Digital Image Watermarking using Fractional Fourier Transform with Different Attacks

Apoorv Tiwari[1] **, Akhilesh pandey**[2]**, Mahendra Kumar**[3]
Department of Computer Science Engineering, Suresh Gyan Vihar University, Jaipur, Rajasthan, India[1, 2]
Department of Electronics, UCE, Rajasthan Technical University, Kota, Rajasthan, India[3]
apurvtiwari27@gmail.com; akhileshMtech10@gmail.com; miresearchlab@gmail.com

ABSTRACT-- ***In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. This work provides Digital image watermarking based on Fractional Fourier transform and two dimensional fast Fourier transform (FFT2) with different malicious attacks (JPEG compression, Salt & peppers noise, Gaussian noise, Rotating ,Blurring, Halftoning attack by Jarvis method). Signal to noise ratio (SNR) is computed to measure image quality for each transform for better results comparatively previous techniques of information hiding.***

KEYWORDS-- Digital Watermarking, Robust Watermarking, Copyright Protection, Fractional Fourier transform (FRFT), Fast Fourier Transform (FFT), Peak Signal to Noise Ratio (PSNR), attacks, Joint Photographic Group Expert (JPEG).

INTRODUCTION

Today‘s work is completely based on the internet, so authenticity is required to protect the content of the data because owner never wants to degrade the quality of his data. Information hiding via digital watermarks for the multimedia data is the compatible way to provide the protection of data. Watermarks are imperceptible and it is predefined pattern inserting into multimedia data to protect or authenticity. The watermark indicates that data is containing a copyright or not [1, 2]. Increase the utilization of Digital Watermark in the numerous applications such as multimedia, communication & several other applications has enhanced the requirement of an efficient method that can accumulate and convey that information. This requirement formulates the image compression & quantization an essential factor and has increased the need for efficient algorithms that can result in high compression ratio with minimum loss. Information hiding is a promising area of research in the field of electronics & communication engineering and computer aided manufacturing system [3].

Most of the cases the digital watermarking is done on gray scale images but color image watermarking can be used to improve the quality of the retrieved watermarked. Colour images can be produced by the intersection of all the three major colors R-G-B. When the intersection of the entire three watermarks has taken, then the final watermark appears to be less noisy. The digital watermarking needs of the world by concentrating on embedding the watermarks in the R-G-B colour planes of the colour images [4, 5].

Many digital watermarking algorithms have been proposed in spatial and transform domain. A simple noise in an image can eliminated the watermark, so that in this approach data security will get affected. On the other hand frequency domain based technique can embed more bits of watermark. DCT discrete cosine transformation and DWT discrete wavelet transformation are most popular. Frequency domain techniques are more robust against any attacks. Robustness of any watermark can be evaluated by applying different attacks. Most popular are rotation, cropping resize, flipping attacks etc. [4, 5, 6, 8].

Finally, the performance of the digital watermarking schemes is evaluated as tradeoffs between images embedded on it, robustness against attacks and embedding induced distortions. The remainder of the paper is organized as follows: In Section II, classification of watermarking techniques. Distortion and attacks is described in Section III. Proposed Method described in section IV and Experimental results and conclusion are presented in Sections V and VI, respectively.

CLASSIFICATION OF WATERMARK ALGORITHMS

Based on the human perception, watermark algorithms are divided into two categories [3]:

a) **Visible Watermarking (alpha>0.1):** Visible watermarking is easily perception by the human eye, means the visible watermark can be seen without the extraction process. For example it can be name or logo of the company.

b) **Invisible Watermarking (alpha<0.1):** In this watermarking mark cannot be seen by human eye. It is embedded in the data without affecting the content and can be extracted by the owner only.

Robust Watermark: If the watermark can survive after common signal processing operation such as filtering and lossy compression.

Basic Requirement for a Digital Watermark Algorithm:

All watermarks contain some important information so watermark cannot be stored in the file header because anyone from the computer can get the digital editing and would be able to convert the basic information and can remove the watermark at the same time. Thus the watermark should really be embedded to the multimedia signals [5].

Original multimedia and watermark data are the input data, watermarked data or image product by algorithm, which consist the secret key and original data.

Properties of a watermark depend on the application to be used. Thus the most important requirement for digital watermarking can be summarized by:

a) **Perceptual Transparency**: This refers to invisibility, means watermark content has the same objective quality as the original content. Watermark should not degrade the quality of the content .The watermark should be imperceptible. Sometimes watermark is embedded to data in the way that can be seen without extraction. These types of watermark are called the visible watermark. For example Logo of a company.

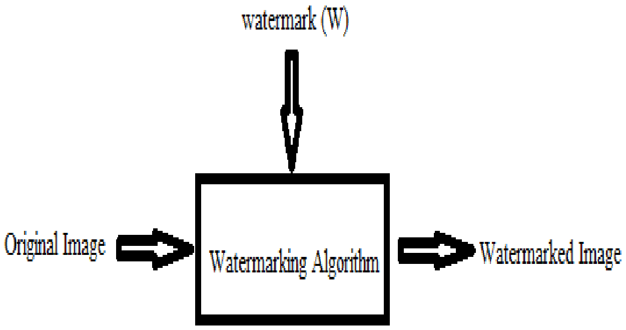

Figure 1: Watermark Embedding Process

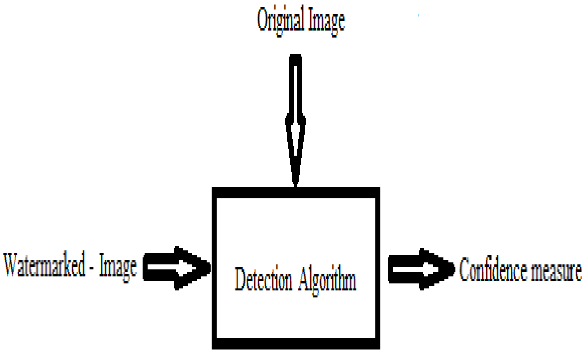

Figure 2: Watermark Extraction Process

b) **Robustness**: This refers the strength of the watermark, means nobody is able to remove, alter or damage the watermark without a secret key. A Robust watermark would be able to detectable after common signal processing operation such as lossy compression, spatial filtering, translation and rotation operation. After several steps to remove the marks that the marks should still be visible and detection which is an algorithm to detect any attempts to remove the marks. If the digital watermark is visible it is called the robust watermark and if it is not easily visible, it is called imperceptible.

c) **Security**: Security directly refers to the watermark withstand capability against attack and noise. They are directly pointed to embbed information. Secret key determine the value of watermark and the location where the watermark is embedded. It must not be possible to retrieve or even modify the watermark without knowledge of secret key.

DISTORIONS AND ATTACKS

First of all, we have to distinguish two “reasons” for an attack against a watermark image [2]:

- Hostile or malicious attacks, which are an attempt to weaken, remove or alter the watermark, and

- Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark.

Lossy image compression is considered the most common form of attack a watermarking scheme has to withstand. The harsh term “attack” can be easily justified: an efficient image compression has to suppress or discard perceptually irrelevant information the invisible watermark. A wide range of attacks has been described in the literature [2, 5, 7, 8]:

Removal attacks

Attempt to separate and remove the watermark. If somebody tries to remove the watermark from the data, this is called a removal attack. The attack is successful if the watermark cannot be detected anymore, but the image is still intelligible and can be used for a particular determined purpose [2]

.

Compression:

Practically all images currently being distributed via Internet have been compressed. The watermark is required to resist different levels of compression; it is usually advisable to perform the watermark embedding in the same domain where the compression takes place.

Proposed Jarvis Halftone Noise:

The grayscale digital image consists of 256 gray levels, while the black and white printers only have one colored ink. So, there is a need to replace wide range of grayscale pixels for printers. These 256 levels of gray should some-how be represented by placing black marks on white paper. Halftoning is a representation technique to transform the original continuous tone digital image into a binary image only of 1's and 0's consisting. The value 1 means to fire a dot in the current position and 0 means to keep the corresponding position empty.

Since the human eyes have the low pass spatial-frequency prosperity, human eyes perceive patches of black and white marks as some kind of average grey when viewed from sufficiently far away. Our eyes cannot distinguish the dots patterns if they are small enough. Instead, our eyes integrate the black dots and the non-printed areas as varying shades of gray. Figure 1(b) shows a typical halftoning image. Zooming in a part of the halftoning image, we can see that the image is actually structured by a certain strategy of distributed black dots.

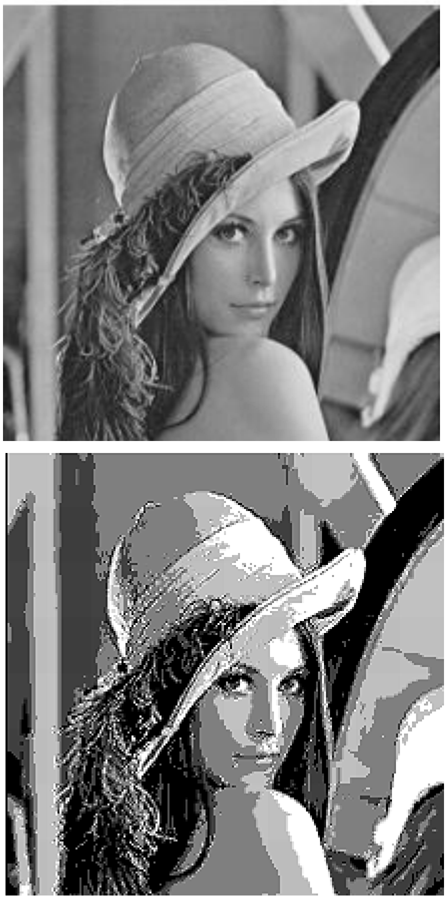

Figure 2.1: (a) The orignal image; (b) The halftoning image

I. Fractional Fourier Transformation Domain Image watermarking

Now-a-days Fractional Fourier transform has been widely used as tool in signal processing, quantum mechanics and quantum optics, pattern recognisation and study of time frequency distribution. The FRFT can be interpreted as the rotation of angle α in the time frequency plane. The basic properties of FRFT as, when rotation angle α= π/2 corresponds to the classical Fourier transform, α= 0 corresponds an Identity operator and when we apply FRFT on a signal, the signal decomposes into chirps i.e., complex exponentials with linearly varying instantaneous frequencies [9].

We use common method for embedding watermarking signals in either space or spatial-frequency domain. We can combine space/ spatial frequency domain, this type of watermarking considered image watermarking in the fractional Fourier transformation FRFT domain, here we use the combination of time and frequency domain [5, 9].

In this way, create more watermarks than in the FT or DCT domain. We use different angles for watermark embedding. This watermarking is robust on some important attacks (such as geometrical transform, filtering, histogram stretching etc.) that could be performed by a pirate. Suppose that a pirate knows watermark key and watermark key position but he can’t able to get the transformation angle without owner’s information [5].

II. Experimental Results of Proposed Technique

Original image is lena.jpg as shown fig. 3.

Fig.3: Original image

Embedding watermark image gray4.jpg as shown fig. 4.

Fig.4: Watermark image

Quality Measurements:

In order to evaluate the quality of watermarked image, the following signal-to-noise ratio (SNR) equation is used:

$$SNR_{dB} = 10\log_{10}\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I^2(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} [I(i,j) - I_w(i,j)]^2}$$

Table: Comparison between FRFT &FFT for different types of attack at Alpha=0.1

ATTACKS	FRFT (PSNR)	FFT (PSNR)
JPEG compression Q=90%	19.6008	19.5973
Halftoning attack by Jarvis method	4.0228	4.0223
Salt & peppers noise	15.6146	15.5874
Rotation	2.1913	2.1913
Blurring	17.2378	17.2378
Blur + Gaussian Noise	11.2657	11.2547

CONCLUSION

Proposed method shows in Table, watermarking process in two frequency domain FrFT and FFT techniques, we notice that the process is the same but we apply different transformation. We have applied 6 attacks at watermarked image and then extracted watermark image from watermarked Image.

The value of SNR in the table indicates that FRFT robust to blurring + Gaussian noise, halftone attack by Jarvis method, salt & peppers noise more than FFT but for other attacks are the same.

References

i. *Edin Muharemagic and Borko Furht, "Survey Of Watermarking Techniques And Applications", Department of Computer Science and Engineering, Florida Atlantic University.*

ii. *Andreja Samˇcovi´c, J´an Tur´an, "Attacks on Digital Wavelet Image watermarks", Journal of Electrical Engineering.*

iii. *Peining Taoa and Ahmet M. Eskicioglub, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", The Graduate Center, The City University of New York.*

iv. *Baisa L. Gunjal, "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms", Department of Computer Engineering, Amrutvahini College of Engineering.*

v. *Igor Djurovic, Srdjan Stankovic, and Ioannis Pitas," Digital watermarking in the fractional Fourier transformation domain", Journal of Network and Computer Applications (2001), page 167 – 173.*

vi. *Vaishali.S.Jabade, Dr.Sachin R.Gengaje "Literature Review of Wavelet based Digital Image Watermarking Techniques", International Journal of Computer Applications, Vol.31, No.1, October2011.*

vii. *P. Meerwald, A. Uhl, "A Survey of Wavelet-DomainWatermarking Algorithms", EI San Jose, CA, USA, 2001.*

viii. *Mohamed A. Suhail and Mohammad S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model", IEEE Transactions On Instrumentation and Measurement, Vol. 52, NO. 5, p.1640-1647, October 2003.*

ix. *Mahendra Kumar et. al., "Implementation of Different Non-Recursive FIR Band-pass filters using Fractional Fourier Transform" in proceedings of 4th IEEE International Conference on Computational Intelligence and Communication Networks (CICN-2012), Mathura, 3-5 Nov. 2012.*

x. *Mahendra Kumar et. al., "Digital image watermarking: A survey", International Journal of Engineering and research applications (IJERA), Jul-Aug, 2013.*

xi. *Mahendra Kumar et.al.," Digital Image Watermarking using Fractional Fourier transform via image compression", In IEEE International Conference on Computational Intelligence and Computing Research 2013, 26-28 Dec., 2013.*