IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 4, Ver. IV (Jul - Aug. 2014), PP 31-37
www.iosrjournals.org

Image Steganography Based on DFrFT

Subhanchi Gupta[*] ,Navneet Kaur[#] ,Praneet Sizariya
[*]*M. Tech. Scholar, ECE Department SIRT, RGPV Bhopal, India*
[#]*Associate Professor, ECE Department SIRT, RGPV Bhopal, India*
Lecturer, CSE Department SV Polytechnic Bhopal, India

Abstract: *As the escalation of internet is one of the main factor of information technology, data hiding techniques has taken a significant role for the transfer of multimedia content. There are many ways to convert data, so it can be understood only by one who knows how to returns it to its original form. The best way to achieve such secure communication is steganography. It is having skill of hiding data in a way to avoid detection by hackers. The Steganography is used to transmit information in a secret way from one place to other place through public channel. Steganography hides the subsistence of a data so that if successful it generally attracts no doubt at all. Hiding a secret message within a larger one in such a way that a viewer cannot detect the presence of contents of the secret message is steganography. In this research paper we propose a steganography technique which embeds the secret messages in frequency domain. For this, various types of transform can be used, we are combining Discrete Fractional Fourier transform (DFrFT) and Least Significant Bit (LSB) algorithm to enhance the security of image. MATLAB platform is used for simulation; results are shown in the form of peak signal to noise ratio (PSNR).*

Keywords: *Data Hiding; Image Steganography; LSB Substitution; DFrFT; PSNR; MSE.*

I. Introduction

Communication users frequently store, send, or receive private information. This can be done by changing the data in a transform form. The resulting data can be understood only by those who know how to return it to its original form. Encryption is a method of protecting information . A major drawback of encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. Decryption is done if enough time is given to someone. A solution to this problem is steganography [1].

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography basically consists of three things:

cover object (used to hide secret message).

secret message to be embed.

stego object (cover object after hiding the secret data).

Steganography and cryptography are different from each other .In cryptography, the contents of a message is kept secret, where as steganography focuses on keeping the existence of a message secret [2]. Steganography and cryptography both are used to protect information from unwanted parties but none of these technology alone is perfect and can be compromised.

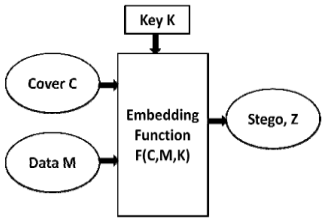


Fig.1: Basic Steganography Model

Many different steganography methods have been proposed during the last few years; most of them can be seen as substitution systems. Such methods try to substitute redundant parts of an image with a secret message; their main disadvantages being the relative weakness against cover modifications.

Earlier spatial domain methods of steganography that is based on Least Significant Bit (LSB) substitution which gives better PSNR result was used. Alternatively other methods involve steganography in frequency domain. Various transforms have been used for various data hiding techniques. DFT, DCT and DFrFT found numerous applications in signal processing and image processing. The area of image processing applications includes steganography, watermarking, compression, encryption [3].

Here, we have introduce discrete fractional Fourier transform (DFrFT) which can be considered as generalization of Fourier transform (FT), it was initially one of the most frequently used tool in signal processing.

Steganography can be used for many applications such as intelligence agencies, defense organizations, in identity cards, for copyright control, in medical imaging etc. The FrFT has found many applications in signal processing and image processing. Signal processing area includes- filtering, de-noising, interference suppression, radar signal processing, and wireless communication systems.

The area of image processing applications includes- steganography, watermarking, compression and encryption and image restoration [3].

This paper is organized as follows. Section

II discusses the basics of steganography and its types i.e. the spatial domain method which involves encoding at the LSBs level, frequency domain techniques and comparison of different data hiding technique.

Section III describes the details of discrete fractional Fourier transform (DFrFT).

Section IV shows results of steganography using this transform. And, section V gives the conclusion.

II. Steganography

The word steganography is derived from Greek words which mean "Covered Writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing"). It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back. With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone "digital". In the realm of this digital world steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed [4].

It is a branch of information hiding in which secret information is covered within other information. The main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. That is unwanted parties should not be able to distinguish any sense between cover-image and stego-image. Thus the stego-image should not deviate much from original cover-image. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. The schematic representation of the steganography is given in Fig. 2:

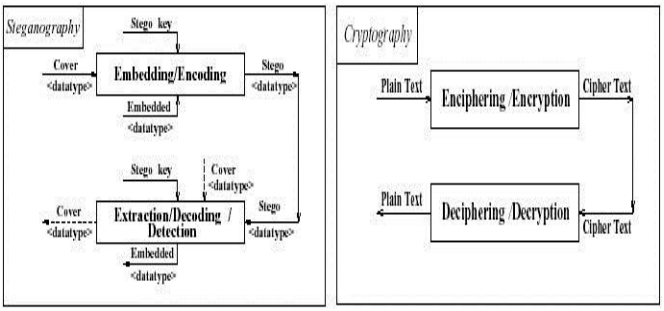


Fig. 2: Steganography versus Cryptography

The techniques of data hiding i.e. steganography, watermarking and cryptography are interlinked. The first two are quite difficult to tease apart especially for those coming from different disciplines. Table 1 summarizes the differences and similarities between steganography, watermarking and cryptography .

Table 1: Comparison of steganography, watermarking and crytography [5]

Creterion/ Method	Stegano graphy	Water marking	Crypto graphy
Carrier	Any digital media	Mostly image/audio files	Usually text based
Secret Data	Payload	Watermark	Plain text
Key	Optional		Necessary
Inputt files	Atleast two unless in self-embedding		One
Output files	Stego-file	Watermarked-file	Cipher-text
Objective	Secrete communication	Copyright preserving	Data protection
Visibility	Never	Sometimes	Always
Flexibilty	Free to choose any cover	Cover choice is restricted	N/A
Fails When	It is detected	It is removed/replaced	De-ciphered

On the basis of the image formats i.e. Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent- Portable Network Graphics (PNG), image steganography are of two types:

a) Steganography in the image spatial domain
b) Steganography in the image frequency domain

Steganography in the image spatial domain:

Spatial features of image are used, in this type of steganography. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits. The LSB substitution embeds the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [4]. The mathematical representation for LSB is as equation 1:

$$x_i' \equiv x_i - x_i \bmod 2^k + m_i \qquad (1)$$

In Equation (1), xi' represents the i^{th} pixel value of the stego-image and xi represents that of the original cover-image. m_i represents the decimal value of the i^{th} block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in equation 2:

$$x_i = x_i \bmod 2^k \qquad \textbf{(2)}$$

Hence, a simple permutation of the extracted m_i gives us the original confidential data [6]. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane. A general framework showing the underlying concept is highlighted in Fig. 3.

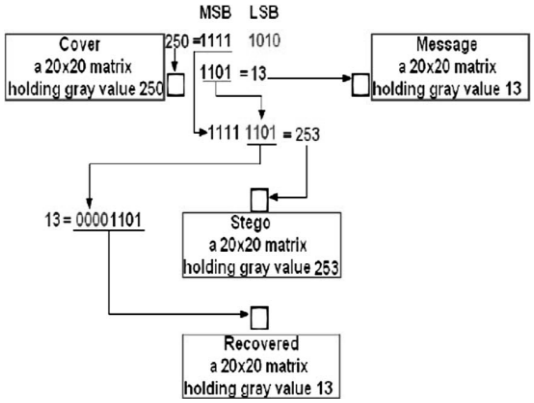


Fig. 3: Steganography in spatial domain. The effect of altering the LSBs up to the 4th bit plane

In the case of steganography, the reconstructed image is only an approximation to the original. Although many performance parameters exist for quantifying image quality, it is most commonly expressed in terms of mean squared error (MSE) and peak signal to noise ratio (PSNR). MSE should be less, for good steganography. A rough approximation of the quality of steganography is provided by PSNR. It should be more for good perception of received image.

Steganography in the image frequency domain:

Robustness of steganography can be improved if properties of the cover image could be exploited. Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it [7]. Using transform-domain techniques it is possible to embed a secret message in different frequency bands of the cover. These methods are more complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in Fast Fourier transform i.e. FFT, Discrete Cosine Transform i.e. DCT or Discrete Fractional Fourier transform i.e. DFRFT.

III. Fractional Fourier Transform

The fractional Fourier transform is a generalization of the ordinary Fourier transform with an order (or power) parameter 'α'. The FrFT belongs to the class of time–frequency representations that have been extensively used by the signal processing community [8]. The FrFT is defined with the help of the transformation kernel K_α as:

$$K_\alpha(t,u) = \sqrt{\frac{1-i\cot\alpha}{2\pi}}\exp\left(j\frac{t^2+u^2}{2}\cot\alpha - jut\csc\alpha\right) \quad \text{if } \alpha \text{ is not multiple of } \pi$$
$$= \delta(t-u) \quad \text{if } \alpha \text{ is multiple of } 2\pi$$
$$= \delta(t+u) \quad \text{if } \alpha+\pi \text{ is multiple of } 2\pi \qquad \textbf{(3)}$$

The FrFT is defined using this Kernel is given by:

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t)\, K_\alpha(t,u)\, dt \qquad \textbf{(4)}$$

Where α = a π/2

The inverse FrFT is given by:

$$x(t) = \int_{-\infty}^{\infty} X_\alpha(u)\, K_{-\alpha}(t,u)\, du \qquad \textbf{(5)}$$

The FrFT is defined for entire time-frequency plane (time and frequency are orthogonal quantities). The angle parameter 'α' associated with FrFT, governs the rotation of the signal to be transformed in time-frequency plane from time-axis in the time-frequency plane. FrFT computation involves following steps:

a. Multiply by a chirp
b. Fourier transform with its argument scaled by 'cscα'
c. Multiply with another chirp
d. Product by a complex amplitude factor

The one-dimensional DFrFT is useful in processing single-dimensional signals such as speech waveforms. For analysis of two-dimensional (2D) signals such as images, we need a 2D version of the FrFT. For an M×N matrix, the 2D FrFT is computed in a simple way. Thus, the generalization of the DFrFT to two-dimension is given by [9].

$$X_{\alpha\beta}(u,s) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K_{\alpha\beta}(u,s;t,r)\, x(t,r)\, dt\, dr \qquad \textbf{(6)}$$

Where

$$K_{\alpha\beta}(u,s;t,r) = k_\alpha(u,t)\, k_\beta(s,r) \qquad \textbf{(7)}$$

In the case of the two-dimensional DFrFT we have to consider two angles of rotation α = aπ/2 and β = b π/2. If one of these angles is zero, the 2D transformation kernel reduces to the 1D transformation kernel [9].

IV. Simulations

In this section, MATLAB is used to simulate the steganography. Then hidden image is embedded in the cover image and transported. Stego-image is the combination of cover image and hidden image. DFrFT is used to convert cover-image in spatial domain into cover-image in frequency domain. LSB substitution algorithm with no of bits 4 is used.

Results for steganography of image in frequency domain with using DFrFT (order α = 0.1 and β = 0.1) are shown as:

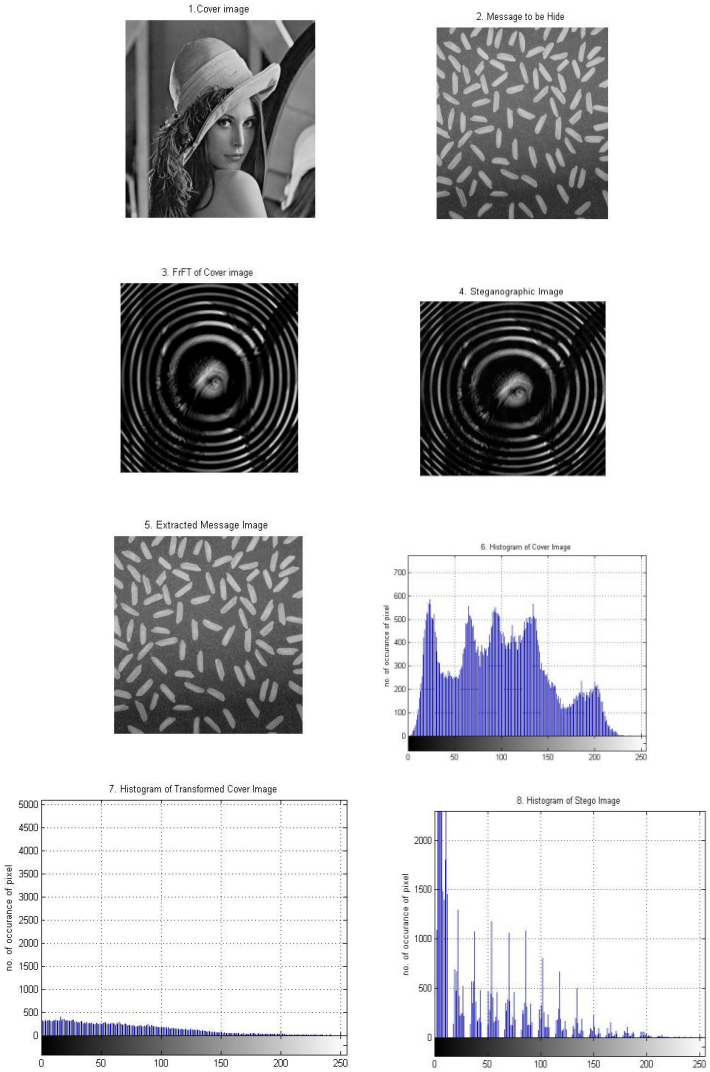
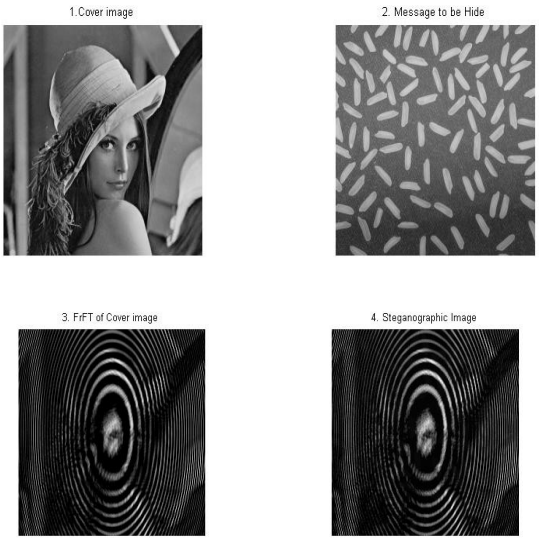


Fig 4: Image Steganography in frequency domain with DFrFT of cover image at order $\alpha = 0.1$ and $\beta = 0.1$

Results for steganography of image in frequency domain with using DFrFT (order $\alpha = 0.1$ and $\beta = 0.5$) are shown as:



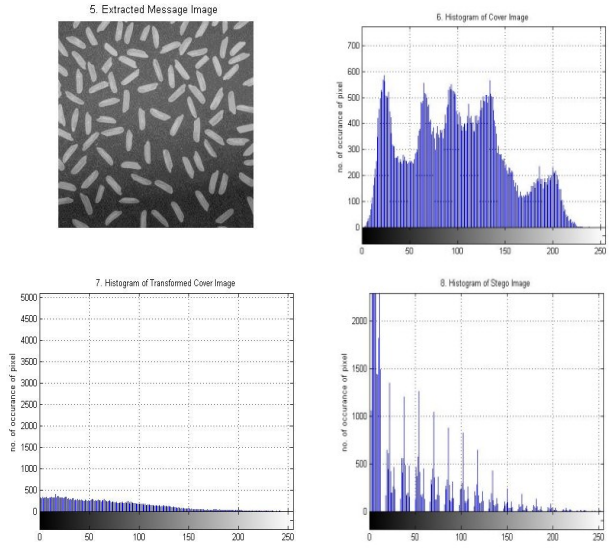


Fig 4: Image Steganography in frequency domain with DFrFT of cover image at order $\alpha = 0.1$ and $\beta = 0.5$

All the above figures shows cover image, transformed cover image, message image, stego image and extracted image, histogram of cover image and histogram of stego image. Although many performance parameters exist for quantifying image quality, it is most commonly expressed in terms of peak signal to noise ratio (PSNR).

Peak Signal to Noise Ratio (PSNR) of cover image to steganographic image is simulated for varying order of transform of FrFT (α and β are same) and results are shown as:

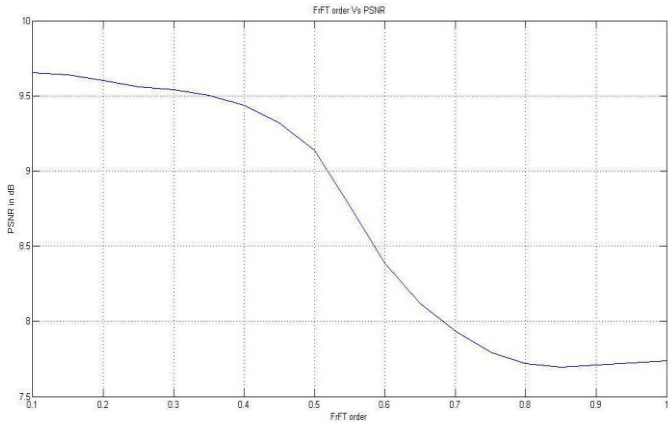


Fig 5: Plot of FrFT order versus PSNR.

Peak Signal to Noise Ratio (PSNR) of cover image to steganographic image is simulated for varying order of transform of FrFT (α and β are different) and results are shown as:

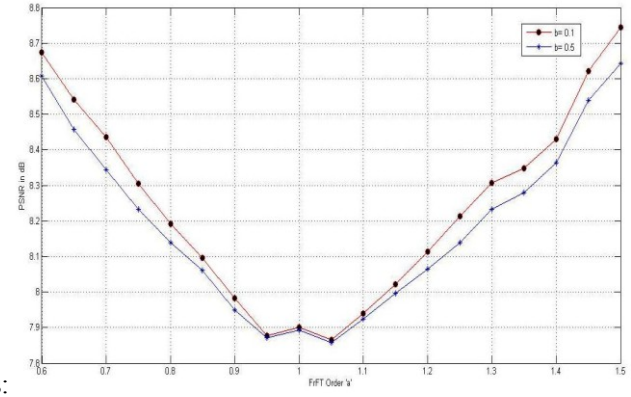


Fig 6: Plot of FrFT order versus PSNR.

It can be seen from the table 3 that PSNR value of cover image to steganographic image are different and PSNR message image to extracted image are same in both the cases.

Table 3: Results showing PSNR

Method	Cover Image	Message Image	PSNR	
			C to S	M to E
Frequency domain with DFrFT of cover ($\alpha=\beta=0.1$)	lena.jpg	rice.png	9.65 dB	29.31 dB
Frequency domain with DFrFT of cover ($\alpha= 0.1$ and $\beta=0.5$)	lena.jpg	rice.png	9.37 dB	29.31 dB

*C = Cover image *E = Extracted image

*M = Message image *S =Stego image

The importance of using DFrFT in steganography is the freedom of choosing its parameter 'α'. The advantage of using DFrFT is that the order acts as a Stego-Key.

V. Conclusion

To transmit confidential data, protection is necessary in order to protect them from malicious users to illegally copy, destroy or change them on internet. The DFrFT is used to make the steganography more robust, as an active opponent may know the extraction algorithm, but the main thing, they does not know about the transformation angles i.e. stego key (Order of FrFT), so without the knowledge of this orders, no one can take inverse of transformed image to extract the message. By varying parameter 'α' and 'β' we can achieve more security over other existing transform techniques. DFrFT is an efficient, more flexible, versatile and powerful tool for applications in digital image processing.

References

[1] G.J. Simmons, The prisoners' problem and the subliminal channel, in: Proceedings of International Conference on Advances in Cryptology, CRYPTO83, August 22–24, 1984, pp. 51–67

[2] Luis B. Almeida, "The Fractional Fourier Transform and Time-Frequency Representations" IEEE transactions on signal processing, vol. 42, no. 11, November 1994.

[3] Johnson, N. F. and Jajodia, S, "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2):, Feb 1998,pp 26-34.

[4] I.S. Yetik, M.A. Kutay, H.M.Ozaktas, "Image representation and compression with the fractional Fourier transform", Opt. Communication. 197 (2001) 275-278

[5] Wang, H and Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[6] Rajiv Saxena and Kulbir Singh, "Fractional Fourier Transform: A Novel Tool for Signal Processing" Journal of Indian Inst. Sci., Jan.–Feb. 2005, 85, pp11–26.

[7] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, South Africa, 2005.

[8] Abbas Cheddad, JoanCondell, Kevin Curran, PaulMcKevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier, Signal Processing 90 (2010) 727–752

[9] Anjali A. Shejul and Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011, 1793-8201.

[10] Ashish Soni, Rakesh Roshan, Jitendra Jain, "Image Steganography in Discrete Fractional Fourier Transform Domain", International Conference on Intelligent System and Signal Processing 2013, ISBN no: 978-1-4799-0316-0©IEEE.