

Analysis of Watermarking Techniques

Gunjan Malik

M.Tech Student, Computer Science Engineering
NorthCap University, Haryana
India

Tarun Kumar

Lecturer
Government Polytechnic College Amroha, UP
India

ABSTRACT

With the widespread use of Internet, transfer of digital data online is enormous. This leads to easy accessibility and vulnerability to attacks of copyrighted content on large scale. Digital data in form of videos, audios, text, images can easily be manipulated, forged and redistributed for profits. To overcome this problem and protect copyrighted content, Digital Watermarking emerged as a useful solution. This paper talks about the literature survey of different watermarking techniques and showcase the comparative description of superiority of one technique over the other.

Keywords

Digital watermarking, DFT, DCT, DWT, Spatial domain, frequency domain, Comparative analysis.

1. INTRODUCTION

With the enhancement of technology, use of digital data is increasing enormously. With the transfer of digital data electronically, the protection of data authenticity and copyright protection has become cumbersome. To deal with this issue one can embed some information in the data which is preferably known as watermarking [1]. Watermarking is most widely used technique to save data from forgery and other non-authentic usage. It prevents claiming of content ownership unauthentically by some third party. In this paper, we are describing different watermarking techniques available and its usage and comparisons among them. We have organized the paper in below sections. Section II will describe various types and classification of watermarking while watermarking techniques are described in section III. Description of historical implementation of the watermarking techniques as per survey is given in section IV. Section V describes the comparative analysis among techniques.

2. CLASSIFICATION OF WATERMARKING

Watermarks are codes which can be in form of text, binary data, numerical data and images or can be signatures. They contain piece of information such as owner's details or origin source that can be embedded in the digital data. They help in safeguarding the intellectual property and creative content which is present in digital form. Watermarking can be of different forms (see Figure 1). Watermark can be embedded in the form of signals if host data is audio or it can be inserted inside the host data in form of text, image or video frames [2]. Watermark can be visible or non-visible, on this factor watermark can be classified into two categories: Visible watermark and non-visible watermark [3]. Visible watermark generally being used to put logo on the data. They are visible to human eye. While in invisible watermark technique watermark is in form of text, image or signature and watermark is invisibly inserted inside the host data. Invisible watermarks can be Fragile or Robust in nature. Fragile watermarks are generally added into digital media with the

aim to detect if any attack was made on the data to destroy the watermark or not, whereas, robust watermarks are robust against several attacks and the information hidden inside the watermark is retained even after attack.

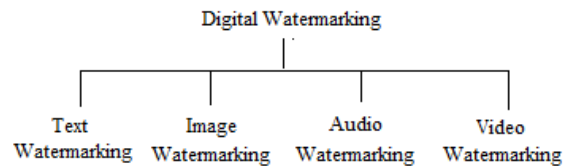


Figure 1: Types of Watermarking

3. WATERMARKING TECHNIQUES

Watermark can be applied either in spatial domain or in frequency domain as shown in Figure 2.

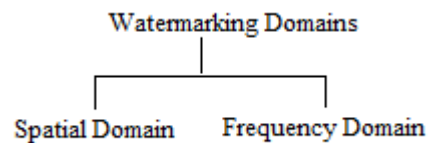


Figure 2: Domains of Watermarking

In Spatial domain, the watermark is applied by modifying pixel values of the host image while the transform coefficients are altered for embedding watermark in frequency domain [4]. Frequency domain is widely used, in comparison to spatial domain due to its robust nature and maintaining the imperceptibility of original image intact.

3.1 Spatial Domain

Two commonly used techniques in spatial domain are: Correlation based technique and Least Significant Bit Modification scheme [2]. This technique is conceptually simple and uses less computational intricacies, hence, suitable for video watermarking where real-time performance is prime goal. However, it is incompetent to attacks, poor imperceptibility and less robust [9].

3.2 Frequency Domain

Commonly used transforms are Discrete Fourier Transformation (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT).

3.2.1 DCT

In DCT, middle frequency bands are the primarily focused zone for watermark embedding after dividing the original image/video frame into sub-bands of lower and higher resolutions. It can be implemented in $O(n \log n)$ operations, thereby, giving faster results. It can overcome attacks such as low pass filtering, blurring, sharpening, but weak against attacks such as rotation, cropping or scaling. Few of the

applications where DCT is applied include fingerprint identity, employee i-cards, pan cards, or medical imaging areas [4].

3.2.2 DWT

In DWT, the image is divided into sub images in hierarchical fashion [4] as lower (LL) and higher resolutions (Horizontal HL, Vertical LH and Diagonal HH) frequency bands. DWT supports multi-resolution characters; hence, it is widely used. Few of the applications where DWT is widely used include government applications, military applications, bank applications or broadcast monitoring [4]. DWT coefficient's magnitude is smaller for other higher bands (HH, LH, and HL) [5][6] and is larger in the lowest bands (LL) at every decomposition level. Embedding watermarks in lower frequency bands leads to enhanced robustness to attacks.

3.2.3 DFT

In DFT, continuous functions are converted into frequency components [2]. It is robust against geometric attacks such as scaling, translation, cropping and rotation. It is better than DCT, DWT or spatial domain as they are not robust and invariant to geometric attacks.

4. HISTORICAL IMPLEMENTATION OF TECHNIQUES

In paper "Evelyn Brannock: Watermarking with Wavelets: Simplicity leads to Robustness" [1], Evelyn used Discrete Wavelet Transform (DWT) technique in frequency domain to implement digital watermarks. 2-dimensional DWT decomposes the digital image into sub-images. The digital image is thus separated into lower and higher resolution bands. The watermark is then embedded inside the high resolution band as it is less sensitive to human vision thus increasing robustness. The watermark can then be extracted from the watermarked image using the 2-dimensional inverse DWT. The experimental result proved that when testing on Embedding watermarks with/without noise, and extracting watermarks with/without noise, Haar wavelet gave better results than other watermarking transforms.

In paper "Luigi Ros: High capacity Wavelet watermarking using CDMA multilevel codes", [7] Luigi Ros used CDMA and multilevel code technique to implement the watermark. Initially, DWT in frequency domain is applied on the host image which separates it into lower resolution and higher resolution bands (horizontal, vertical and diagonal) sub images. Then, multilevel CDMA algorithm is applied for wavelet based watermarking scheme. This technique gave robust results against attacks such as filtering, cropping and compression.

In paper "Salwa A.K Mostafa: Video watermarking scheme based on PCA and wavelet transform", Salwa A.K Mostafa, [8] used binary logo watermarks to embed into video frames by using the concept of linear transform PCA and discrete wavelet transform. The video is divided into video frames and then on each frame DWT is applied to get two frequency bands (LL-HH). Next PCA is applied to provide complete decorrelation among bands thus enabling data hiding. Lastly, binary watermark is inserted into the luminance parts of PCA components of LL and HH blocks. In this paper, lowest and highest frequency bands are chosen to apply PCA and to embed watermark. Later to achieve the watermarked image, inverse PCA and inverse DWT is applied. To perform watermark extraction, the watermarked image and the original referenced image is taken and compared and the watermark is extracted. To check the robustness of the image, wide range of

attacks such as MPEG coding, JPEG coding, Gaussian noise addition, contrast adjustment, cropping, resizing, rotation, sharpen filters, etc. are applied.

In paper "Maria Chroni: Watermarking images in frequency domain by exploiting self-inverting permutations", [10] Maria Chroni used integer type watermark to embed in host image in frequency domain using DFT technique. Firstly, integer is converted into a self-inverting permutation giving representation of 2-D object. Next, Discrete Fourier transform (DFT) using FFT is applied to get cosine and sine components. Then, the integer watermark is embedded inside the high frequency band area by modifying the magnitude values of the coefficients and the watermarked image is obtained. For extracting the watermark, the marked areas are located and the watermark is reconstructed.

In paper "Maria Chroni: Watermarking images using 2D representation of self-inverting permutations", [11] spatial domain is used to embed numerical watermarks in digital images. Firstly, the integer watermark is converted into self-inverting permutation using the concept of Bitonic Permutations. Next the watermark is embedded into the host image in spatial domain by modifying the pixel values which are undetected by human vision.

In paper "Mohamed RADOUANE: Robust Method of Digital Image Watermarking using SVD Transform on DWT Coefficients with Optimal Block" [12], Mohamed watermark image is undergone DWT and SVD transformation before it's getting embedded into the original image which has been already altered by SVD transformation on the maximum entropy blocks obtained from the usage of DWT. This technique makes the watermark more robust against the attacks as watermark is applied on the maximum entropy blocks only.

In paper "Jeril George: Color Image Watermarking using DWT-SVD and Arnold Transform", original and watermark images first split into RGB channel to act as input for further embedding process. DWT and SVD has been applied on the blue channel of the original image while first Arnold transformation has been applied on blue channel of watermark image which in turn act as key (available to owner and distributor). After Arnold transformation, SVD has applied on watermark image and then watermark image is embedded into the original image. The usage of key while extracting the watermark makes this technique as semi blind technique [13] and makes it robust against the attacks. Another advantage of using Arnold transformation is that there is no need of original image while extracting the watermark.

5. COMPARISON OF TECHNIQUES

Following section shows the comparison among DCT, DFT and DWT and how DWT overpowers other techniques.

From the survey on different watermarking techniques, the result is DWT is more robust than other Techniques even though it involves computational complexities. DWT has unique frequency regions whereas DCT and DFT are full image/video frame transforms [7]. It implies that if any change is made in the transform coefficients, then the entire image will be affected in case of DCT and DFT whereas, in DWT, only the modified part of image will be affected locally and not the entire image. Also, DWT method yields more robust results than DCT, DFT as in DWT; the image is hierarchically divided into lower and higher bands. The lower LL band can then be further sub divided into four sections

giving 2-level DWT and so on. Thus, watermark can be embedded in 2nd or further level of DWT [8]. Also, human visual system (HVS) can be accurately modeled using wavelet transform as compared to other transforms which allows embedding higher energy watermarks in those regions where HVS is less sensitive [9]. DWT fits in well for scaling and geometric attacks in comparison to DCT technique. Another advantage of DWT is that since it facilitates viewing of image in multiple resolutions, hence, the internal details of the original image can be viewed from different levels if remain undetected at one level.

Table 1. Comparison Between Spatial Domain And Frequency Domain

Spatial Domain	Frequency Domain
Simple technique to use by modifying pixel values	Complex to use by modifying transform coefficients
Lack Imperceptibility	High imperceptibility
Less robust, incompetence in dealing with a range of attacks	More robust against different types of attacks
Restricted capacity of an image to hold the watermark	High capacity to hold watermark
Involves less computational cost	High computational cost involved
Poor performance suitable only for video watermarking where video quality is given priority over robustness to attacks.	Better performance and results

It should be noted here that, performing watermarking in high frequency band tends to be less robust but has lesser effect on the quality of original image, while performing watermarking in low band will achieve better robustness but at the expense of significant alteration to the original image. Thus, a mid-band scheme is used since it can provide a good trade-off between the imperceptibility and robustness as in DCT technique. Hence, frequency domain is better than spatial domain for Watermarking Techniques.

6. CONCLUSION

In this paper we have tried to showcase the concept and importance of watermarking. A survey of different watermarking techniques based on historical researches that can be used for copyright protection of digital data is presented. These techniques can be classified into many categories based on different domains. We have also discussed the advantages and disadvantages of the techniques and highlighted the comparisons among them. The results indicate that frequency domain is more robust than spatial domain and DWT technique outperforms other transforms in terms of performance, imperceptibility and robustness against attacks.

7. REFERENCES

- [1] Evelyn Brannock, Michael Weeks, Robert Harrison, "Watermarking with Wavelets: Simplicity Leads to Robustness", 978-1-4244-1884-8/08/\$25.00 ©2008 IEEE.
- [2] Ekta Miglani, Sachin Gupta "Digital Watermarking Methodologies - A Survey", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcse.com Volume 4, Issue 5, May 2014.
- [3] Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi "A New Robust Digital Image Watermarking Technique Based On Joint DWT DCT Transformation", Third 2008 International Conference on Convergence and Hybrid Information Technology, 2008 IEEE.
- [4] Radhika v. Totla, K.S.Bapat, "Comparative Analysis of Watermarking in Digital Images Using DCT & DWT", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.
- [5] Ying Zhang, Jiqin Wang, Xuebo Chen, Watermarking Technique Based On Wavelet Transform For Color Images, 2012 IEEE.
- [6] Qing Liu, Jun Ying Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis" 2012 IEEE.
- [7] Luigi Rosa, "High Capacity Wavelet Watermarking using CDMA Multilevel codes", Via Paolo della Cella 3, 10139, Turin, ITALY.
- [8] Salwa A.K Mostafa, A. S. Tolba, F. M. Abdelkader, Hisham M. Elhindy "Video Watermarking Scheme Based on PCA and DWT", International Journal of Computer Science and Network security, VOL.9 No.8, August 2009.
- [9] Dr.Nasseer Moyasser Basheer, Shaimaa Salah Abdulsalam, "Watermarking Algorithm in DWT using HVS Characteristics", The Fourth Scientific Conference of the College of Computer Science & Mathematics, Iraqi Journal of Statistical science 2011.
- [10] Maria Chroni, Angelos Fylakis, and Stavros D. Nikolopoulos, "Watermarking images in Frequency domain by exploiting self-inverting Permutations".
- [11] Maria Chroni, Angelos Fylakis, and Stavros D. Nikolopoulos, "Watermarking images using 2D representation of self-inverting permutations".
- [12] Mohamed RADOUANE, Rochdi MESSOUSSI, Raja TOUAHNI, Tarik BOUJIHA, "Robust Method of Digital Image Watermarking using SVD Transform on DWT Coefficients with Optimal Block", 2014 IEEE.
- [13] Jeril George, Satishkumar Varma, Madhumita Chatterjee, "Color Image Watermarking using DWT-SVD and Arnold Transform", 2014 IEEE.