Digital Image Watermarking: A Survey

Roma Rewani[1], Mahendra Kumar [2], Aditya Kumar Singh Pundir [3]

Department of Electronics[1, 2, 3]
JNU Jaipur[1], Mewar University Gangrar[2], JNU Jaipur [3]
Rajasthan, India

ABSTRACT

Recently, works are completely based on the internet, so authentication 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.

Many digital watermarking algorithms have been proposed in spatial and transform domain. The performance of the digital watermarking schemes is evaluated as tradeoffs between number of bits embedded on it, robustness against attacks and embedding induced distortions. This work provides a review of information hiding techniques of Digital image watermarking.

Keywords: *Digital Watermarking, Robust Watermarking, Copyright Protection, Fractional Fourier transform (FRFT), Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), Peak Signal to Noise Ratio (PSNR), attacks, Joint Photographic Group Expert (JPEG).*

I. 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 number of bits embedded on it, robustness against attacks and embedding induced distortions.

II. Classification of Watermark Algorithms

In this section we discuss different classification of watermarking algorithm [1, 2].

Firstly, According to type of document, watermarking technique can be divided into four groups:

a) Text watermarking
b) Image watermarking
c) Audio watermarking
d) Video watermarking

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

a) **Visible Watermarking:** Visible watermarking are 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:** 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.

Third watermark algorithms are classified based on information for detection [1, 2, 3]:

a) **Blind or public watermarking:** In public watermarking during the process of watermark detection we required only secret key. Here,we do not need the original image.For example : Copy control applications must send different watermarks for each user and receiver must be able to recognize

b) **Non blind or private watermarking:** In private watermarking original signal is required for detection of the watermark.

c) **Semi–blind watermarking:** In semi blind watermarking sometimes it may need some extra information for detecting the watermark. Here some extra information required to access the original signal just after adding the watermark.

Fourth, Classification based according to the additional feature 'robustness':

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

b) **Fragile watermark:** A fragile watermark should be able to be detected any change in signal and also possible to identify the signal before modification.

c) **Semi-Fragile Watermark:** Semi fragile watermark are very sensitive in nature. They can be change to a watermarked image.

Finally based on Embedding processing domain, watermark technique can be divided into:

a) **Spatial Domain:** Spatial domain refers to the image plane itself means watermark data to be embedded in the pixel value. In this method use some minor changes in pixel value intensity. Spatial domain technique is having least complexity and high payload over they cannot withstand low pass filtering and common image processing attacks.

b) **Transform Domain:** Transform domain have imperceptibility as well as robust. Transform domain is also called frequency domain because value of frequency can be altered from there original value.

c) In this approach low frequency component of image data should be modified in according to the watermarked data in a robust way through the transform domain techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

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.

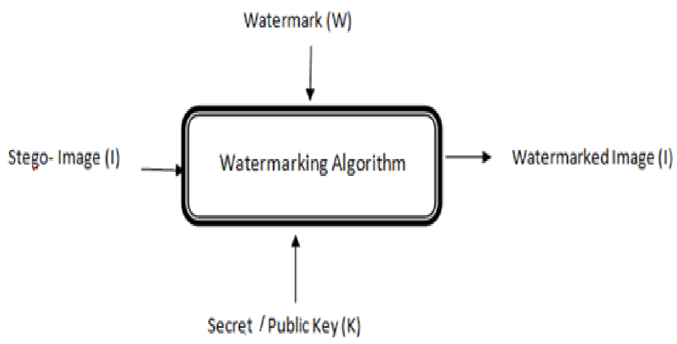

Figure 1: Watermark Embedding Process [1, 2]

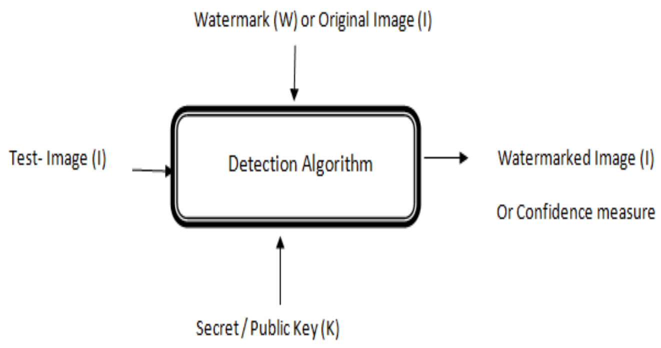

Figure 2: Watermark Extraction Process [1, 2]

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.

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.

III. DISTORIONS AND ATTACKS

First of all, we have to distinguish two "reasons" or "purposes" 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. Many such attack operations have been proposed [2]:

- Lossy image compression (JPEG, JPEG 2000)
- Addition of Gaussian noise
- Denoising
- Filtering
- Median filtering and blurring
- Signal enhancement (sharpening, contrast enhancement)

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. For instance, the Discrete Cosine Transform (DCT) domain image watermarking is more robust to Joint Photograph Expert Group (JPEG) compression than the spatial-domain watermarking. Also, the Discrete Wavelet Domain (DWT) domain watermarking is robust to JPEG 2000 compression.

Additive noise: a random signal with a given distribution (e.g. Gaussian, uniform, Poisson, Bernoulli) is added to the image unintentionally.

Denoising: It explore the idea that a watermark is an additive noise (which can be modeled statistically) relative to the original image. These attacks include: local median, midpoint, trimmed mean filtering, Wiener filtering, as well as hard and soft thresholding.

Filtering attack: it's linear filtering: high-pass, low pass, Gaussian and sharpening filtering, etc. Low-pass filtering, for instance doesn't introduce considerable degradation in watermarked images, but can dramatically affect the performance since spread-spectrum-like watermarks have non negligible high-frequency spectral contents. To design a watermark robust to a known group of filters that might be applied to the watermarked image, the watermark message should be designed in such a way to have most of its energy in the frequencies which filters change the least.

IV. 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].

V. DWT Domain Image Watermarking

Wavelet transform is a time domain localized analysis method with the window’s size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. It can distill the information from signal effectively. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district .Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. The following figure represents the watermarking system in DWT [3, 6, 7].

VI. DCT Image watermarking

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT. It’s referred as ‘Energy compaction Property’ [6].

As DCT is having good energy compaction property, many DCT based Digital image watermarking algorithms are developed. Common problem with DCT watermarking is block based scaling of watermark image changes scaling factors block by block and results in visual discontinuity [9]. In this chapter, we propose a visible watermarking technique that modifies the DCT coefficients of the host image using eqn. (1). We call an embedding factor we try different values for it to achieve visible watermarking we find α =10 a good value and we also use α =0.09 for invisible watermarking. We have also proposed a modification to make the watermark more robust [8].

VII. Conclusion

In this paper, we discuss watermarking process in three frequency domain DWT, DCT and FRFT, we notice that the process is the same but we apply different transformation techniques, also we can note that the two method have the same robust for all types of attack except blurring we can note that FRFT more robust than DCT.

The value of PSNR shows the FRFT robust to blurring attack more than DCT but for other attacks are the same.

References

[1] Edin Muharemagic and Borko Furht, “Survey Of Watermarking Techniques And Applications”, Department of Computer Science and Engineering, Florida Atlantic University.

[2] Andreja Samˇcovi´c, J´an Tur´an, “Attacks on Digital Wavelet Image watermarks”, Journal of Electrical Engineering.

[3] 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.

[4] Baisa L. Gunjal, “An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms”, Department of Computer Engineering, Amrutvahini College of Engineering.

[5] 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.

[6] 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.

[7] P. Meerwald, A. Uhl, “A Survey of Wavelet-DomainWatermarking Algorithms”, EI San Jose, CA, USA, 2001.

[8] 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.

[9] 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.