-90^o or 270^o	0.986	0.980	0.994
Cropping	5%	0.995	0.992	0.996
	10%	0.985	0.986	0.991
	15%	0.980	0.986	0.989
	20%	0.964	0.980	0.970
Scaling	Zoomin=2 Zoomout=0.5	0.967	0.900	0.972
	Zoomin=4 Zoomout=0.25	0.889	0.861	0.890
	Zoomin=0.25, Zoomout=4	0.822	0.824	0.890
	Zoomin=0.5, Zoomout=2	0.984	0.932	0.962
Joint Attack	Scaling & rotation	0.947	0.921	0.942
Median Filtering	For 3×3	0.980	0.989	0.956
	For 4×4	0.975	0.982	0.980
	For 5×5	0.968	0.972	0.971
Weiner Filtering	For 3×3	0.980	0.986	0.994
	For 4×4	0.984	0.979	0.990
	For 5×5	0.974	0.972	0.982
Gaussian filtering	For 3×3	0.990	0.982	0.992
	For 4×4	0.983	0.979	0.987
	For 5×5	0.972	0.971	0.980
Sharpning		0.968	0.976	0.991
Gamma correction attack	At 0.5	0.985	0.995	0.998
	At 0.6	0.992	0.991	0.996

Types of Attacks	Images Parameter	Baboon	Pepper	Leena
	At 0.7	0.991	0.990	0.992
Colour tone		0.985	0.982	0.980

The table 3 provides an information of proposed scheme in terms of perceptibility analysis along with their comparison over existing schemes and clearly depicts the superiority of proposed scheme over existing scheme.

Table 3. Comparative of proposed scheme with contemporary schemes based on imperceptibility (in dB)

Images	Lai et. al. [29]	Rastegar et. al. [30]	Lagzian et. al. [31]	Sun et. al. [33]	Lang et. al. [34]	Proposed
Lena	50.89	45.933	38.52	32.032	29.46	**53.24**
Pepper	——	45.954	——	——	——	**54.22**
Baboon	——	45.922	——	——	——	**56.14**

The results in table 4 are summarized for spicific best results for particular image from the set of test image and compare also their results alog with specific existing scheme as well.

Table 4. Comparison of proposed scheme over contemporary schemes under various attacks

Attacks	**Makbol et. al. [32]**	**Lai et.al. [29]**	**Rastegar et.al. [30]**	**Sun et. al. [33]**	**Lang et.al. [34]**	**Proposed**
Salt & pepper noise at 0.3 density	0.8926	—	0.8258	0.820	0.824	**0.920**
Speckle noise at 0.01	0.952	—	0.9667	—	—	0.936
Gaussian noise $M = 0, \sigma = 0.4$	0.8835	—	0.82	0.790	—	**0.923**
Rotation 2°	0.981	—	0.9628	—	—	**0.996**
Rotation -30°	0.9823	0.9780	—	—	—	**0.994@** -90°
Cropping at 20%	**0.989**	—	—	—	—	0.980
Joint attack scaling & rotation	—	—	—	—	—	**0.984**
Gaussian filtering for 3×3	0.987	—	0.9843	—	—	**0.990**
Median filtering for 3×3	**0.982**	0.9597	0.9746	—	—	0.980
Wiener filtering for 3×3	0.984	—	0.9569	—	—	**0.993**
Gamma correction at 0.7	0.9935	**0.9982**	—	—	—	0.994
Colour tone	—	—	—	—	—	**0.985**
Sharpening	—	—	—	—	—	**0.991**

CONCLUSION

In this paper, we presented a RDFRFT-MPDFRFT based invisible watermarking technique for authentication, which is highly robust against several common signal processing attacks. The proposed scheme tested under the different attacks includes geometric, intentional and unintentional, filtering, image processing attacks and different noise perturbation for salt pepper, speckle and Gaussian noise at different concentration level, scaling, gamma correction, cropping at different level, JPEG compression, rotation at different angles, joint attack includes both cropping and rotation simultaneously, filtering operations like median, gaussian and weiner filtering operations. The experimental results demonstrates that the proposed scheme preserves high image imperceptibility and robustness. The imperceptibility of lena image is 2.35dB, pepper image 8.266 dB and baboon image 10.218 dB better over the Lai et al.[29] and Rastegar et. al.[30]. The robustness of proposed schems is much superior over the existing scheme as shown in terms of normalized correlation coefficient parameter. The proposed scheme shows inferior response for JPEG compression, cropping and gamma correction for certain levels. This higher imperceptibility and robustness feature of the proposed scheme it more efficient for watermarking video processing applications.

References

[1] R. Ni, Q. Ruan, Y. Zhao, Pinpoint authentication watermarking based on a chaotic system, Forensic Science International 179, 54–62, 2008.

[2] C. Deng, X. Gao, X. Li, D. Tao, Local histogram based geometric invariant image watermarking, Signal Processing 90, 3256–3264, 2010.

[3] O. Findik, I. Babaoglu, E. Ulker, A color image watermarking scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm, Optics Communications 283, 4916–4922, 2010.

[4] F. Huang, Z.H. Guan, A hybrid SVD-DCT watermarking method based on LPSNR, Pattern Recognition Letters 25, 1769–1775, 2004.

[5] J.C. Patra, J.E. Phua, C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing 20, 1597–1611, 2010.

[6] S.D. Lin, S.C. Shie, J.Y. Guo, Improving the robustness of DCT-based image watermarking against JPEG compression, Computer Stan- dards & Interfaces 32, 54–60, 2010.

[7] D. Kundur, D. Hatzinakos, Towards robust logo watermarking using multiresolution image fusion, IEEE Transactions on Multimedia 6, 185–197, 2004.

[8] W.H. Lin, Y.R. Wang, S.J. Horng, A wavelet-tree-based watermarking method using distance vector of binary cluster, Expert Systems with Applications 36, 9869–9878, 2009.

[9] H.M. Al-Otum, N.A. Samara, A robust blind color image watermarking based on wavelet tree bit host difference selection, Signal Processing 90, 2498–2512, 2010.

[10] Lagzian S, Soryani M, Fathy M. A new robust watermarking scheme based on RDWT–SVD. IJIIP Int J Intell Inform Process, 2(1): 22–9, 2011.

[11] Campisi P, Kundur D, Neri A. Robust digital watermarking in the ridgele domain. IEEE Signal Process Lett;11(10):826–30, 2004.

[12] E. Ganic, A.M. Eskicioglu, Robust embedding of visual watermarks using DWT-SVD, Journal of Electronic Imaging 14 (4) 043004, 2005.

[13] A.A. Mohammad, A. Alhaj, S. Shaltaf, An improved SVD-based watermarking scheme for protecting rightful ownership, Signal Processing 88, 2158–2180, 2008.

[14] C.C. Lai, An improved SVD-based watermarking scheme using human visual characteristics, Optics Communications 284, 938–944, 2011.

[15] N.K. Nishchal, Optical image watermarking using fractional Fourier transform, Journal of Optics 38 (1), 22–28, 2009.

[16] D. Cui, Dual digital watermarking algorithm for image based on fractional Fourier transform, in: Proceedings of Second Pacific–Asia Conference on Web Mining and Web Based Applications, Wuhan, pp. 51–54, 2009.

[17] M.A. Savelonas, S. Chountasis, Noise-resistant watermarking in the fractional Fourier domain utilizing moment-based image representation, Signal Processing 90, 2521–2528, 2010.

[18] D. Sharma, R. Saxena and N. Singh, "Robust watermarking against geometric attacks using Multiple parameter discrete fractional fourier transform and least significant bit", International journal of security and its applications, vol. 8, no.5, pp. 439-456, 2014

[19] S. C. Pei and W. L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Process. Lette.*, vol. 13, no. 6, pp. 329–332, Jun. 2006.

[20] S. C. Pei and W. L. Hsue, "The random discrete fractional Fourier transform," *IEEE Signal Process. Lette.*, vol. 16, no. 12, pp. 1015–1018, 2009.

[21] V. Namias, "The fractional order Fourier transform and its application to quantum mechanics", IMA Journal of Applied Mathematics, vol. 25, no. 3, pp. 241–265,1980

[22] L. B. Almeida, "The fractional Fourier transform and time-frequency representations", IEEE Trans. Signal Process., vol. 42, no. 11, pp. 3084–3091, 1994.

[23] A. Sahlin, H. M. Ozaktas and D. Mendlovic, "Optical implementation of the two-dimensional fractional Fourier transform with different orders in the two dimensions" Elsevier Optics Communication, vol. 120, issue 3-4, pp. 134-138,1995

[24] C. Candan, M. A. Kutay and H. M. Ozaktas, "The discrete fractional Fourier transform", IEEE Trans. on Signal Process., vol. 48, no. 5, pp. 1329–1337, 2000.

[25] S. C. Pei and M. H. Yeh, "Improved discrete fractional Fourier transform," Opt. Lett., vol. 22, no. 14, pp. 1047–1049,1997

[26] S. C. Pei, M. H. Yeh, and C. C. Tseng, "Discrete fractional Fourier transform based on orthogonal projections," IEEE Trans. Signal Processing, vol. 47, pp. 1335–1348, May 1999

[27] B. W. Dickinson and K. Steiglitz, "Eigenvalues and eigenvectors of the discrete Fourier transform", IEEE Trans. Acoust. Speech Signal Process., vol. 30, no. 1, (1982), pp. 25–31.

[28] Z. Liu and S. Liu, "Randomization of the Fourier transform," *Opt. Lett.*, vol. 32, pp. 478–480, 2007.

[29] Lai CC, Tsai CC. Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11), 3060–3, 2010.

[30] Rastegar S, Namazi F, Yaghmaie K, Aliabadian A. Hybrid watermarking algorithm based on singular value decomposition and radon transform. Int J Electron Commun (AEU), 65(7):658–63, 2011.

[31] Lagzian S, Soryani M, Fathy M. Robust watermarking scheme based on RDWT–SVD: embedding data in all subbands. In: International symposium on artificial intelligence and signal processing (AISP). pp. 48–52, 2011

[32] Nasrin M. Makbol, Bee Ee Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition" Int. J. Electron. Commun. (AEÜ) 67, pp.102–112, 2013

[33] Jin-ying Sun, JunLang, Chengqiang Miao, Nan Yang, Shenquan Wang, "A Digital Watermarking Algorithm based on Hyperchaos and Discrete Fractional Fourier Transform", 5th International Congress on Image and Signal Processing (CISP 2012), pp. 553-556, 2012

[34] Jun Lang, Jin-ying Sun,Wen-fang Yang, "A Digital Watermarking Algorithm Based on Discrete Fractional Fourier Transformation", International Conference on Computer Science and Service System pp. 692-694, 2012