# Secured Image Steganography using Different Transform Domain

Akanksha Kaushal
ECE Department
Ujjain Engineering College
Ujjain, India

Vineeta Chaudhary
ECE Department
Ujjain Engineering College
Ujjain, India

## ABSTRACT
In today's communication world, data sharing and transfer is increasing exponentially. The threat of an attacker accessing secret information has been an ever existing concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat. Steganography is the art of hiding the existence of the communication message before sending it to the receiver. In this paper it is proposed to use Discrete Fractional Fourier transform (DFrFT) as basic tool in image processing for data hiding technique called steganography. A comparative study of steganography in spatial domain and frequency domain based on Discrete Fourier transform (DFT), Discrete cosine transform (DCT), Discrete Fractional Fourier transform (DFrFT) is made. Peak signal to noise ratio (PSNR) and Mean square error (MSE) of cover image and stego image are used as performance index and it is found that among three frequency domain methods DFrFT based steganography gives better results in terms of PSNR and MSE and also provide more security for communication. MATLAB platform is used for simulation, results show that the proposed technique provides more security, better PSNR and lower MSE of cover image and stego image.

## General Terms
Image, Peak signal to noise ratio, Mean square error.

## Keywords
Steganography, Cryptography, Discrete Fourier transform, Discrete cosine transform, Discrete fractional Fourier transform.

## 1. INTRODUCTION
**I**n this modern world, internet offers great convenience in transmitting large amounts of data in different parts of the world. However, the safety and security of long distance communication remains an issue. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret [1]. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. 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 differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret.

Earlier used spatial domain methods of steganography are based on Least Significant Bit (LSB) substitution which giver better PSNR result but fail to prevent attacks and are easily detected so a need arises for alternative methods for steganography. Alternatively other methods involve steganography in frequency domain. Various transforms such as DFT, DCT have been used for various data hiding techniques. DFT and DCT found numerous applications in signal processing and image processing. The area of image processing applications includes steganography, watermarking, compression, encryption and image restoration.

In this paper, it is proposed to use discrete fractional Fourier transform (DFrFT) for steganography, which is a generalization of Fourier transform (FT) [2].

This paper is organised as follows. Section 2 briefly discusses the types of steganography i.e. (2.1) the spatial domain method which involves encoding at the LSBs level and (2.2) frequency domain methods such as Discrete Fourier Transform (DFT), Discrete Cosine transform (DCT) and Discrete Fourier transform (DFrFT). Section 3 shows simulation work and performance analysis of these methods. Finally section 4 gives the conclusion.

## 2. TYPES OF STEGANOGRAPHY
Steganography is a branch of information hiding in which secret information is camouflaged 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 (image not containing any secret message) and stego-image (modified cover-image that containing secret message).

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 three types:

- Steganography in the image spatial domain
- Steganography in the image frequency domain
- Adaptive steganography

Steganography in spatial domain and frequency domain are explained in this section. Adaptive steganography is not discussed in present work.

### 2.1 Steganogaphy in Image Spatial Domain
Here spatial features of image are used. 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 [3]. The mathematical representation for LSB is as equation 1:

$$x'_i = x_i - x_i \bmod 2^k + m_i \quad (1)$$

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:

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

Hence, a simple permutation of the extracted mi gives us the original confidential data [5]. 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. 1.

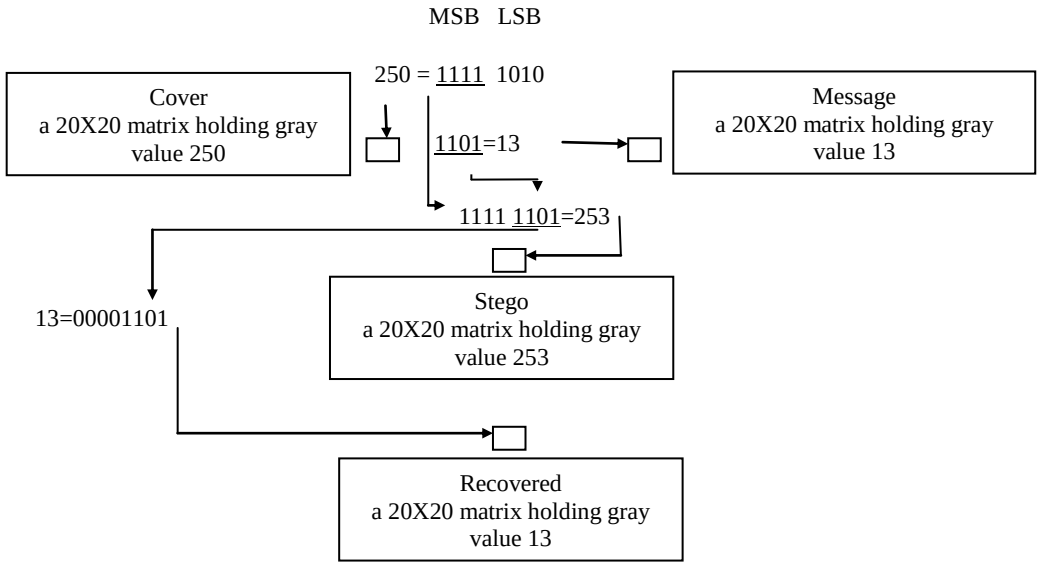


**Fig. 1: Steganography in spatial domain. The effect of altering the LSBs up to the 4th bit plane**

PSNR and MSE are used as performance parameters. Although this method gives good results in terms of PSNR and MSE but it is more prone to attacks and can be easily detected thats why frequecy domain methods are recommended to use for secure steganography

## 2.2 Steganography in 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 [4]. 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 like Discrete Fourier transform i.e. DFT, Discrete Cosine Transform i.e. DCT or Discrete Fractional Fourier transform i.e. DFrFT can be applied.

The Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components. The output of the transformation represents the image in the Fourier or frequency domain, while the input image is the spatial domain equivalent. In the Fourier domain image, each point represents a particular frequency contained in the spatial domain image [6]. The Fourier Transform is used in a wide range of applications, such as image analysis, image filtering, image reconstruction and image compression. For a square image of size N×N, the two-dimensional DFT is given by:

$$F(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\, e^{-i2\Pi\left(\frac{ki}{N}+\frac{lj}{N}\right)} \quad (3)$$

where *f(i,j)* is the image in the spatial domain and the exponential term is the basis function corresponding to each point *F(k,l)* in the Fourier space [7].

Like other transforms, the Discrete Cosine Transform (DCT) attempts to decorrelate the image data. After decorrelation each transform coefficient can be encoded independently without losing compression efficiency. For a square image of size N×N, the two-dimensional DCT is given by:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\Pi(2x+1)}{2N}\right]\cos\left[\frac{\Pi(2y+1}{2N}\right] \quad (4)$$

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 [9]. 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].

$$X_{\alpha\beta}(u,s) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K_{\alpha\beta}(u,s;t,r)\, x(t,r)\, dt\, dr \qquad (5)$$

Where

$$K_{\alpha\beta}(u,s;t,r) = k_{\alpha}(u,t)\, k_{\beta}(s,r) \qquad (6)$$

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. The parameter ' α' (transform order) act as security key for DFrFT, by varying the parameter α we can achieve more security over existing transform techniques.

## 2.3 Adaptive Steganography

Adaptive steganography is a special case of two former methods. It is also known as masking. In this paper adaptive steganography is not discussed.

## 3. SIMULATTION WORK AND PERFORMANCE ANALYSIS

The block diagram shown below indicate the flow of procedure for steganogrpahy in spatial domain (fig 2) and steganography in frequency domain(fig 3).


**Fig.2: Block Diagram for Steganography in Spatial Domain**

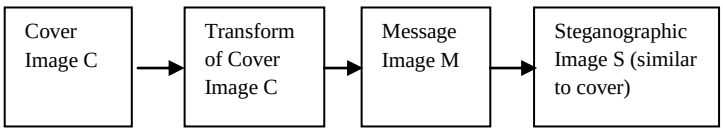


**Fig.3: Block Diagram for Steganography in Transform Domain**

Here for the simulation MATLAB version 7.12.0.635 (R2011a) is used, hidden image is an image to be embedded in the cover image and transported. Stego-image is the combination of cover image and hidden image. 2D-DFT, DCT & DFrFT is used to convert cover-image in spatial domain into cover-image in frequency domain then LSB substitution algorithm with no of bits 4 is used. Result images for steganography of image in spatial domain and transform domain are shown using fig (4-17). Fig.4 and fig.5 show cover image and message image which are common for all the applied methods. Fig.6,fig.7,fig.8 represent steganography in spatial domain with 4 number of LSB substituted. Fig.9,fig.10,fig.11show image steganography using 2D-DFT. Fig.12,fig.13,fig.14 show image steganography using DCT and fig.15,fig.16,fig.17 show image steganography using DFrFT for the fractional order value α = aπ/2 and β = b π/2, here we have shown result for a= 0.256 and b= 1.739.

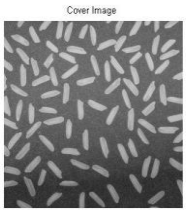


Fig.4 Cover Image


Fig.5 Message Image

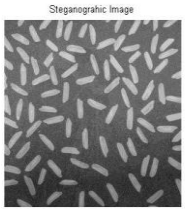


Fig.6 Steganographic Image


Fig.7 Extracted Message Image

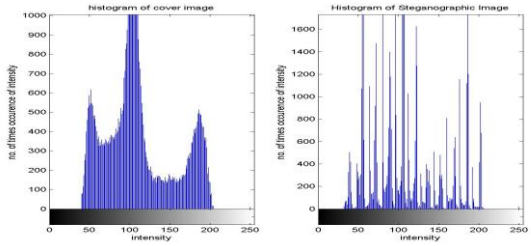


**Fig.8 Histogram of Cover Image and Steganographic Image**

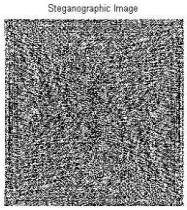


Fig.9 Steganographic Image Using 2D-DFT


Fig.10 Extracted Message Image using 2D-DFT

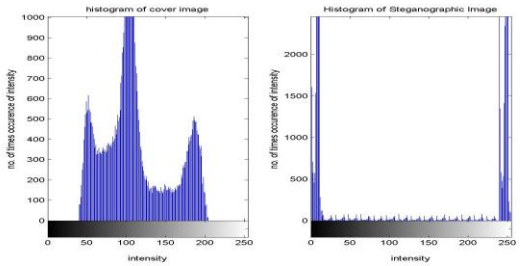


Fig.11 Histogram of Cover Image and Steganographic Image using 2D-DFT


Fig.12 Steganographic Image Using DCT


Fig.13 Extracted Message Image Using DCT

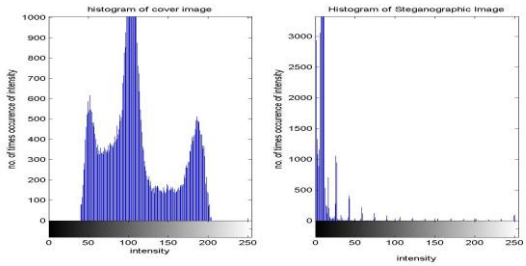


Fig.14 Histrogram of Cover image & Steganographic Image using DCT

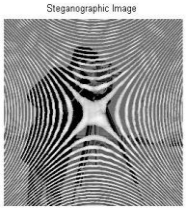


Fig.15 Steganographic Image Using DFrFT


Fig.16 Extracted Message Image Using DFrFT

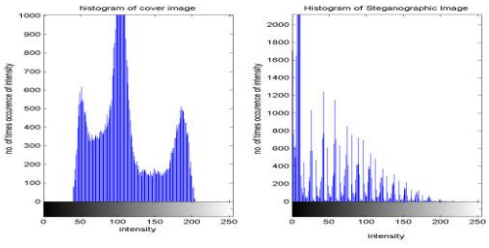


Fig.17 Histogram of Cover Image and Steganographic Image using DFrFT

Comparison of PSNR and MSE values in spatial domain method and using different transform is given in table no. 1.

**Table 1 Comparison of PSNR and MSE values in spatial domain method and using different transform**

| Method | Cover Image | Message Image | PSNR | | MSE | |
|---|---|---|---|---|---|---|
| | | | M to E | C to S | M to E | C to S |
| Spatial domain | rice.png | cameraman.tif | 29.01 dB | 32.46 dB | 82.156 | 37.175 |
| Transform domain with DFT | rice.png | cameraman.tif | 29.01 dB | 6.23 dB | 82.156 | 1.557e+004 |
| Transform domain with DCT | rice.png | cameraman.tif | 29.01 dB | 7.29 dB | 82.156 | 1.222e+004 |
| Transform domain with DFrFT | rice.png | cameraman.tif | 29.01 dB | 8.52 dB | 82.156 | 9.201e+003 |

*C = Cover image *E = Extracted image

*M = Message image *S =Stego image

It is clear from the above table; DFrFT gives better PSNR and MSE performance against DFT and DCT. It also add more security over these two transforms because a wide variation range for α and β can be used for DFrFT.

## 4. CONCLUSION

This paper presents a comparative study of image steganography in spatial domain and frequency domain. LSB techniques in a spatial domain have a high payload capacity and give good performance results but they often fail to prevent statistical attacks and are thus easily detected and if the presence of hidden information is revealed or even suspected the purpose of steganography is partly defeated therefore it is recommended to use the promising frequency domain techniques for steganography using DFT, DCT and DFrFT. Results show that DFrFT gives better PSNR and MSE performance against DFT and DCT. Security of hidden information is a major issue in communication and the transform order α of DFrFT acts as a security key.

## 5. REFERENCES

[1] Wang,H and Wang, S, "cyber warfare steganography vs steganalysis " communication of the ACM, 47:10, october 2004.

[2] Bracewell RN. The fourior transform and its application McGraw-Hill 1986.

[3] Morland,T steganography and steganalysis Leiden institute of advance Computing science.

[4] 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, Feburary,2011, 1793-8201.

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

[6] R.Fisher, S.Perkins, Awalker and Walfort "Fourier Transform".

[7] Rajiv Saxsena and Kulbir Singh" Fractional Fourier Transform: A Novel Tool for Signal Processing"Journal of Indian Inst Scn, Jan.-Feb.2005,85,11-26.

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

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