Image Steganography using Discrete Fractional Fourier Transform

Ashish Soni
Dept of Electronics & Communication, Acropolis Technical Campus, Indore
ashishsoni15@gmail.com

Jitendra Jain
Dept of Electronics & Communication, Jaypee University of Engineering & Technology, Guna
jitendrajn69@gmail.com,

Rakesh Roshan
Dept of Electronics & Communication, Rishiraj Institute of Technology, Indore
rakeshroshan19@gmail.com

***Abstract*— The Fractional Fourier transform (FrFT), as a generalization of the classical Fourier transform, was introduced many years ago in mathematics literature. For the enhanced computation of fractional Fourier transform, discrete version of FrFT came into existence i.e. DFrFT. This paper illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The simulation result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key i.e. order parameter of this transform.**

***Keywords*— *Information Hiding; Steganography; Stego Keys; Fourier Transform and Discrete Fractional Fourier Transform*.**

I. INTRODUCTION

For many years Information hiding has captured the imagination of researchers. Two basic methods of information hiding are cryptography and steganography. The term steganography means "cover writing" and cryptography means "secret writing". These techniques are used to address digital rights management, protect information, and conceal secrets. Information hiding techniques provide an interesting challenge for digital forensic investigations.

The message is encrypted before transmission and decrypted at the receiver side with the help of a key. Nobody, except the one having the key, can determine the content of the key. The message is called the plain text and the encrypted form is called the cipher text [1]. The information is protected at the time for transmission. However, after decryption, the information becomes unprotected and it can be copied and distributed.

In steganography, the message is embedded into the digital media rather than encrypting it. The digital media content, called the cover, can be determined by anybody; however, the message hidden in the cover can be detected by the one having the true key. The message stays in the message after the receiver gets the data. This allows steganography to protect the embedded information after it is decrypted. Steganography is therefore broader than cryptography.

In this paper, we have introduce fractional Fourier transform (FrFT) which can be considered as generalization of Fourier transform (FT), it was initially one of the most frequently used tool in signal processing [2]. FRFT domain combines space and frequency domain. It indicates spectral content of the signal/image as well as the time location of the spectral components.

The FrFT has found numerous applications in signal processing and image processing. Signal processing area includes- filtering, de-noising, interference suppression, radar signal processing, electromagnetic wave propagation, and wireless communication systems. The area of image processing applications includes - steganography, watermarking, compression and encryption and image restoration [3].

II. STEGANOGRAPHY

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. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". 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. 1:

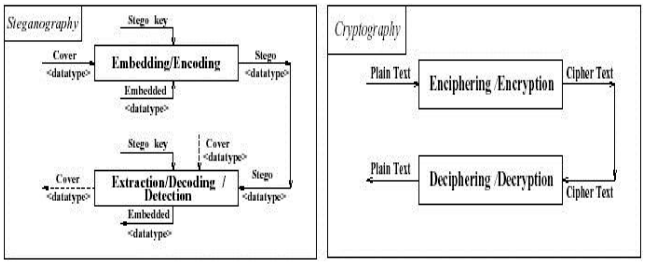

Fig. 1. Steganography versus Cryptography

Steganography has been widely used, including in recent historical times and the present day. Various methods are used such as invisible inks, tiny pin punctures on specific characters, pencil marks on handwritten characters, typewriter correction ribbon, etc. [4].

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.

978-1-4799-0317-7/13/$31.00©2013 IEEE

Table I. Comparison of steganography, watermarking and crytography

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		Necessa ry
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

The most popular image formats used on the internet are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent- Portable Network Graphics (PNG). Most of the methods of steganography are developed aimed to exploit the structures of these particular formats. On the basis of these formats, image steganography are of three types:

1) *Steganography in the Image Spatial Domain*: 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 basic concept of LSB substitution is to embed 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 [5]. The mathematical representation for LSB is as equation 1:

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

In equation (1), x'_i represents the i^{th} pixel value of the stego-image and x_i 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:

$$m_i = x_i \bmod 2^k \qquad (2)$$

Hence, a simple permutation of the extracted m_i gives us the original confidential data. This method is easy and straight forward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane.

2) *Steganography in the Image Transform 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. Using transform-domain techniques it is possible to embed a secret message in different frequency bands of the cover. Frequency domain transformation can be applied either in discrete cosine transform (DCT), discrete wavelet transform (DWT) or Discrete Fractional Fourier transform (DFRFT). Transform domain methods have a lower payload compared to spatial domain algorithms.

3) *Adaptive Steganography*: Adaptive steganography is special case of two former methods. It is also known as "Statistics aware embedding" [6] and "Masking" [7]. This method takes statistical global features of the image before attempting to embed secret data in DCT or DWT coefficients. The statistics will dictate where to make changes.

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). For a good steganography, MSE should be less. PSNR is provided only to give us a rough approximation of the quality of steganography. PSNR should be more for good perception of received image.

III. Fractional Fourier Transform

The ordinary Fourier transform and related techniques are of great importance in many areas of science and engineering. 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 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. The FrFT is defined with the help of the transformation kernel K_α as [9].

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

The FrFT is defined using this Kernel is given by:

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

Where $\alpha = a\,\pi/2$

The inverse FrFT is given by:

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

When FrFT is analyzed in discrete domain there are many definitions of Discrete Fractional Fourier Transform (DFrFT) [10].

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 FrFT 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: The 1D FrFT is applied to each row of matrix and then to each column of the result. Thus, the generalization of the FrFT to two-dimension is given by [11].

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

Where

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

In the case of the two-dimensional FrFT we have to consider two angles of rotation $\alpha = a\pi/2$ and $\beta = b\,\pi/2$. If one of these angles is zero, the 2D transformation kernel reduces to the 1D transformation kernel.

IV. Simulation and Results

In this simulation, the cover image is a carrier of embedded image; hidden image is an image to be embedded in the cover image and transported. LSB algorithm is used to hide an image in a cover image. Stego-image is the combination of cover image and hidden image. FrFT is used to convert stego-object in spatial domain into stego-image in frequency domain. Various orders of FrFT are taken into account. Results for steganography of image in spatial domain and transform domain are shown as:

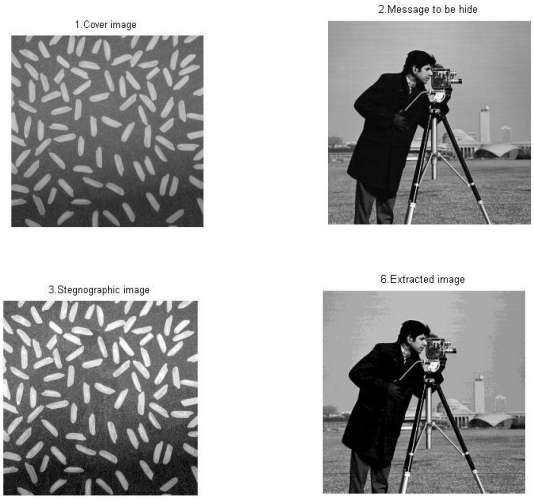

Fig. 2. Steganography in image spatial domain

Fig. 3. Steganography in image transform domain

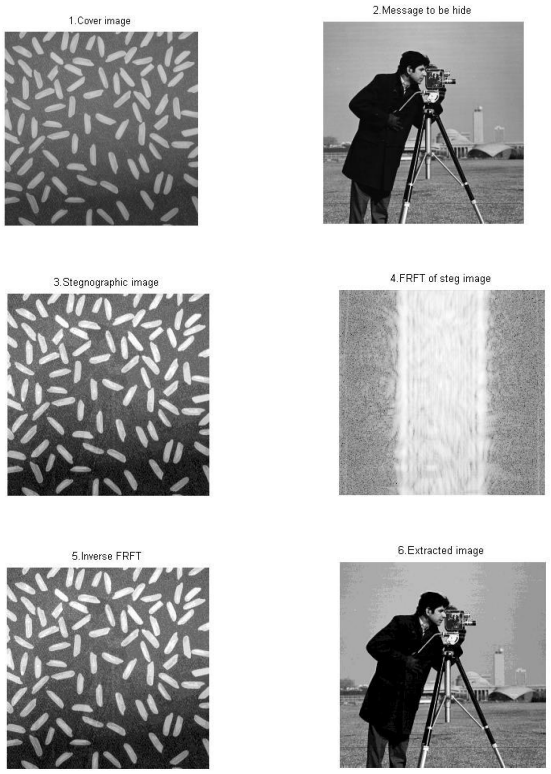

Fig. 4. Steganography in image transform domain

Table II. Comparison of PSNR values of different methods

Method	Cover Image	Message Image	PSNR	
			M to E	C to S
Spatial domain	rice.png	cameraman.tif	29.01 dB	32.46 dB
Transform domain	rice.png	cameraman.tif	29.01 dB	7.81 dB
*Transform domain	rice.png	cameraman.tif	29.01 dB	32.46 dB

In Fig. 2, steganography of image is done in spatial domain. In this method no need of transform is required. Extraction is easy in this case. In Fig. 3, steganography is done in transform domain, where cover image is transformed using FrFT of order $\alpha = 0.78$ and $\beta = 0.25$. In Fig. 4, Steganography is done in transform domain, where steganographic image is transformed using FrFT of order $\alpha = 0.78$ and $\beta = 0.25$. PSNR is same but it adds additional security keys i.e. order of FrFT.

V. Conclusions

To transmit confidential data, protection is necessary to protect them from malicious users to illegally copy, destroy or change them on internet. Steganography is the art of hiding data into other data. In steganography using FrFT it is observed that FrFT makes the full use of the additional degree of freedom provided by its fractional order 'α' to achieve an optimum domain for which PSNR is more and MSE is less than any other two dimensional transform. By varying parameter 'α' we can achieve more security over other existing transform techniques.

Acknowledgment

The Authors would like to thank Head, Dept. of Electronics and Communication Engineering, Jaypee University of Engineering and Technology, Guna. Authors also thank to Director, Acropolis Technical Campus, Indore.

References

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier, Signal Processing 90 (2010) 727–752.

[2] Bracewell RN. The Fourier transform and its applications. McGraw-Hill, 1986.

[3] Ashutosh Kumar Singh and Rajiv Saxena, "Recent developments in FRFT, DFRFT with their applications in signal and image processing", Recent Patents on Engineering, 2011, Vol. 5, No. 2.

[4] William Stallings. Cryptography and Network Security. Pearson education, Inc. 2011.

[5] 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.

[6] Provos, N. and Honeyman, P. "Hide and seek: An introduction to steganography". IEEE Security and Privacy, 01(3), pp.32-44,2003.

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

[8] Rajiv Saxena and Kulbir Singh, "Fractional Fourier Transform: A Novel Tool for Signal Processing" Journal of Indian Inst. Sci., Jan.–Feb. 2005, 85, 11–26.

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

[10] Soo-Chang Pei and Jian-Jiun Ding, "Closed-Form Discrete Fractional And Affine Fourier Transforms", IEEE Transactions On Signal Processing, Vol. 48, No. 5, May 2000.

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

Ashish Soni received his B.E. degree in 2009 and M.Tech. from Jaypee University of Engineering & Technology, M.P. in 2012. Currently he is working as Assistant Professor in Acropolis Technical Campus, Indore. His research area of interests is Fractional Fourier Transform, Image Compression and Digital Image Processing.

Jitendra Jain has completed his B. Tech degree in 2009 and M.Tech. degree in 2012. Currently he is Research Scholar in Jaypee University of Engineering and Technology, Guna. His area of interest is Analog and Digital Electronics, Digital Signal Processing, VLSI, and Information and Coding Theory.

Rakesh Roshan completed his B.Tech. from Jaypee University of Information and Technology, Waknaghat in 2010 and M.Tech. from Jaypee University of Engineering and Technology, Guna in 2012. Currently he is working as Assistant Professor in Rishiraj Institute of Technology, Indore His area of research includes Information and Coding, Wireless Communication and Digital Image Processing.