ISSN 2250-3153

Study of Watermarking Techniques Used in Digital Image

O P Singh, Satish Kumar, G R Mishra, Charu Pandey, Vartika Singh

Deptt. of Electronics & Electrical Engineering (ASET), Amity University, Uttar Pradesh, Lucknow_mishra

Abstract- The imaging technology is being improving day by day, there are a lot of chances of reproduction and manipulation of digital contents such as digital image, digital audio and digital video, hence a strong digital copyright mechanism must be developed in place. So the protection of data content from unauthorized users and the issue of copyright management play very important role. Digital watermarking is being used to secure the data of researchers and to hide the information inside a signal which cannot be easily detected by unauthorized users. A digital watermarking can be defined as a stream of bits embedded in a data file that offers features such as IPM (Intellectual Property Management) and proof of ownership. The digital watermarking has two basic concepts- first is content protection and second is copyright management. In this paper, an overview of some Digital Watermarking techniques is discussed such as Discrete Cosine transform (DCT) and Digital Wavelet Transform (DWT) and its purpose, methods, limitations and applications.

Index Terms- Human Visual System (HVS), Human Auditory System (HAS), Copyright Protection, Digital Watermarking.

I. INTRODUCTION

Digital watermarking is a burgeonic field that requires continuous efforts to find best possible way in protecting multimedia content its security concern [1]. Watermarking is a process that embeds data into a multimedia object to protect the owner's ownership to the objects. A watermark is a pattern of bits embedded into a digital image audio or video files that give the file copyright information. Unlike printed watermarks, which are intended to be somewhat visible (like the very light compass stamp watermarking). Digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible [2]. Now a day due to internet connection it has become very feasible to download any data worldwide through web. So watermarking is a useful technique to reduce piracy. Intellectual property management and protection (IPMP) motivated the researchers and service providers to seek efficient encryption and data hiding techniques [2]. A simple idea is to include password or a key that is relatively difficult to be "hacked" in a given time. There are many types of digital information and data such as Digital Image, Digital Audio and Digital Video.

Digital audio and video watermarking techniques rely on the perceptual properties of a human auditory system (HAS) and human visual system (HVS) respectively. The HVS is less sensitive as compared to the HAS. More challenging idea is to embed imperceptible audio watermarks. HAS consists of larger dynamic range. The stream of bits embedded in an audio file is much smaller in size as compared to the auxiliary information in a video file for watermarking [3]. Watermarked image is transformed image in which the original image remains intact, recognizable, remains persistent in viewing and printing and retransmission and dissemination. The functioning of digital watermarking concept is shown in figure (1):

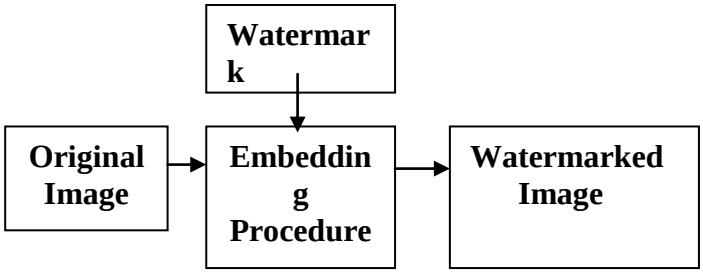

Fig.1 Functioning of Digital Watermarking

In order to have effective watermarking, following properties are being followed such as unobtrusive, robust, secure and high capacity and protect intellectual property. The details of these properties are described below [4]:

1. Unobtrusive- The idea watermark should be completely invisible.
2. Robust- The watermark should be resistant to distortion introduced during normal use or in a continuous attempt to remove the present watermarking.
3. Secure & High Capacity- The identification of the owner should be degrade gracefully in the face of attack.
4. To Protect Intellectual Property-Watermark must service image modification.
    a. There should be imperceptibility in visible watermark, so that it will not affect the experiences of viewing.
    b. A proper authority can easily detect the watermark embeddd.
    c. It is very difficult or impossible to remove a watermark at least without visibly degrading the original image.

II. METHODOLOGY TO BE ADOPTED IN WATERMARKING

The process of watermarking is done two ways namely Watermark Embedding and Watermark Extraction [1].

Consider the function f which is a function of I and W, where I=original Image, W=watermark to embed and I' denotes the watermarked image which is also the function of I and W.

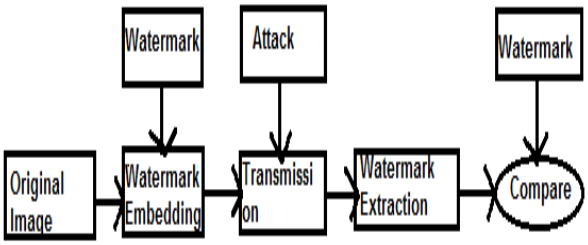

Fig.2 Process of watermark embedding and extracting methods

$$I' = f(I,W)$$

Common approach is as follows:

Select a subset of coefficients from the original image I:

$$J = j_1, j_2 \ldots j_n$$

Corresponding watermark sequence is given below:

$$X = x_1, x_2 \ldots x_n$$

When X embeds into J then adjusted sequence can be written as

$$J' = J + X = j'_1, j'_2 \ldots j'_n.$$

Put j' back and take the place of J, then we get the watermarked image I'. Let E denote the extraction function and I' the image to be examined. Extract the watermark W' from the watermarked image I'. If the correlation function C (W,W') satisfies

$C(W,W') \; T \geq T$, *where T is the threshold value)*

Then we consider, there is a watermark W in I' image.

Signal-to-noise ratio (SNR) is common theory in signal processing. Suppose the original image is I(m,n) and the output image is $\hat{I}$(m,n) then SNR is defined as:

$$SNR=10\log_{10}[\sum_m\sum_n I^2(i,j)/\sum_m\sum_n\{I(i,j)-D^2(i,j)\}]$$

When SNR approaches infinity, the original image and output image are totally the same.

Another similar one is Peak SNR (PSNR). For images with 255 gray levels, the PSNR is defined as:

$$PSNR=10\log_{10}[\sum_m\sum_n(255)^2/\sum_m\sum_n\{I(i,j)-D^2(i,j)\}]$$

III. Classification

Watermarking techniques are categorized into four methods such as text watermarking, image watermarking, audio watermarking and video watermarking [1]

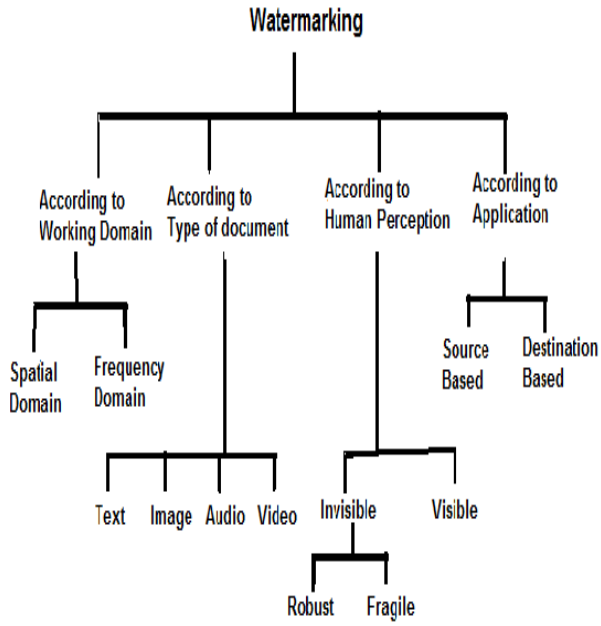

Fig.3 Classification of Watermarking

In the case of images, watermarking techniques are commonly distinguished based on two working domains: Spatial domain and frequency domain. In spatial domain, the pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of the original image [5]. However in the Frequency or transform domain, the values of certain frequencies are altered from their original image. Meanwhile, based on human perception, digital watermarks are divided into three categories as follows:

(a) Visible watermark, where the secondary translucent overlaid into the primary content which would be seen visible by careful inspection [6].
(b) Invisible-Robust watermark is embedded in such a way that alterations made to the pixel value are perceptually unnoticed.
(c) Invisible-Fragile watermark is embedded in such a way that any manipulation of the content would alter or destroy the watermark.

From application point of view, digital watermarks could also be Source based where a unique watermark identifying the owner is introduced to all the copies of a particular content being distributed [7]. Destination based is where each distributed copy gets a unique watermark identifying the particular buyer.

IV. Technology Used in Watermarking

Watermark in Frequency and wavelet domain is more robust and compatible to popular image compression standards as

compared to spatial-domain. Thus the frequency and wavelet domain watermarking is being explored much more by researchers. To embed a watermark, the frequency or wavelet transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT). However, in the wavelet domain, the Discrete Wavelet Transform (DWT) is being used by the researchers.

1) Discrete Cosine Transform (DCT) Domain watermarking Technique- The first efficient watermarking scheme was introduced by Koch[7].He pointed out that the image is first divided into square blocks of size 8x8 for DCT computation. A pair of mid-frequency coefficient is chosen for modification from 12 predetermined pairs. Bors and Pitas developed a method that modified DCT coefficients satisfying a block site selection constraint [8]. After dividing the image into blocks of size 8x8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson [9]. Cox developed the first frequency domain watermarking scheme [10]. After that a lot of watermarking algorithms in frequency domain have been developed [13].

The watermarking concept has been elaborated through block diagram. Insert watermark into the block, transformed block back into spatial domain and move on to the next block, and write the watermarked image out to a file. Finally separate the watermark from the image using DCT block [10]. Compare the watermark extracted image from the original image, and then if the change is less than threshold then the image is not distorted.

.

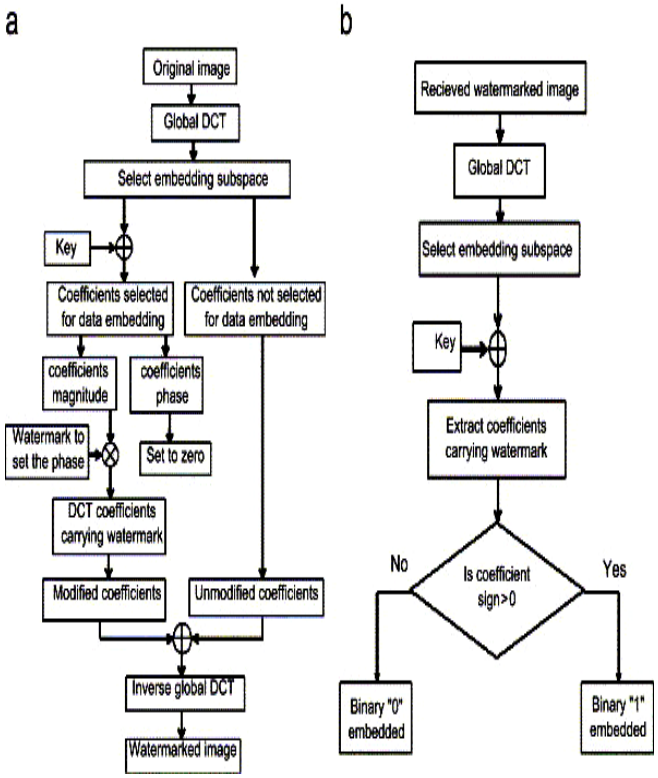

Fig.4 DCT Domain Watermarking Technique for embedding and extracting of an image[6]

Experimental Analysis- The experiment is carried out on various images. One major reason why frequency domain watermarking schemes are attractive is their compatibility with existing image compression standards, in particular, the JPEG standard. The compatibility ensures those schemes a good performance when the watermarked image is subject to lossy compression, which is one of the most common image processing methods today. In consequence, those schemes become particularly useful in practical applications [12].

Fig.5 DCT Domain Watermarking Technique going from Top Left to Right A. Original Image B. Watermarked Image C. Watermark D. Extracted Watermark

2) Wavelet Domain Watermarking Technique: Another possible domain for watermark embedding is that of the wavelet

domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image as well as in horizontal, vertical and diagonal detail components [4]. The process can then be repeated to compute multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform. Wavelet transform has more accurate model aspects of the HVS as compared to the FFT or DCT [1]. This allows us to use higher energy watermarks in regions where HVS is known to be less sensitive, 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 [14].

One of the most straightforward technique is to use a similar embedding technique to that used in the DCT, i.e. the embedding of a CDMA sequence in the detail bands according to the expression shown as under:

$$I_{Wu,v} = \begin{Bmatrix} W_i + \propto |W_i| x_i, u, v \in HL, LH \\ W_i, u, v \in LL, HH \end{Bmatrix}$$

Embedding of a CDMA Watermark in the Wavelet Domain where Wi denotes the coefficient of the transformed image, xi the bit of the watermark to be embedded, and a scaling factor. To detect the watermark we generate the same pseudo-random sequence used in CDMA generation and determine its correlation with the two transformed detail bands. If the correlation exceeds some threshold T, the watermark is detected[15].

Fig.6 Wavelet Domain Watermarking Technique – Going from Top Left to Right A. Original Image B. Watermarked Image C. Extracted Watermark D. Watermark

This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. During detection, if the correlation exceeds T for a particular sequence a '1' is recovered; otherwise a zero. The recovery process then iterates through the entire pseudo noise sequence until all the bits of the watermark have been recovered [16].

Furthermore, as the embedding uses the values of the transformed, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients. This technique would prove resistant to JPEG compression, cropping, and other typical attacks.

V. APPLICATIONS

There are a large number of applications such as:

1) **Identification of the owner-** It is used to establish ownership of the content similar to copyright protection.
2) **Copy protection-** It is used to prevent people from making illegal copies of copyrighted content.
3) **Content authentication-** It detects all the types of modifications in the content and shows it as a sign of invalid authentication.
4) **Fingerprinting-** It is used to trace back illegal duplication and distribution of content.
5) **Broadcast monitoring-** It is specifically used for advertisements and entertainment industries.
6) **Medical application-** It is known as invertible watermarking and it is used to provide authentication and confidentiality in a reversible manner without effecting medical image in any way.

VI. CONCLUSIONS

This paper presents a comprehensive study of some techniques of watermarking of image data and detailed descriptions and implementation of recent techniques have been explored. DCT and DWT domains watermarking are comparatively much better than the spatial domain encoding since DCT domain watermarking can survive against the attacks such as noising, compression, sharpening, and filtering. However, the DWT technique for the insertion of digital watermark is efficient because embedded information in the image can be recovered. It is completely secured since the embedded information is not visible to any non authorized person. The DWT techniques always achieve a higher performance of recovery. Hence DCT and DWT techniques both are much better than any other transformation technique.

REFERENCES

[1] R.C. Gonzalez, R.E. Woods, "Digital Image Processing", Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002.

[2] Dhruv Arya , "A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques"

[3] Jen-Sheng Tsai, Win-bin Huang and Yau-Hwang Kuo, "On the Selection of optimal Feature Region Set for Robust Digital Image Watermarking", *IEEE Transactions on Image Processing, Vol.20,No.3,March 2011.*

[4] Patrick Bas, Jean-Marc Chassery, and Benoit Macq, "Geometrically Invariant Watermar king Using Feature Points", *IEEE Transactions on Image Processing, Vol.11,No.9,Sepetember 2002.*

[5] Munesh Chandra, Shika Pandey, and Rama Chaudary, "Digital Watermarking Technique for Protecting Digital Images", *IEEE 2010.*

[6] Inegar J. Cox , Joe Kilian, F.Thomson Leigthon and Talal Shamoon , "Secure Spread Spectrum Watermarking for multimedia", *IEEE Transactions on Image Processing, Vol.6,No.12,December 1997.*

[7] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", *IEEE Transactions on Image Processing,Vol.51, No.4, April 2003.*

[8] M. D. Swanson, B. Zhu and A. H. Tewfik, "Robust Data Hiding for Images", IEEE Digital Signal Processing Workshop, pp. 37-40, Department

of Electrical Engineering, University ofMinnesota,http://www.assuredigit.com/tech_doc/more/Swanson_dsp96_robust_datahiding.pdf, September 1996

[9] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure sprea spectrum watermarking for multimedia"

[10] M. B. Martin and A. E. Bell, "New Image Compression Techniques Multiwavelets and Multiwavelet Packets", IEEE Trans. Image Process.,vol. 10, no. 4, pp. 500–510, Apr. 2001.

[11] J. Lebrun and M. Vetterli, "Balanced Multiwavelets: Theory and Design," IEEE Trans. Signal Process., vol. 46, no. 4, pp. 1119–1125, Apr. 1998.

[12] L. Ghouti, A. Bouridane, M. K. Ibrahim and S. Boussakta, "Digital Image Watermarking Using Balanced Multiwavelets", IEEE Trans.Signal Process., vol. 54, no. 4, pp. 1519-1536

[13] Callinan and D. Kemick, "Detecting Steganographic Content in Images Found on the Internet", Department of Business Management, University of Pittsburgh at Bradford.

[14] Jin S. Seo and Chang D.Yoo, "Image Watermarking Based on Invariant Regions of Scale-Space Representation", IEEE Transactions on Image Processing, Vol.54, No.4, April 2006.

[15] E.Koch , J.Rindfrey and J.Zhao, "Copyright Protection of Multimedia Data", in proceedings International Conference Digital Media and Electronic Publishing,1994.

[16] H. Kellerer, U. Pferschy, and D. Pisinger, Knapsack Problems. Berlin:Springer,2004.

[17] Jen-Sheng Tsai, Win-bin Huang, Chao-Leigh Chen, Yau-Hwang Kuo "A Feature-Based Digital Image Watermarking for Copyright Protection and Content Authentication" IEEE, 2007.

AUTHORS

First Author – O P Singh, Deptt. of Electronics & Electrical Engineering (ASET), Amity University, Uttar Pradesh, Lucknow_mishra, Email: opsingh@amity.edu
Second Author – Satish Kumar, Deptt. of Electronics & Electrical Engineering (ASET), Amity University, Uttar Pradesh, Lucknow_mishra, Email: skumar2@lko.amity.edu
Third Author – G R Mishra, Deptt. of Electronics & Electrical Engineering (ASET), Amity University, Uttar Pradesh, Lucknow_mishra, Email: gr_mishra@rediffmail.com
Fourth Author – Charu Pandey, Deptt. of Electronics & Electrical Engineering (ASET), Amity University, Uttar Pradesh, Lucknow_mishra, Email: charu.pandey15@gmail.com
Fifth Author – Vartika Singh, Deptt. of Electronics & Electrical Engineering (ASET), Amity University, Uttar Pradesh, Lucknow_mishra, Email: vartika5988@gmail.com