

Research Article

A Fractional Random Wavelet Transform Based Image Steganography

¹G.K. Rajini and ²G. Ramachandra Reddy (SMIEEE)

¹School of Electrical Engineering, VIT University, Vellore, Tamilnadu,

²Department of ECE, S.V. University, Tirupati Andhra Pradesh, India

Abstract: This study presents a novel technique for image steganography based on Fractional Random Wavelet Transform. This transform has all the features of wavelet transform with randomness and fractional order built into it. The randomness and fractional order in the algorithm brings in robustness and additional layers of security to steganography. The stegano image generated by this algorithm contains both cover image and hidden image and image degradation is not observed in it. The steganography strives for security and payload capacity. The performance measures like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity Index Measure (SSIM) and Universal Image Quality Index (UIQI) are computed. In this proposed algorithm, imperceptibility and robustness are verified and it can sustain geometric transformations like rotation, scaling and translation and is compared with some of the existing algorithms. The numerical results show the effectiveness of the proposed algorithm.

Keywords: DWT, fractional random wavelet transform, image steganography, MSE, network attacks, PSNR, SSIM, security, UIQI

INTRODUCTION

The essence of image steganography lies in concealing secret image in such a way that none apart from the sender and intended recipient can realize the presence of hidden information. Steganography is an art of embedding secret image into another image called cover image and the resultant image obtained is the Stegano image. The growing possibilities of modern communication of digital files need the special means of security especially on computer network. The network security is becoming more important as the number of data files being exchanged on the Internet increases. Therefore, the confidentiality and data integrity requires protection against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding and information security. The information security implies protecting information systems from unauthorized access, use, disclosure, disruption, modification, destruction, inspection and recording. The steganographic techniques have erupted in both spatial and transform domains in both complexity and usage. These techniques predominantly keep secrets safe and secure. Randomness plays an important role in preserving the information which becomes unintelligible to unauthorized user and it is evident that due to randomness, only the authorized person can retrieve information.

In this study, we describe a new method of steganography based on Fractional Random Wavelet

Transform (FrRnWT), a family of wavelet transform that inherits excellent mathematical properties of Wavelet Transform (WT), Fractional Random Transform (FrRnT). It describes the information in spatial and frequency domain with randomness, due to rotation of time frequency plane. The features of FrRnWT are exploited for hiding technique in Image Steganography. The modern secure image steganography presents a challenging task of transferring the embedded image to the destination without being detected in an insecure channel. Animations were used as cover object to transfer information and its robustness justified when applied to digital image steganography (Tadiparthi and Sueyoshi, 2006).

The transform domain method of image steganography embeds the image into cover image in the frequency bands of cover image which makes them more robust for attacks and are suitable for confidential information exchange. In this technique, the secret image is hidden in the low frequency (LL) subband coefficients of FrRnWT of cover image. After applying IFRnWT, the stegano image is obtained at the receiving end. Extraction process is performed to retrieve the hidden image from the stegano image.

The objective is to exploit the fascinating feature of FrRnWT, the various parameters like embedding coefficient, fractional order of this transform, the random matrix that is generated possesses independent elements and for an anonymous intruder it is very difficult to predict the very existence of the hidden

image in the cover image. It is highly impossible to frame the random matrix and to predict the fractional order thus providing high network security.

FRACTIONAL RANDOM WAVELET TRANSFORM (FrRnWT)

This study focuses on the development of FrRnWT and is described with the following discussion. The first and foremost transform developed for signal representation in transform domain is Fourier Transform (FT). It converts a signal from time versus amplitude to frequency versus amplitude and does not provide the instant of occurrence of the frequency component. To eliminate the drawbacks of FT, Short Time Fourier Transform (STFT) was introduced in which moving window is applied and then FT is applied to the signal within the window as the window is moved over a whole real line (Mallat, 1989). The performance of the STFT is limited by the length and type of window. It does not provide good results for signals having low frequencies of longer duration and high frequencies of shorter duration. Later Wavelet Transform (WT) was developed which possesses both time and frequency domain information and has multiresolution features, but suffers from poor directional selectivity (Kingsbury, 2001).

Recently researchers came out with a new mathematical transform called Fractional Fourier Transform (FrFT) that can be viewed as the rotation through an angle of FT and it is a kind of time-frequency joint representation of the signal in fractional domain (Liu *et al.*, 2008). Later Discrete Fractional Fourier Transform was presented by (Candan *et al.*, 2000) which satisfies the essential properties of continuous Fractional Fourier Transform. Moreover researchers have attempted to give randomness to the FrFT and named it as Fractional Random Transform (FrRnT) (Namais, 1980). The randomness is included by selecting a random transform kernel with similar properties as FrFT kernel and this transform serves as a numerical tool for signal and image processing. An interesting mathematical transform called FrRnWT has emerged which combines both excellent properties of FrRnT and WT and is used as a tool for image biometric encryption and decryption (Bhatnagar *et al.*, 2012). FrRnWT gives uniform randomness while maintaining the low frequency components and this ability proves superior to both DWT and FrWT in the sense that for every different fractional order it will produce different uniform randomness in the detail coefficients.

MATHEMATICAL DEVELOPMENTS OF FrRnWT

Due to the seperability of the transform, two dimensional FrRnWT can be obtained taking the one-dimensional transforms along both axes:

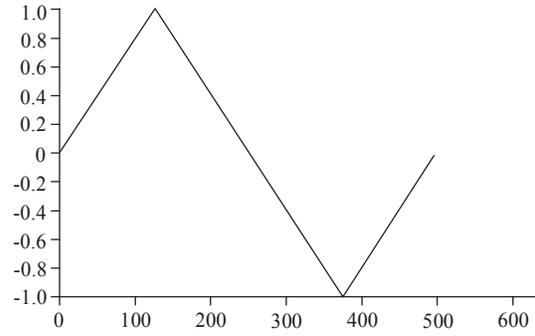


Fig. 1: Triangular waveform

$$W_{\alpha_x, \alpha_y}(u, v, a_1, b_1, a_2, b_2) = FrRnWT_{\alpha_y}^{t_y \rightarrow v} \times \{FrRnWT_{\alpha_x}^{t_x \rightarrow u}\{f(t_x, t_y)\}\} \quad (1)$$

where, a_1, a_2 and b_1, b_2 are scaling and translation parameters along x and y directions, respectively. The 2D-DWT of DFrRnT values $X(n_1, n_2)$ is then:

$$W_\varphi(j_0, k_1, k_2) = \frac{1}{\sqrt{MN}} \sum_{n_1=0}^{M-1} \sum_{n_2=0}^{N-1} X(n_1, n_2) \varphi_{j_0, k_1, k_2}(n_1, n_2) \quad (2)$$

$$W_\psi^i(j_0, k_1, k_2) = \frac{1}{\sqrt{MN}} \sum_{n_1=0}^{M-1} \sum_{n_2=0}^{N-1} X(n_1, n_2) \psi_{j, k_1, k_2}^i(n_1, n_2) \quad (3)$$

where, $i = \{H, V, D\}$, j_0 represents arbitrary scale and k_1, k_2 are translation parameters. Eq. (2) represent approximation coefficients at scale j_0 and Eq. (3) represents detail coefficients at scale $j \geq j_0$ of $X(n_1, n_2)$. Thus the obtained 2D-FrRnWT has all the properties of DWT and FrRnT incorporated in it.

The Inverse Wavelet Transform (IWT) can be obtained by the following expression:

$$X(n_1, n_2) = \frac{1}{\sqrt{MN}} \sum_{k_1} \sum_{k_2} W_\varphi(j_0, k_1, k_2) \varphi_{j_0, k_1, k_2}(n_1, n_2) + \frac{1}{\sqrt{MN}} \sum_{i=H, V, D} \sum_{j=j_0}^{\infty} \sum_{k_1} \sum_{k_2} W_\psi^i(j, k_1, k_2) \psi_{j, k_1, k_2}^i(n_1, n_2) \quad (4)$$

By the application of IFRnT to $X(n_1, n_2)$, the images can be extracted.

Fractional random wavelet transform for 1D signal:

Figure 1 represents the 1D triangular waveform. Figure 2 depicts the comparison of DWT and FrRnWT for a triangular signal. In this simulation analysis, we have considered the five-level of decomposition with 0.25 as fractional transform order for FrRnWT. In DWT, the approximate part is the subsampled version and detail parts provide the variations in signal values

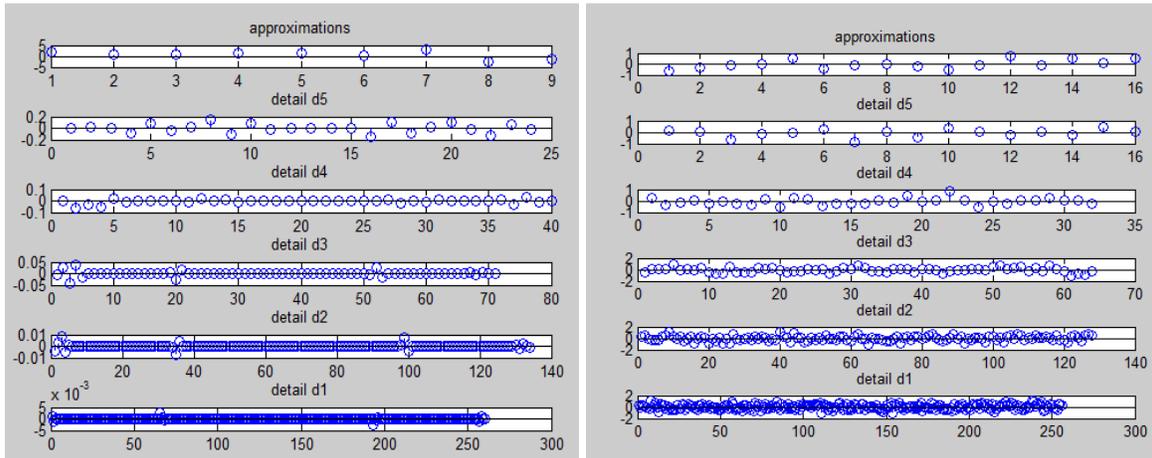


Fig. 2: (a): WT decomposition; (b): FrRnWT decomposition with $\tau = 0.25$



(a): Original image (b): One-level WT (c): One-level FrRnWT (d): Three-level WT (e): Three-level FrRnWT

Fig. 3: Visual assessment of WT and FrRnWT

in subsequent samples which describes the derivatives of the signal. The peaks or extremas of the signal produce zero derivatives and detail part is zero at these instances. The FrRnWT gives uniform randomness to each level and maintains the structure of the low frequency components. This feature of FrRnWT proves its superiority over DWT.

Fractional random wavelet transform for 2D signal: Figure 3 gives the visual assessment and comparison of WT with FrRnWT for the original image of size 512×512 . DWT of an image which possess multiresolution property while FrRnWT has a unique property of describing the information in spatial and frequency domain with randomness. Due to its rotation of time-fractional-frequency plane over an arbitrary angle, FrRnWT provides uniform randomness while maintaining the low frequency components of an image and this was exploited in image encryption and decryption (Bhatnagar *et al.*, 2012). Here we bring another exciting application of FrRnWT which is image steganography

The Fig. 3a shows the cover image, Fig. 3b gives the single level wavelet decomposition which gives us the multiresolution feature of an image; Fig. 3c clearly predicts the decomposition of a single level FrRnWT of an image which facilitates for image secrecy and network security. The LL component comprises of size 256×256 suitable for embedding secret image of size 256×256 to hide. Fig. 3d shows the three level

decomposition of the DWT and Fig. 3e shows decomposition of three levels FrRnWT where secret image of size 64×64 can be embedded.

IMPLEMENTATION OF FrRnWT APPROACH TO IMAGE STEGANOGRAPHY

A typical colour image is represented by the triplets: Green plane, Red plane and Blue plane. The proposed image steganography embeds the image to be hidden in the first level low frequency subband of the FrRnWT of cover image's blue plane. It is observed that Blue plane provides better results and coincides with specification and requirements of International Telecommunication Union (ITU), 1992. After applying IFRnWT, the resultant stegano image carrying hidden image is obtained and it does not produce artifacts related to the existence of the secret image. The cover and secret image are obtained after implementing the extraction process. The most successful applications of image steganography is greatly dependent on finding a suitable method for embedding the secret image and the creation of stegano image. Ranking the performance of a specific algorithm is of paramount importance for the success of the embedding process. The primary goal of steganography is to design embedding function that is statistically undetectable and capable of communicating practical (i.e., large) payloads. The Figure 4 formulates the developed algorithm by means of a flow chart.

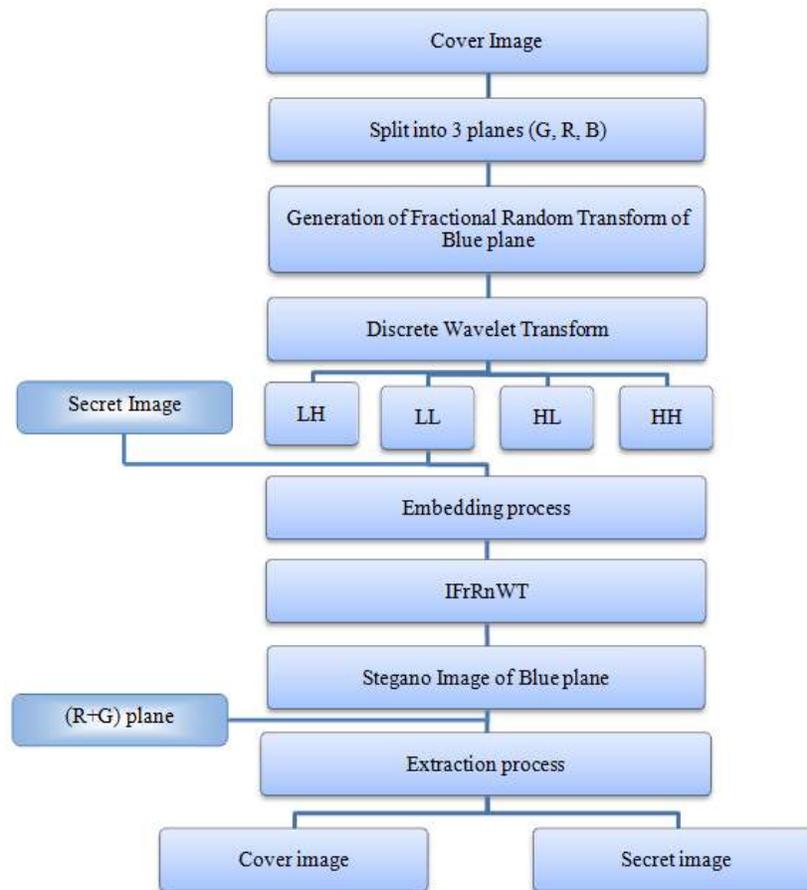


Fig. 4: Flowchart of the proposed algorithm

The algorithmic steps of the flowchart are as follows:

Input: Cover color image of size 512×512 and random matrix, of size 512×512 , secret gray scale image of size 256×256 , fractional order value and embedding coefficient.

Output before extraction: Stegano image, a color image of size 512×512 .

Output after extraction: Cover image of size 512×512 and extracted secret image of size 256×256 .

Embedding process:

- Split the colour cover image into three colour planes viz., Red, Green, Blue.
- Compute the FrRnT by operating it on the blue plane of the cover image.
- Decompose the output of the FrRnT into wavelet subbands viz., LL, LH, HL, HH.
- Divide the secret image and LL subband of FrRnWT into non overlapping blocks of equal size.
- Embed the secret image into LL subband of FrRnWT using the expression (5):

$$(1 - \rho) * \beta_1 + (\rho * \beta_2) \tag{5}$$

The blocks of LL subband of FrRnWT of cover image are represented by β_1 . The blocks of secret image are represented by β_2 and ρ represent the embedding coefficient. Thus the secret image is embedded in the cover image.

- Compute IFrRnWT and stegano image pertaining to the blue plane is obtained.
- Insert Red and Green plane details to the intermediate stegano image.

Extraction process:

- Compute FrRnWT to the stegano image. Perform extraction process at the receiving end using (6):

$$(\gamma_1 - ((1 - \rho) * \gamma_2)) / \rho \tag{6}$$

The blocks of LL band of stegano image, secret image and embedding coefficient are represented by γ_1, γ_2 and ρ respectively.

- Retrieve the hidden image from stegano image.
- Compute the PSNR and MSE for the stegano and secret image.

RESULTS ANALYSIS

To evaluate the performance of the proposed algorithm, the pepper image of size 512×512 is considered as the cover image and cameraman image of size 256×256 is considered as secret image as in Fig. 5a and b, respectively.

The one-level FrRnWT is performed for blue plane of cover image and is shown in Fig. 5c. LL band is chosen for embedding, as most of the energy is concentrated in it. The LL band of FrRnWT is shown in Fig. 5d. The secret image and LL band of DWT decomposition are divided into non overlapping blocks. The divided secret image is embedded into the LL band of FrRnWT's cover image using the expression (5) and subsequently IFrRnWT is applied. The resultant stegano image obtained comprises of both secret image and the cover image and is shown in Fig 6a. The secret

image cannot be visualized by the vendors which is the unique feature of the proposed algorithm. The imperceptibility and network security of the stegano image is high and the artifacts are not observed.

To retrieve the secret image from the stegano image, the extraction process is performed and faithful reconstruction with acceptable visual quality is obtained as shown in Fig. 6b. The stegano images were obtained with both fractional and integer order, to ascertain the role of fractional order in image steganography. When the integer order is used, the stegano image looks blurred and leads to suspicion that some hidden information is present whereas when fractional order is used, the stegano image is identical to the cover image. The performance measures are evaluated in the next section to realize the superiority of fractional order as depicted visually in Fig. 7.

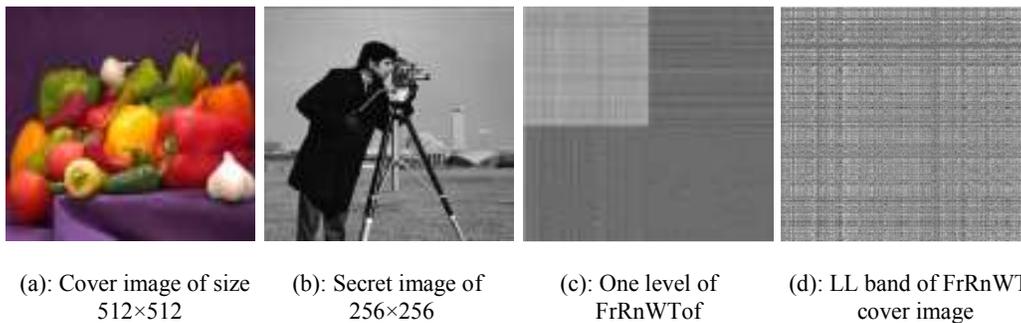


Fig. 5: Numerical Simulations of 2D-FrRnWT with cover and secret image

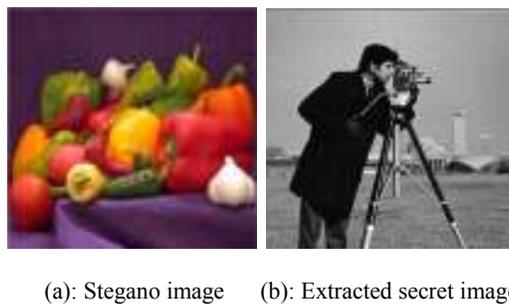


Fig. 6: Numerical results of FrRnWT after extraction process

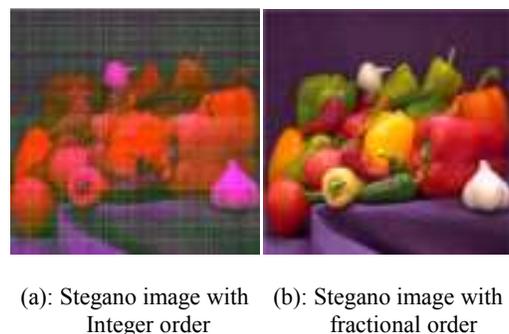


Fig. 7: Numerical results of stegano image

Table 1: Performance measures of stegano image and extracted secret image

Type of order	Stegano image			Extracted secret image		
	PSNR	MSE	SSIM	PSNR	MSE	UIQI
Fractional	40.6691	5.5741	0.9989	278.9459	8.2887e-024	1.000
Integer	11.1594	4.9790e+003	0.8666	18.8252	4.9614e+006	4.2819e-005

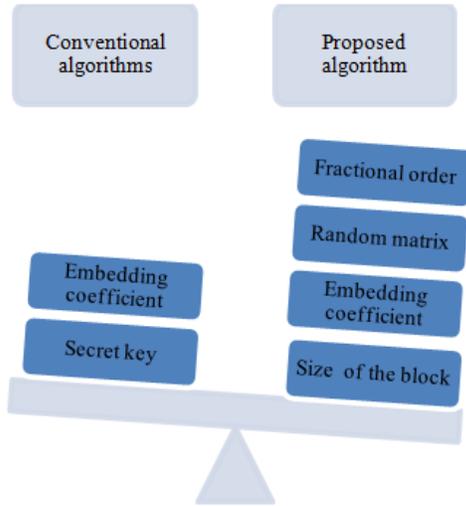


Fig. 8: Comparison of security layers of the proposed algorithm

Figure 8 depicts the comparison of conventional algorithms and proposed algorithm and it is evident that the proposed algorithm outperforms conventional algorithm with respect to security issues. Additional layers of security are provided with following parameters namely the fractional order value, the embedding coefficient, the random kernel matrix Q that possess $N(N + 1)/2$ independent elements. The number of steps needed to search the random matrix is $2^{N(N+1)/2}$ which a tedious process. In addition to this block size of an image used for embedding can also not be predicted and can be considered as the another layer of security.

Performance measures: The performance of the proposed technique is evaluated with widely used quality metrics like PSNR, MSE, SSIM and UIQI (Wang and Li, 2002; Wang and Bovik, 2011).

Performance comparison of Fractional and Integer order: The performance measures of the proposed work are evaluated and are shown in Table 1. It is clearly evident that fractional order based steganography outperforms integer order.

Comparisons of different frequency bands: The secret image is embedded in LL subband of FrRnWT domain and it is justified that the other subbands possess less magnitude coefficients and do not produce good results. The performance measures of stegano image for different subbands are tabulated in the following Table 2.

Table 2: Performance measures for stegano image indifferent frequency bands

Type of frequency band	PSNR	MSE	SSIM
LL Band	44.513	4.5837	0.9989
LH Band	7.5089	1.154 ⁴	0.8589
HL Band	7.0558	1.2089 ⁴	0.8654
HH Band	6.6399	1.3462 ⁴	0.7854

Table 3: PSNR and MSE for DWT and FrRnWT

Decomposition levels	PSNR	MSE	Security
1- level DWT	40.66	5.57	Moderate
2- level DWT	40.27	6.13	
3- level DWT	39.87	6.69	
1- level FrRnWT	44.43	2.33	High
2-level FrRnWT	43.55	2.92	
3- level FrRnWT	42.66	3.51	

Comparison with DWT: Image Steganography with FrRnWT domain looks very promising. Searching such a random matrix coded with uniformly distributed random numbers is highly impossible. Similarly identifying the existence of the secret image in the stegano image is not feasible without the knowledge of embedding coefficient and Fractional order value.

The drawbacks of DWT with respect to PSNR, MSE, superiority and efficiency of FrRnWT for varying levels of decompositions are summarized in Table 3. The impact of the embedding coefficient (ρ) on PSNR and MSE for the stegano image and secret image are depicted in Fig. 9a and b. With low ρ value PSNR increases and MSE decreases for the stegano image and it is the vice versa for the secret image.

To analyze the efficiency of the proposed algorithm, it is tested on wide range of images and is found to be insensitive to various image formats. We implemented the proposed scheme with MATLAB (2009a) and tested its effectiveness with quality metrics PSNR and MSE using many image formats and colour planes and it is tabulated in Table 4. Detecting an embedded message defeats the primary goal of steganography, that of concealing the existence of a hidden message. The subjective tests are carried out by people who look for visual differences between the images (original and stegano image) trying to find which one of them is the original. The percentage of success is 80% and it can be concluded that the message is invisible. These subjective test's rules and recommendations are defined by the ITU.

Security attacks: The embedded data has to remain intact even if the stegano image undergoes transformation due to intentional or unintentional stegano attacks. Robustness refers to the ability of detecting the stegano image even after common signal processing operations (Cheddad *et al.*, 2010). Examples of intentional attacks on images include histogram

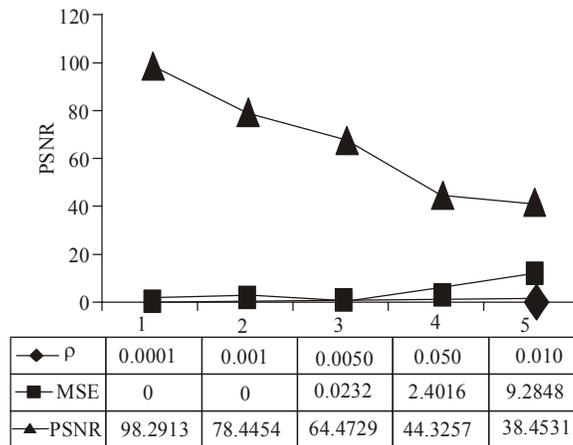


Fig. 9: (a) Stegano image

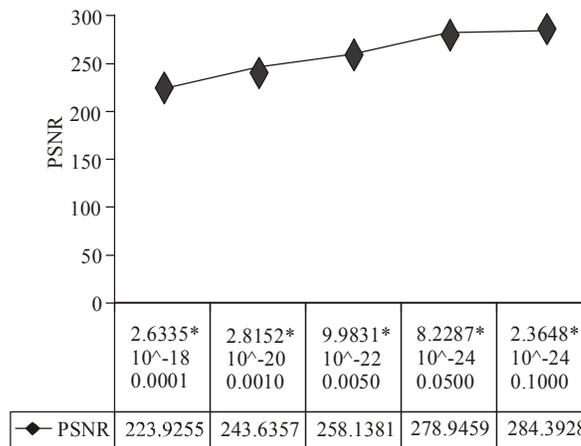


Fig. 9: (b) Secret image

Table 4: Comparison of PSNR and MSE for different test images and different channels

		$\rho = 0.05 \& \tau = 0.5$					
		Channel I Red		Channel II Green		Channel III Blue	
Cover image	Secret image	PSNR	MSE	PSNR	MSE	PSNR	MSE
Peppers.jpg	Cameraman.tif	36.08	16.03	41.51	4.58	42.43	3.71
Lena.png	House.tif	36.37	14.57	43.47	2.92	44.67	2.21
PCB board.jpg	X-ray.jpg	35.62	17.80	33.44	29.43	35.63	17.74
Logo.png	Rose.jpg	35.57	18.02	36.00	16.30	36.43	14.78
Krishna.jpg	Fingerprint.bmp	34.78	19.98	36.06	12.76	37.09	13.44

attacks, spatial filtering, lossy compression and geometric distortions like rotation, translation, scaling which deliberately modify the content and those of unintentional attacks include noise in channel.

Figure 10 clearly reveals that the embedded image does not impair the image quality. The simplest often unreliable, method of analyzing an image for possible embedded data is by analyzing the image visually and looking for anomalies or artifacts after embedding. Many steganography methods, including LSB-and DCT-based methods, leave noticeable distortions in smooth or homogeneous areas of an image. From a visual perspective, both the images appear to be

identical as shown in Fig. 10a and b and their histograms in Fig. 10c and d are remarkably similar. There is no obvious change on the histograms and it clearly states that the hidden image is not apparent to the observer. The unintentional attacks like noise do not reveal the existence of the hidden image.

However, for most of the images in our test set, the impact of geometrical distortions like Rotation, Scaling and Translation (RST) is not too severe as shown in Table 5. The cropping attack causes synchronization failure of the stegano image and secret image is distorted. As a result no information is carried over and retransmission has to be done.

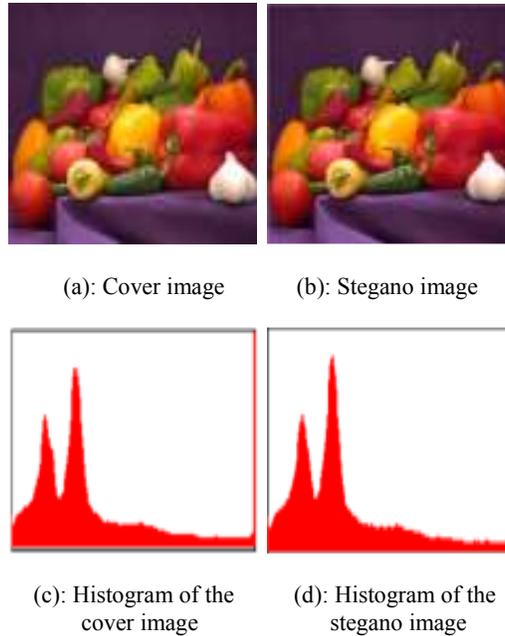


Fig. 10: Simulation results of cover and stegano image to verify histogram attack

Table 5: Comparison of stegano images for various attacks

Type of attack	PSNR	MSE	SSIM
With no effect	44.51	4.58	0.9989
With noise (Poisson)	34.76	21.69	0.9987
With filter (unsharp)	32.01	40.92	0.9999
With compression (SPIHIT_3d)	40.89	3.88	0.9732
RST effects (Selection of Control Points)	14.78	20.14	0.7532

Table 6: Comparative study of related work on performance measures

Reference	Methodology	Performance	
		PSNR	MSE
Mandal and Sengupta, 2011	Minimum deviation of fidelity	39.6	3.46
Hemalatha <i>et al.</i> , 2012	Integer wavelet transform	41.91	----
Ghoshal and Mandal, 2011	Scheme for image authentication	33.2	11.20
Shiva Kumar <i>et al.</i> , 2011	Hybrid domain LSB technique	41.21	----
Proposed Method	Fractional Random Wavelet Transform (FrRnWT) approach	44.390	2.3398

Comparison with related work: We demonstrate the performance of the proposed method in comparison to the other methods and FrRnWT approach is found to be superior in terms of PSNR and MSE. Table 6 lists the performance measures of related work which includes various methodologies viz. (Mandal and Sengupta, 2011, Hemalatha *et al.*, 2012, Ghoshal and Mandal, 2011 and Shiva Kumar *et al.*, 2011).

CONCLUSION

With the emergence of networks and digital technologies and increasing use of communication for transferring files in electronic format, new techniques for information hiding have become necessary. Since no observer can search the value of fractional order, random matrix with uniformly distributed random numbers, it is highly impossible to work out the same to

identify the existence of the hidden image in the cover image. The essence of FrRnWT can be realized with an effective combination of embedding coefficient, fractional order and formation of random matrix and the size of the block. Hence when an application needs the randomness as its key factor FrRnWT provides better results. We have also presented a comparative study of other existing methods with the proposed algorithm. It provides better quality metrics namely PSNR, MSE, SSIM and UIQI for retrieval and faithful reconstruction of the hidden image with unique security measures. We conclude in this study, that the most promising technique of image hiding using Fractional Random Wavelet Transform provides a unified framework for highly secured, robust image steganography. This work looks to have potential future applications in medical field, where we can embed patient's information such as X-Ray, CT-scan images, preserve DNA sequences,

avoid wrong diagnosis and also for secure vigilance and intelligent agencies.

ACKNOWLEDGMENT

The authors express special thanks to the Management of S.V.University, Tirupati, Andhra Pradesh and VIT University, Vellore, Tamil Nadu, India for providing infrastructure and consistent encouragement.

REFERENCES

- Bhatnagar, G., Q.M.J. Wu and B. Raman, 2012. A new fractional random wavelet transform for fingerprint security. *IEEE T. Syst. Man Cybernetics, Part A: Syst. Humans*, 42(1): 262-275.
- Candan, C., M.A. Kutay and H.M. Ozaktas, 2000. Discrete fractional fourier transform. *IEEE T. Signal Process.*, 48(5).
- Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. *Signal Process.*, 90(3): 727-752.
- Ghoshal, N. and J.K. Mandal, 2011. A steganographic scheme for colour image authentication (SSCIA). *Proceeding of 2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, pp: 826-831.
- Hemalatha, S., U.D. Acharya, A. Renuka and P.R. Kamath, 2012. A secure image steganography technique using integer wavelet transform. *Proceeding of 2012 World Congress on Information and Communication Technologies (WICT)*, pp: 755-758.
- International Telecommunication Union (ITU), 1992. Information Technology- Digital Compression and Coding of Continuous-Tone Still Images-Requirements and Specifications Recommendation T.81. ITU Sept., 1992.
- Kingsbury, N., 2001. Complex wavelets for shift invariant analysis and filtering of signals. *Appl. Comput. Harmonic Anal.*, 10: 234-253.
- Liu, Z., H. Zhao and S. Liu, 2008. A discrete fractional random transform. *Optical Communication*, February, 2008.
- Mallat, S.G., 1989. A theory for multiresolution signal decomposition: The wavelet representation. *IEEE T. Pattern Anal. Mach. Intell.*, 11(7): 674-693.
- Mandal, J.K. and M. Sengupta, 2011. Steganographic technique based on minimum deviation of fidelity (STMDf). *Proceeding of 2nd International Conference on Emerging Applications of Information Technology (EAIT)*, pp: 298-301.
- Namias, V., 1980. The fractional order fourier transform and its application to quantum mechanics. *J. Inst. Math Appl.*, 25(3): 241-265.
- Shiva Kumar, K.B., K.B. Raja and S. Pattnaik, 2011. Hybrid Domain in LSB Steganography. *Int. J. Comput. Appl.*, 19(7), (0975-8887).
- Tadiparthi, G.R. and T. Sueyoshi, 2006. Steganim-a novel information hiding technique using animations. *Eng. Lett.*, 13: 3.
- Wang, Z. and Q. Li, 2011. Information content weighting for perceptual image quality assessment. *IEEE T. Image Process.*, 20(5): 1185-1198.
- Wang, Z. and A.C. Bovik, 2002. A universal image quality index. *IEEE Signal Process. Lett.*, 9(3): 81-84.