A Review On Watermarking Techniques And Its Applications

Jyoti Hazrati and Kavita Rawat,
hazratijyoti@gmail.com,kavirawat93@yahoo.in

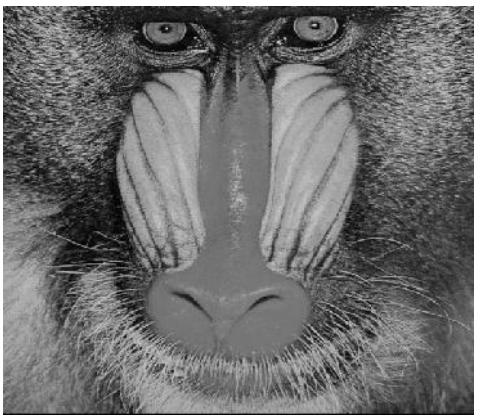
ABSTRACT : Due to the rapid and extensive growth of e-publishing, data can now be distributed much faster and easier. Unfortunately, we can still see many technical challenges in discouraging unauthorized copying and distributing of electronic documents. One potential solution for claiming the ownership is to use electronic stamps or so-called digital watermarks. A digital watermark is a "secret key dependent" signal "inserted" into digital multimedia data. Watermark can be later detected/extracted in order to make an assertion about the data. A digital watermark can be-Visible (perceptible) and Invisible (imperceptible).There are a big variety of methods which were devised to the ends mentioned above. We describe the implementation of different methods widely being used in watermarking process and our basic focus is on theoretical implementation of Fractional Fourier transform which is the best method for watermarking. Analysis have shown that implementation of FRFT increases the privacy of data by a large extent. This implementation speeds up the classical code by an average factor from 2 to 4.

Keywords: **Fractional Fourier Transform, COX watermarking, Wavelet watermarking.**

I. INTRODUCTION :

Watermarking is a technique used to hide data or identifying information within digital multimedia. This discussion will focus on the watermarking of digital images through many ways such as digital video, audio, and documents are also normally watermarked. Digital watermarking is becoming popular now a days, especially for adding undetectable identifying marks, like the author or copyright information. Because of this use, evaluation of watermarking techniques is done on the basis of their invisibility, recoverability, and robustness. In this manuscript, we have implemented techniques and evaluated its susceptibility to attack by various image processing techniques. The fractional Fourier transform is well known and has many applications. In this short report we shall only be interested in theoretical implementation of different techniques widely being used for watermarking . Therefore we restrict ourselves to the essentials of the theory. Digital watermarking can be classified into two classes depending on the domain of watermark insertion : the spatial domain and the frequency-domain watermarking. It is easy to implement Spatial domain watermarking and requires no original image for detection of watermark. Sometimes, it fails under signal processing attacks .Besides, the quality of the original image data can be severely degraded since the watermark is directly applied on the pixel values. Frequency domain watermarking provides more protection under most of the signal processing attacks. But existing frequency-domain watermark algorithms require the original image for comparison in the process of watermark retrival, which is not practical for a huge image database.

Original Image



Watermark

II. Watermark Attacks :

- Active Attacks.

a. Hacker attempts to remove or destroy the watermark.
b. Watermark detector unable to detect watermark.
c. Not serious for authentication or covert communication.

- Passive Attacks.

a. Hacker tries to find if a watermark is present.
b. Removal of watermark is not an aim.
c. Seriousforcovert communications.

- Collision Attacks.

a. Hacker uses several copies of watermarked data (images, video etc.) to construct a copy with no watermark.
b. Uses several copies to find the watermark.
c. Serious for fingerprinting applications.

- Forgery Attacks.

a. Hacker tries to embed a valid watermark.
b. Serious in authentication.
c. If hacker embeds a valid authentication watermark, watermark detector can accept the updated media.

III. Watermark Embedding :

First lets give some notations that are used later. *X*: the original gray-level image. *W*: the digital water mark. Since only the middle-frequency range of the host image will be processed during the watermark embedding, the size of a watermark image *W* is assumed to be smaller than that of the original image *X*.

Step 1. We divide the original image *X* and the water mark *W* into blocks. For example, blocks with size 8×8 pixels for *X* and blocks with size pixels for *W*.

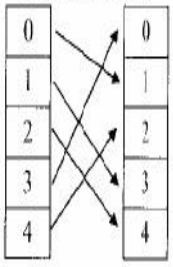
Step 2. To survive cropping of picture, each watermark block is need to be dispersed over its corresponding image block, since without appropriate adjustment for the spatial relationship of the watermark, a simple picture-cropping operation can be used to eliminate the watermark.

Step3.To enhance the perceptual invisibility, the features of the original image should be considered. In effect, watermark blocks which have more information (more detail, more complex content) should be embedded in image blocks which have more information. To this end, for each image block of size 8×8 and each watermark block of size 8*8. These variances are then sorted and blocks are matched according to the magnitude of variance.

Index of image block	Variances
4	33.2
0	30.5
3	22.2
1	16.7
2	8.2

Index of watermark block	Signed pixels No.
2	10
3	8
1	7
0	3
4	2

Permutation mapping of the watermark block



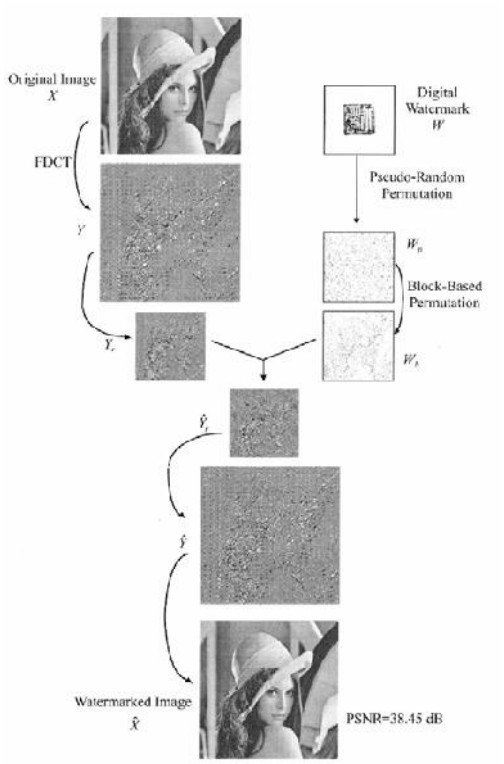


Fig. 5. Watermark embedding steps.

Step 4. Discrete cosine transform (DCT) is performed on blocks of image *X*. Each block is independently DCT transformed .
Y= FDCT(*X)*

Where FDCT denotes the operation of forward DCT.

Step 5. Now we need to extract out the middle-frequency coefficients from *Y*. The reason that why middle-frequency coefficients are used is two folded. First, the human eye is more sensitive to noise in lower frequency components than in higher frequency one, so we should not put the watermark in low frequencies, otherwise visible artifacts would arise after watermark embedding. Second, the information hidden in the higher frequency components might be discarded after quantization operation of lossy compression. Therefore, for invisibly embedding the watermark that can be survive lossy data compression, a reasonable trad-off is to embed the watermark into the middle-frequency range of the image.

Step 6. Now, a permuted digital watermark and a reduced image both with size 21*MM*× are obtained.Actually, we chose to embed each watermarked pixel by modifying the polarity between the corresponding pixels in neighboring blocks, which is an effective way to achieve the invisibility and survival for low compression ratio of JPEG.

Step 7. Finally, map the modified middle-frequency coefficients into *Y* to get *rY*ˆ*Y*ˆ. Then, inverse DCT (IDCT) is performed on the associated result to obtain the embedded image.
Xˆ= FDCT(*Y^)*

IV. Watermark Extraction

The extraction of watermark requires three things:1. original image 2. the watermarked image 3. the watermark or the permutation mapping.

Step 1. Both the original image X and the image in question $\tilde{X}$ are DCT transformed.

Step 2. Generate the reduced images which contain only the middle-frequency coefficients and then use these middle-frequency DCT coefficients to produce the polarity patterns.

Step 3. Perform **XOR** operation on the two polarity patterns to obtain a permuted binary data.

Step 4. Reverse block-based image-dependent permutation and reverse pseudorandom permutation. Thereafter, we can get the embedded watermark.

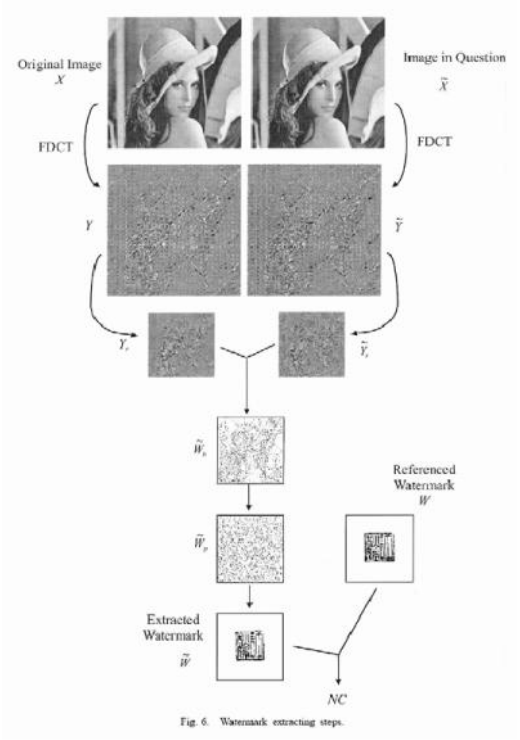


Fig. 6. Watermark extracting steps.

V. TECHNIQUES :

1.FRACTIONALFOURIER TRANSFORM :

Till now, many people had applied techniques like LAPLACE TRANSFORM and FOURIER TRANSFORM for watermarking in images. Laplace transform works in frequency domain whereas Fourier transform works in time domain. In both these techniques, data is dependent on only one variable. So, its very easy to crack the data . A new technique called FRACTIONAL FOURIER TRANSFORM has also been developed which is known by very less number of people. This technique works on both the domains i.e. Time domain and Frequency domain. So, it becomes quite almost impossible for the third party to crack the data . The proposed scheme is based on the consideration that an image is as an element of a vector space, that may be expressed as a linear combination of the elements of any orthogonal basis of this space. Accordingly, the image is analyzed in orthogonal basis prior to the watermark embedding. Image representation by a subset of coefficients facilitates image component selectivity, which can be used so as to exclude the image components mostly affected by the presence of noise. The proposed scheme is robust under the presence of additive noise, as it is concluded from the results of the experimental evaluation performed. In FRFT method, original image is divided into two parts, one is the image portion which is to be displayed completely and other portion which to be completely hidden. The portion of the image which is to be kept visible is divided into integer array and this array is kept as it is. The FRFT algorithm is applied on the matrix which is to be kept hidden. Then the modified matrix extracted after the algorithm operation is added to the original image integer matrix .A multiplier is used to decrease the visibility of the watermark. This multiplier generally lie between 0 an 1 so as to lower down the visibility of hidden data. As the value of multiplier is increased , the visibility extent of the watermark goes on increasing.

4 LSBs Watermarked

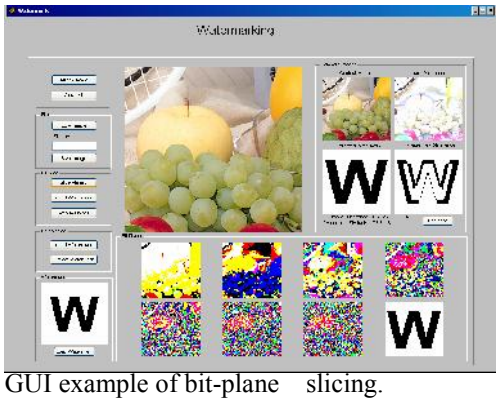
7 LSBs watermareked

2.COX METHOD AND BIT-PLANE METHOD FOR WATERMARKING :

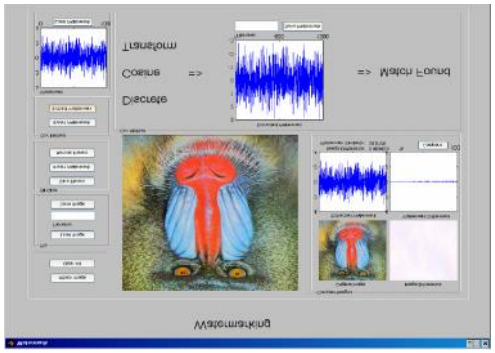
There are a multitude of different methods by which are used for image watermarking. The Cox method and the bit-plane method allow to take two very different approaches to watermarking. Bit-plane slicing approach is designed to work primarily as a fragile

watermark. It shows the degree to which changes are made to an image. The second one,on the other hand, is designed to be robust. It works in the frequency domain, allowing it to pursue resistance for many common attacks to the image.

In implementing these methods, we had to learn and create the processes to add a watermark and extract a watermark from digital images. To evaluate the degree to which watermarking affects the original image, the GUI was designed to show the image difference graphically as well as numerically in a relative error format. This helps the user evaluate the invisibility of the watermark, as they can compare the changes made by watermarking to the original image. When the watermark is extracted from an image, the difference between the watermarks is also shown both graphically and numerically. This will help the user decide if a watermark can be consistently recovered with the given method.



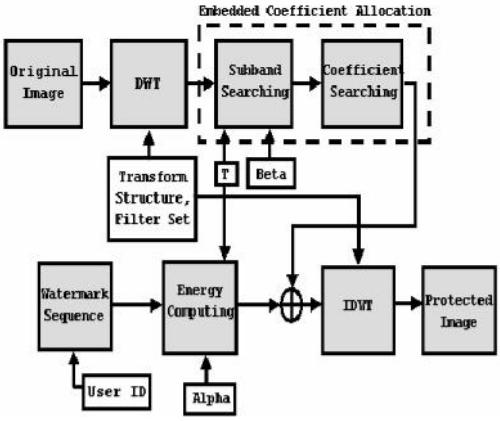
GUI example of bit-plane slicing.



AN EXAMPLE OF COX WATERMARKING

3.WAVELETBASED WATERMARKING:

An adaptive watermark casting method is developed to determine significant wavelet subbands and then select a couple of signicant wavelet cofficients in these subbands for watermark embedding. A blind watermark retrieval technique that can detect the embedded watermark without the help from the original image is proposed.



VI. Applications of watermarking:

- Proof of ownership.
- Copy prevention or control.
- Content protection (visible watermarks).
- Media Bridging
- Broadcast Monitoring

VII. Summary:

Till now we have mentioned various techniques in order to hide some data or information from being cracked by unauthorized people. Out of these, Fourier and Laplace Transform are widely being used for hiding the data. In this report, we have enhanced the advantages of using fractional fourier transform to replace the techniques being used. This technique must be implemented widely as it works both in frequency and time domain so making data more secure from unauthorized access. Other methods used were Cox method and Bit plane method where Cox method is far more robust than bit-plane slicing method. There are some cases that where the Cox method failed to produce an extractable watermark were cropping attacks. We hope that this data will be helpful for those who are interested in watermarking techniques.

III. References:

[1] Cox, I., M. Miller and J. Bloom, 2002. Digital Watermarking, Academic Press, USA

[2] Langelaar, G., I. Setyawan and R. Lagendijk, 2000. "Watermarking Digital Image and Video Data: A State-of-Art Overview," IEEE Signal Processing Magazine, 17(5):20-46.

[3] Voloshynovskiy, S., S. Pereira and T. Pun, 2001. "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks," Comm. Magazine, 39(8): 118-126.

[4] H.M. Ozaktas, Z. Zalevsky, M. Kutay, The Fractional Fourier Trans- form, John Wiley and Sons, New York, NY, 2001.

[5] J. Guo, Z. Liu, S. Liu, Watermarking based on discrete fractional rando