Weighted Fractional Fourier Transform based Image Steganography

Sudhir Keshari
Electronics & Communication Engineering
Malaviya National Institute of Technology
Jaipur, India
E-mail: keshariec604@gmail.com

Shri Gopal Modani
Electronics & Communication Engineering,
Malaviya National Institute of Technology
Jaipur, India
E-mail: shrigmodani@gmail.com

***Abstract*—In this paper an innovative technique for image Steganography has been proposed based on Weighted fractional Fourier Transformation (WFRFT). The secret image is embedded in the intermediate domain of the cover image. Window size of 2 x 2 is selected from the cover image and converted into its intermediate domain between spatial and frequency by using WFRFT. Now, bits of the secret image, which are formed by converting them into binary form, are embedded within the two LSB positions of the real part of the transformed image. Finally, inverse WFRFT is performed to convert back from intermediate domain into spatial domain to generate the stego image. Secret image is received at recipient side through the reverse procedure of adopted at transmitter. The experimental results has demonstrated and discussed through histogram analysis for verifying the proposed technique.**

Keywords – Cover image, Secret image, Stego image, Weighted fractional Fourier transform (WFRFT), Least Significant Bit (LSB), Image Steganography.

I. INTRODUCTION

Multitude use of visual data has made the world more lively and interesting. Maps, sketches, pictures, photographs and videos are frequently transferred from one place to other place with a rapid rate by using electronic mails and mobile phones equipments. Consequently, the usage of visual data in digital form has increased since last few years. So it is necessary to authenticate these visual data between sender and intended recipient. Authentic visual data are transmitted and received by the military, police, financial institutions and entertainment industry. These applications force the techniques for carrying secrete communication called Steganography. Steganography is art of writing hidden message in such a way that no one, apart from sender and recipient, know about hidden message. Information which is concealed inside the cover image is called payload. The main goal is to protect secret communication of payload between sender and intended recipient against the malicious users. Thus, such methods are to be preferred in which minimum amount of degradation on the cover data occurred.

Several techniques are available for concealing the image payload, also called payload for simplification, inside the cover image without changing its visible properties. Instead of direct embedding the payload within the cover image, [1] Debnath Bhattacharyya, Jhuma Dutta, Poulami Das have used the frequency domain.

In this paper, a new technique for embedding the payload inside the cover image has been proposed by using weighted fractional Fourier transform. Our research work is organized as follows, in section I, scope and applications of Steganography in the real world have been described. In section II, fundamental ideas of WFRFT has been discussed and claimed that the image Steganography based on WFRFT is superior to image Steganography based on Discrete Fourier Transform (DFT) [1]. In section III, proposed technique has been presented. In section IV, simulation results have been shown and analyzed with the proposed technique. Finally, Section V concludes the paper.

II. PRIMILIMIRIES

Weighted Fractional Fourier transform (WFRFT) is an important tool to analysis the intermediate domain between time and frequency. The intermediate domain is determined by a parameter given by a user, who is transmitting the payload for the purpose of image Steganography. WFRFT generalizes the conventional Fourier transform (FT) based on the idea of fractionalizing the eigenvalues of FT.

Any kind of FRFT $\mathcal{F}^a$ for a continuous invertible signal $f(x)$ can be defined as follows:

$$\mathcal{F}^a[f(x)] = w_0(a)f(x) + w_1(a)F(x) + w_2(a)f(-x) + w_3(a)F(-x) \quad (1)$$

$$\text{Where } F(k) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty} f(x)e^{-jkx}dx \quad (2)$$

$$w_l(a) = cos\left[\frac{(a-l)\pi}{4}\right] cos\left[\frac{2(a-l)\pi}{4}\right] exp\left[\frac{3(a-l)\pi i}{4}\right] \quad (3)$$

978-1-4577-0792-6/11/$26.00 ©2011 IEEE

$$w_l(a) = cos\left[\frac{(a-l)\pi}{4}\right] cos\left[\frac{2(a-l)\pi}{4}\right] exp\left[-\frac{3(a-l)\pi i}{4}\right] \quad (4)$$

Where a is a real number called transform order, $F(k)$ is the Fourier transform of a signal $f(x)$, k is frequency domain and $w_l(a)$ its weighting coefficients where $l = 0,1,2,3$. And $f(x)$, $F(x)$, $f(-x)$ and $F(-x)$ are itself signal, Fourier transform, time inversion of signal and frequency inversion of Fourier transform respectively .

Apart from the description about WFRFT for continuous signal, discrete signals play a significant role in the field of image processing because image pixels are in the discrete form. So, WFRFT for an arbitrary complex sequence $x(n)$ is defined as:

$$\mathcal{F}^a[X_0(n)] = w_0(a)X_0(n) + w_1(a)X_1(n) + w_2(a)X_2(n) + w_3(a)X_3(n) \quad (5)$$

$\{X_0(n), X_1(n), X_2(n), X_3(n)\}$ are 0 – 3 times DFT of $X_0(n)$ respectively, and $X_0(n)$ is the DFT of $X3(n)$. Here, the weighting coefficients could be generated by eqs. (3)– (4). The conventional DFT is defined as:

$$\begin{cases} X(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n) e^{-j\frac{2\pi}{N}kn} \\ x(n) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} X(k) e^{j\frac{2\pi}{N}kn} \end{cases} \quad (6)$$

It is also called 4 – WFRFT and its complete details are available in the reference [2].

The advantage of using the WFRFT with respect to DFT is that transform order which determines the intermediate domain between spatial and frequency is considered as a secret key which can be used as image Steganography as well as image encryption simultaneously.

III. PROPOSED TECHNIQUE

The proposed technique emphasizes the innovative technique for embedding the payload inside the cover image for secret communication. This technique utilize gray scale cover image of size (M x N) and payload of size (M/2 x N/2) – 16 bits (maximum). WFRFT is used to transform the image from spatial domain to the intermediate domain. The complete description about the insertion and extraction process of payload is described in the following section:

A. Insertion Procedure

1. Select the cover image and payload of size (M, N) and (M/2, N/2) respectively.
2. Obtain blocks of window size 2x2 from the cover image and repeat step 3 to 8 until the finishing of the cover image.
3. Perform Weighted fractional Fourier transform with transform order a for obtaining the intermediate domain which consists real and imaginary components.
4. Concentrate only on the real component of intermediate domain.
5. Convert into binary form on considering absolute real values.
6. Select the first pixel value of the payload and convert it into binary 8 – bit form.
7. Take two-two bits of first pixel of payload and insert into two bit LSB positions of each pixels of 2x2 window.
8. Finally inverse weighted fractional Fourier transform of same transform order is performed.
9. Finally, Stego image is produced for transmission.

B. Extraction Algorithm

1. Stego image is considered as input of the receiver.
2. Obtain blocks of window size 2x2 of stego image and repeat step 3 to 8 to produce payload.
3. Perform the weighted fractional Fourier transform of same transform order a.
4. Concentrate only on the real component of intermediate domain.
5. Convert into binary form on considering absolute real values.
6. Extract two LSB bits from each pixel of block size of 2x2 and replace these positions by '0', so that there are fewer changes in the gray values of the cover image.
7. Finally, perform inverse weighted fractional Fourier transform of same transform order of block obtain in the 06 step.
8. Combine all extracted bits and convert them into decimal form to produce the first pixel of payload.

IV. SIMULATION RESULTS and DISCUSSION

The performance of proposed technique have been done on MATLAB platform and is analyzed by selecting the cover image of 'lena.jpg' of size 512x 512 and payload 'camerman.tif' of size 256x256. The spatial domain of cover image is transformed into intermediate domain by using WFRFT with transform order α and the order can be considered as a secret key for image Steganography. The results corresponding to proposed technique are shown below:

Figure 1 & 2 shows the cover image and payload. Embedding process has been done with help of

Fig. 1 Cover image

Fig. 4 Recover cover image

Fig. 2 Payload

Fig. 5 Received payload

Fig. 3 Stego image

Fig.6 degradation of cover image at recipient side

combination of WFRFT with transform order 0.7and LSB techniques. The advantage of LSB technique is that there is less reduction in the pixels values of the cover image as a result resembles the cover image called Stego image as shown in the figure 3. Moreover, it is important to note that payload should be received at receiver side without any degradation. After extracting the image from stego image produced payload is shown in the figure 5 and recover cover image which have less pixels value relative to the original cover image as shown in the figure 4. The reduction of pixels values of recover cover image with respect to original cover image has been shown in the figure 6. Histogram analysis gives complete description about the pixels gray scale values. Figure 7 – 11 show the histograms of original cover image, stego image, payload, recover cover

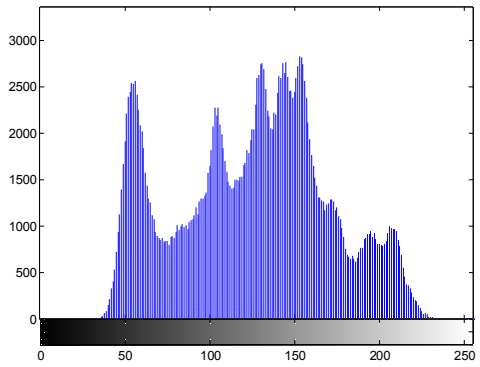

Fig.7 Histogram of cover image

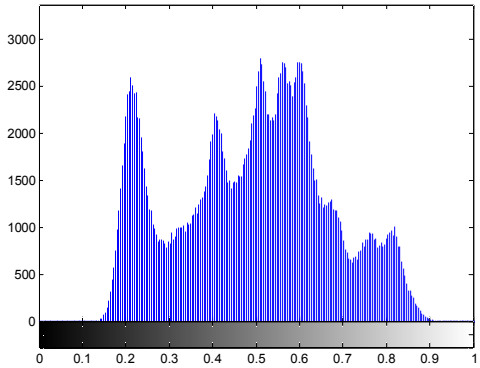

Fig.8 Histogram of Stego image

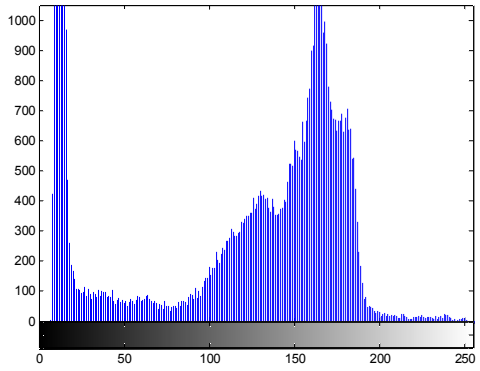

Fig.9 Histogram of payload

image and recover payload respectively. From the histogram analysis, it is concluded that the original cover image and Stego image have similar histogram not same, as well as at receiver side, stego image and recover cover image have also similar histogram. There is no significant difference between pixels of the cover image and the stego image. The difference is created when the bits corresponding to payload

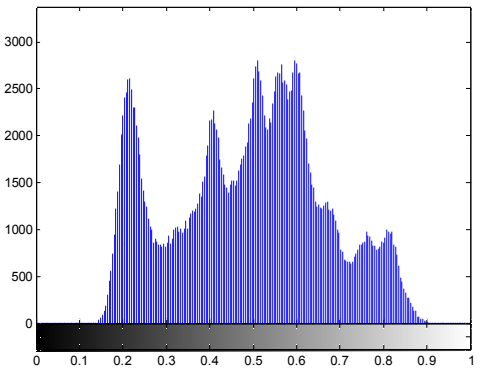

Fig.10 Histogram of recover cover image

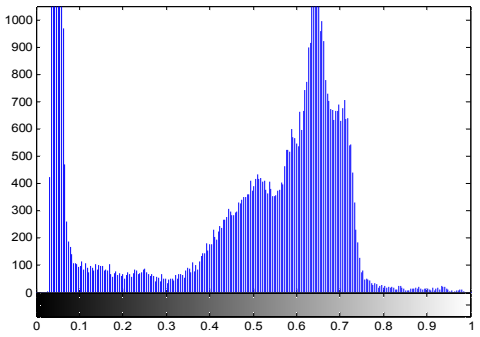

Fig.11Histogram of received payload

are extracted from the stego image and then filled it with zeros. Consequently, it is difficult to identify the payload in the stego image.

V. CONCLUSION

In this paper, we have proposed a new technique for embedding the payload inside the cover image by using the weigthed fractional Fourier transform. The advantage of WFRFT over Fourier transform is that the transform order corresponding to the WFRFT can be considered as a secret keys. This technique can be utilized for practical purpose.

VI. REFERENCE

[1]. Debnath Bhattacharyya, Jhuma Dutta, Poulami Das, "Discrete Fourier transformation based Image Authentication technique", *8th IEEE, Int. Conf. on cognitive informatics (ICCI)*, 2009.

[2]. Mei Lin, Sha XueJun, Ran QinWen, Zhang MaiTong, "Research on application of 4 – weighted fractional Fourier transform in communication system", *Science China*, Vol. 53 No. 6, pp. 1251–1260 June 2010.