Contrast of Watermarking Techniques in different domains

Mansi Hasija[1] ,Alka Jindal[2]

**[1] PEC , University of Technology
Chandigarh, India**

**[2] PEC , University of Technology
Chandigarh, India**

Abstract

Digital watermarking has gained a lot of importance for digital media recently. It deals with hiding secret bits of information with a digital content as a cover. This is very useful for many applications like copyright control, authenticity of documents, captioning, broadcast monitoring etc. Various techniques for watermarking have been proposed in the recent past. The brief discussion of some techniques with their results are presented in this paper which forms the basis of comparison between these techniques.

Keywords: *Watermarking, DCT,DWT*

1.Introduction

Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. With digital multimedia distribution over World Wide Web, Intellectual Property Right (IPR) are more threatened than ever due to the possibility of unlimited copying. One solution would be to restrict access to the data using some encryption technique .However encryption does not provide overall protection. The above problem can be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership. The same "watermarking" concept may be used in multimedia digital contents for checking the authenticity of the original content. This technology embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected. Continuous efforts are being made to device a good watermarking scheme.The following paper is divided into Sections. Section 2 describes Digital Watermarking technology. Section 3 the various watermarking techniques .Section 4 watermarking techniques are compared. Section 5 conclusion is described.

2. Digital Watermarking

Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. This kind of watermark contains the author and user's information, which could be the owner's logo, serial number or control information[1]. Watermarking has found use in many application fields: copyright protection, content indexing, data monitoring and tracking, and data authentication. In next subsections we discuss the watermark embedding and extraction procedure, different domains for watermark embedding and parameters to evaluate the performance of a watermarking technique.

2.1 Watermark Embedding and Extraction

A watermarking algorithm embeds a visible or invisible watermark in a given multimedia object. The embedding process is guided by use of a secret key which decided the locations within the multimedia object (image) where the watermark would be embedded.

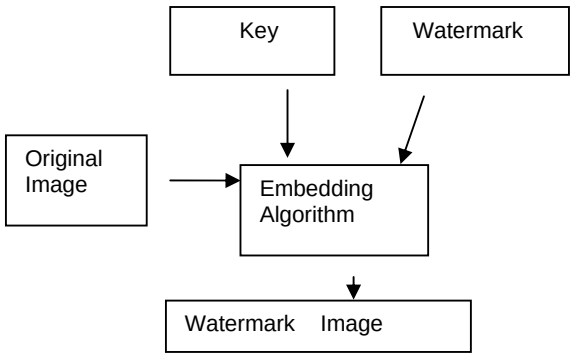

Figure1: Watermark Embedding

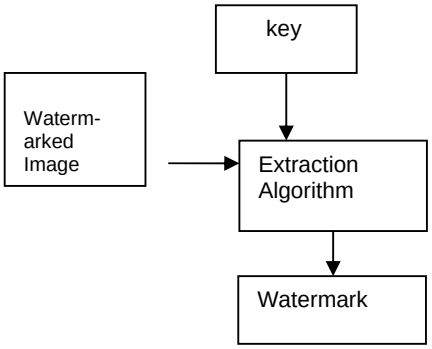

Figure 2: Watermark Extraction

For watermark extraction we use the key and watermarked image to extract the watermark.

2.2 Watermarking Domains

Based on their embedding domain, watermarking schemes can be classified either as Spatial Domain (The watermarking system directly alters the main data elements, like pixels in an image, to hide the watermark data) or Transformed Domain (the watermarking system alters the frequency transforms of data elements to hide the watermark data). The latter has proved to be more robust than the spatial domain watermarking.

Some spatial domain watermarking techniques like LSB are generated a watermark using an m-sequence generator. The watermark was embedded to the LSB of the original image. The watermark, however, was not robust to additive noise.
Described the patch work algorithm, it chooses randomly n pair of image point (ai,bi) and increased the ai by one, while decreased the bi by one. The watermark was detected by comparing the sum of the difference of ai and bi of the n pairs of the points with 2n provided, certain statistical propriety like image intensity are uniformly distributed. The scheme is extremely sensitive to geometric transformation

To transform an image to its frequency representation, one can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT) . Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies)
One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (FM) of an 8x8 DCT block as shown in figure 3 .

FL	FL	FL	FM	FM	FM	FM	FH
FL	FL	FM	FM	FM	FM	FH	FH
FL	FM	FM	FM	FM	FH	FH	FH
FM	FM	FM	FM	FH	FH	FH	FH
FM	FM	FM	FH	FH	FH	FH	FH
FM	FM	FH	FH	FH	FH	FH	FH
FM	FH	FH	FH	FH	FH	FH	FH
FH	FH	FH	FH	FH	FH	FH	FH

Figure 3: DCT block

FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image.

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in figure 4

<table>
<tr><td>LL_2</td><td>HL_2</td><td rowspan="2">HL_1</td></tr>
<tr><td>LH_2</td><td>HH_2</td></tr>
<tr><td colspan="2">LH_1</td><td>HH_1</td></tr>
</table>

Figure 4 : 2 Scale 2 Dimensional DWT

The Fourier Transform DFT is an important image processing tool which is used to decompose an image into its sine and cosine components. DFT of a real image is generally complex valued, which results in the phase and

magnitude representation of an image. The strongest components of the DFT are the central components which contain the low frequencies. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions.

2.3 Paramaters for Evaluation of a watermarking technique

The peak signal to noise ratio (PSNR) is used to evaluate the image quality by calculating the mean square error (MSE) between the images to compare.

$$MSE = \frac{1}{N} \sum (X_p - Y_p)^2$$

Where p is the unity of the N pixels in the image. x and y are the grayscale of the images to compare.
With above information we calculate PSNR by equation where X_{max} is max luminance (i.e. for 8-bit image, $X_{max} = 255$).

$$PSNR = 10 \log_{10} \frac{(X\_max)^2}{MSE}$$

We calculate PSNR between original watermark and watermark that is extracted from host image after attack. The higher the PSNR shows the better quality of extracted watermark. So, if we have bigger PSNR, it shows least difference between original and extracted watermark and more robustness against attack.
The accuracy rate AR is defined as

$$AR = \frac{CP}{NP}$$

Where NP is the number of pixels of the watermark image and CP is the number of correct pixels in the watermark image that is retrieved from the attacked image

3. WATERMARKING TECHNIQUES

In [1] a spatial watermarking technique for gray scale images .The algorithm is implemented via pixel by pixel comparison between host image and watermark. For the each pixel of host image, if its correspond value equal to compared pixel in watermark, we save its position as key. First two positions of key vector are the dimensions of watermark. For watermark extraction, First, we create m×n(size of watermark) matrix. Then we fill this matrix with values from host image that their positions are saved in key .After implementation of extraction algorithm we compare extracted watermark and original watermark. The algorithm was found to be robust against many attacks.
In [2] a new watermarking technique for color images based on embedding four identical watermarks into blue component of host image. Blue component is decomposed into 128*128 regions; each region is divided into a non-overlapping blocks of 8*8. The watermark embedding algorithm can be described as follows:

If $W_{(i,j)} = 1$

$$x^*(i, j) = x(i, j) + \alpha \quad , \ 1 <= i,j <= 8$$

else

$$x^*(i, j) = x(i, j) - \alpha \quad , \ 1 <= i,j <= 8$$

Where $W_{(i,j)}$ represents an encrypted watermark bit, $x^*(i, j)$ and $x(i, j)$ represent the watermarked intensity pixel and the original intensity pixel at location (i, j) , respectively, α is the embedding strength.. In the extraction process, the original image is available and five watermarks can be extracted from different regions of the watermarked image and only one watermark is detected or constructed from the five watermarks according to the highest value of normalized cross correlation (NCC).
In [3] a watermarking technique in transform domain was proposed by taking DWT of a image and adding PN sequences to H1 and V1 components of the image. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components One of the many advantages over the wavelet transform is that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform The proposed method was implemented in MATLAB and technique is proved to be resistant to JPEG compression, cropping.
In [4] a collusion attack resistant watermarking scheme for Colored images using DCT. It improved on the classical middle band coefficient Exchange watermarking scheme by averaging of middle frequency coefficients of the image. In this scheme we choose any 4 coefficients from the FM region of its DCT block Calculate the average of 18 middle band coefficients ,hide 0 for all 4 chosen

coefficients assign the value of coefficients which is less than the average, if the average is greater than the coefficients value hide 1.

In [5] lossless watermarking scheme was suggested which applied fuzzy integral to find similarity between DCT coefficients of original image and watermark. For each block in watermark image, the best match block in the original image is selected by applying fuzzy integral and the corresponding block number is kept as secret key. The watermark extraction of the proposed method uses secret key to extract watermark and it does not require the original image.

In [6] a new watermarking scheme was proposed for JPEG images using modified DCT. The advantage is that it minimizes blocking artifacts which are common JPEG images, thus improving the visual quality. It is robust against many attacks.

The Modified DCT for a two dimensional array is defined as:

$$X(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} s(i,j) \cos\left[\frac{\Pi}{N}(2k+1)(i+n)\right] \cos\left[\frac{\Pi}{N}(2l+1)(j+n)\right]$$

where , $n = \frac{1}{2}\left(\frac{N}{2} + 1\right)$

For watermark embedding we embed a binary image as watermark into the higher frequency components in Modified DCT using a random key. Then a inverse transformation is applied to obtain the final watermarked image.

4. COMPARISION OF WATERMARKING TECHNIQUES

In the given table 1 below the watermarking techniques are compared.

Name of Technique	***Domain***	***Resistance against Attacks***	***Host Image***	***Advantages of Using this technique***	***Disadvantages of using this technique***
Spatial domain Algorithm for Gray Scale Images Watermarking[2]	Spatial	Gaussian noise, compression, Weiner filtering	Gray Scale	Simple and easy to implement algorithm	Cannot be used for colored images, less robust against Gaussian noise attack
Novel Multiple Spatial Watermarking Technique in Color Images[3]	Spatial	Median filtering, compression, Image cropping, scaling, rotation	Color Image	Can be used for Color images. Robust against a variety of attacks	Complex algorithm
A DWT Domain Visible Watermarking Techniques for Digital Images[4]	DWT	Compression	Gray Scale	Using DWT it is more accurately model aspects of HVS as compared to FFT and DCT	Not robust against various attacks
Collusion Attack Resistant Watermarking Scheme for Colored Images using DCT[5]	DCT	Collusion attack	Color Image	Specially designed for collusion attack	Finding suitable color channel for watermark embedding is not easy
A new Lossless Watermarking Scheme Based on Fuzzy integral and DCT[6]	DCT	Compression, Gaussian noise, Median filtering	Gray Scale	A blind watermarking technique which find usage in real applications	Usage of fuzzy integral adds to more computation overhead

An improved digital watermarking technique for protecting JPEG[7]	DCT	Rotation, Scaling, filtering	Gray Scale	Eliminates blocking artifacts thus improving the visual quality	MDCT is complex than DCT

Table 1 : Various Watermarking techniques

4. CONCLUSION

In this paper, we described the digital watermarking technique. Then we presented some digital watermarking techniques implemented in different domains and compared these techniques. These techniques were found to be robust against many attacks.
Spatial domain watermarking technique for gray scale images[2] is very simple and easy to implement can find usage in copyright protection. Collusion attack resistant watermarking scheme [5] can find usage in source tracking (different recipients get differently watermarked content)
Future work can be done to study more watermarking techniques and find a new watermarking technique which is robust against attacks

REFERENCES

[1] YanqunZhang"Digital Watermarking Technology: A Review" 2009 ETP International Conference on Future Computer and Communication

[2] Houtan Haddad Larijani and Gholamali Rezai Rad "A New Spatial Domain Algorithm for gray scale images watermarking" Proceedings of the International Conference on Computer and Communication Engineering 2008 May 13-15, 2008 Kuala Lumpur, Malaysia

[3] Ibrahim Nasir, Ying Weng, Jianmin Jiang "Novel Multiple Spatial Watermarking Technique In Color Images"Fifth International Conference on Information Technology: New Generations

[4] Munesh Chandra "A DWT Domain Visible Watermarking Techniques for Digital Images"2010 International Conference on Electronics and Information Engineering (ICEIE2010)

[5] Vikas Saxena, J.P Gupta "Collusion Attack Resistant Watermarking Scheme for Colored Images using DCT" IAENG International JournalofComputerScience,34:2,IJCS_34_2_02

[6] Reza Mortezaei, Mohsen Ebrahimi "A new lossless watermarking Scheme based on fuzzy integral and DCT domain"2010 International Conference on Electronics and InformationEngineering(ICEIE 2010)

[7] Afzel Noore "An Improved Digital Watermarking Technique for Protecting JPEG images" WPM P2.08
0-7803-7721-4/ 03 © 2003 IEEE