Advanced Research in Electrical and Electronic Engineering
p-ISSN: 2349-5804; e-ISSN: 2349-5812 Volume 3, Issue 2 January-March, 2016, pp. 123-127

http://www.krishisanskriti.org/Publication.html

An Overview on Digital Image Watermarking and Its Techniques

Ajeet Pratap Singh[1], Sumita Mishra[2] and Sachin Kumar[3]

[1,2,3]Department of ECE, ASET Amity University, U.P., India
E-mail: [1]syanaps@gmail.com, [2]smishra3@lko.amity.edu, [3]skumar3@lko.amity.edu

Abstract—*The Digital image watermarking technology is being improved day by day, there are a lot of possibilities of reproduction and manipulation of digital multimedia such as digital image, digital audio and digital video. Hence the digital image watermarking methods have been designed and implemented for the purpose of protection. In this paper, we present an overview on Image Watermarking techniques. In digital watermarking techniques, we discuss the various factors used in watermarking, properties and application area where watermarking technique required to be used. The digital watermarking is a passive protection tool that used to secure the data of researchers and the information is hidden inside a signal which cannot be easily detected by unauthorized users. The digital watermarking can be defined as a stream of bits embedded in a data file. Digital watermarking has two basic concepts- first is content protection and second is copyright management. In this paper, two most commonly used transforms are discussed such as Discrete Cosine transform and Digital Wavelet Transform and its methods, purpose, limitations and applications.*

1. INTRODUCTION

Today's various types of data are embedded on digital media over the internet worldwide. The digital media is commonly used in present era. These types of data, which includes images, videos, audios, or texts are stored and transmitted in a digital form can be easily copied without any loss of quality and efficiently as per original data. Hence the protection of digital media is very important. We know that the internet is a fastest medium of transferring data to any place in a world. Since this technology grown up the threat of piracy and copyright very obvious thought is in owners mind. Hence Watermarking is a process of secure data from these threats. The information is stored in digital form due to ease of reproduction, retransmission and even manipulation allowed to pirate either to remove a watermark and violate a copyright or to cast the same watermark after altering the data to forge the proof of authenticity. The design of techniques for preserving the ownership of digital information will be the basis of the development of future multimedia services.

2. DIGITAL IMAGE WATERMARKING

The Digital Image Watermarking is a technique of embedding of owner copyright identification with the host image. In bank currency notes, a watermark is embedded which is used to check the originality of the currency note which is shown in fig.1.

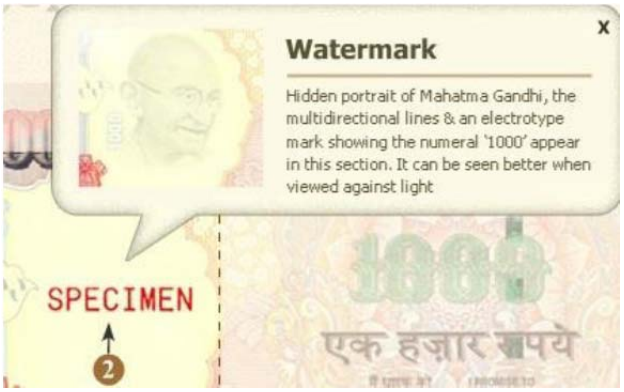

Fig. 1 An example of watermark on Indian currency note

The same concept of Watermarking is used in digital multimedia contents for checking the authenticity of the original content. The digital media has the capability to embed additional data into the original media data in a way which is perceptually and sometimes also statistically undetectable. This data-embedding potential can be exploited to build protection mechanisms against the threats, or to provide additional functionalities. In this paper an overview of the watermarking techniques carried out with their pros and cons. First of all it provides a general description of the desirable characteristics of digital watermarking system. The Digital image watermarking is actually derived from Steganography, a process in which digital content is hidden with the other content for secure transmission of Digital data. The steganography and watermarking are very similar particularly, when the data to be secure is hidden in process of transmission over some carrier. The main difference between these two processes are in steganography the hidden data is on highest priority for sender and receiver but in watermarking both source image and hidden image, signature or data are on highest priority.

The process of watermarking is divided into two parts such as embedding of watermark into host image and extraction of watermark from image. The process of image watermarking is done at the source end. In this process watermark is embedding in the host image by using any watermarking process which is shown in Fig. 2. The process of Extraction watermarking is a reverse process of embedding watermarking image.

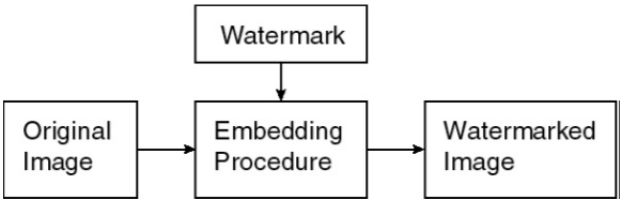

Fig. 2: Embedding image watermarking process

3. PROPERTIES OF DIGITAL WATERMARKING TECHNIQUES

The watermarking property in any particular application depends on the requirements of that specific application. Some of the digital watermarking technique properties are given as under:

I. **Transparency or Fidelity:** The digital watermarking should not affect the quality of the original image after it is watermarked. The digital watermarking should not introduce visible distortions because of such distortions it reduces the commercial value of the image.

II. **Robustness:** Watermarks can be removed intentionally or unintentionally by simple image processing operations like contrast or brightness adjustment, gamma correction etc. Hence watermarks should be robust against various attacks.

III. Capacity or Data Payload: The watermark should be able to carry enough information to represent the uniqueness of the image as we know that different application has different payload requirements. Hence this property describes how much data should be embedded as a watermark to successfully detection during extraction.

IV. Embedding Effectiveness: The effectiveness of watermarking system is the probability of detecting watermark(s), especially at the receiving point. The desired effectiveness should be 100%, but it is often not possible because of the requirement of perceptual similarity conflicts. Hence, it's application dependent to sacrifice effectiveness for better performance with respect to other characteristics.

V. Blind and Informed Detection: In blind watermarking systems (i.e. copy control application), there is no need of original or any information about the original image. But, in informed watermarking systems (i.e. transaction tracking), the detector needs the original or some information about the original image (i.e. without watermarked). The private and public watermarking systems can be used alternatively for informed and blind watermarking approaches respectively. The blind detection process is computationally complex having low PSNR value but offers very high security while informed detection process is having high pay load and very high PSNR value having simple embedding and extracting methods.

VI. Computational Complexity: The computational complexity indicates the amount of time watermarking process takes to encode and decode. To ensure security and validity of watermark, more computational complexity is required.

4. WATERMARKING APPLICATIONS

The applications of digital watermarking are given as:

I. Copyright Protection: The digital Watermarking can be used to protecting utilisation of copyrighted material over the unreliable network like Internet or peer-to-peer (P2P) networks. The content aware networks (p2p) could incorporate the watermarking technologies to report or filter out copyrighted material from such networks.

II. Content Archiving: The watermarking can be used to insert digital object identifier to help archive digital contents like images, audios or videos. It can also be used for classifying and organizing digital data. Generally digital data is identified by their file names and this technique is able to easily change their file names.

III. Broadcast Monitoring: The broadcast Monitoring is a technique of cross-verifying whether the content that was supposed to be broadcasted has really been broadcasted or not. The watermarking can also be used for broadcast monitoring. This has major application in commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration or not.

IV. Tamper Detection: The digital contents can be detected by embedding fragile watermarks for tampering. When fragile watermark is destroyed or degraded, it indicates the presence of tampering and hence the digital contents can't be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image has tampered or not.

V. Digital Fingerprinting: The digital fingerprinting is a technique that used to detect the owner of the digital content. The fingerprints are unique to the owner of the digital data.

Therefore, a single digital content can have different fingerprints because they can be related to different users.

5. CLASSIFICATION OF WATERMARKING

The classification of digital watermarking is shown in figure 3.

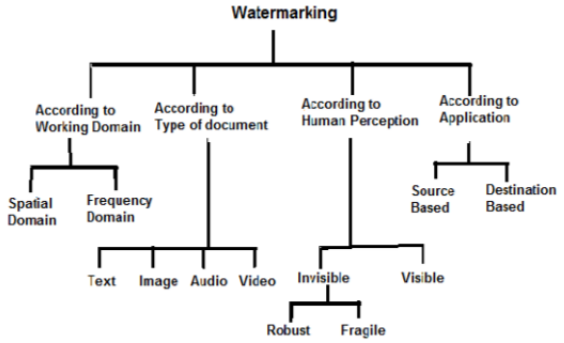

Fig. 3: Classification of Watermarking

The watermarking techniques, based on type of document are classified into four categories such as: Text watermarking, Image watermarking, audio watermarking and video watermarking.

The image watermarking techniques, based on working domain are two types such as: Spatial domain and Frequency domain. In frequency or transform domain, the values of certain frequencies are altered from their original image. And in spatial domain, the pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of original image.

The image watermarking, based on human perception is two types such as: Visible watermark and Invisible watermark. In visible watermark, the secondary translucent is overlaid into the primary content which would be seen visible by careful inspection. Invisible watermark is subdivided into two categories such as: Robust and Fragile. The robust watermark is embedded in such a way that alterations made to the pixel value are perceptually unnoticed. The fragile watermark is embedded in such a way that any manipulation of the content would alter or destroy the watermark.

The watermarking techniques, based on application are two types such as: Source and Destination. In source based digital watermarks, each distributed copy is introduced a unique watermark identifying the particular owner. In destination based digital watermarks, each distributed copy gets a unique watermark identifying the particular buyer.

6. WATERMARKING APPROACHES

The watermarking approaches in Frequency and wavelet domain are more robust and compatible to popular image compression standards as compared to spatial domain. Hence the frequency and wavelet domain watermarking is being explored much more by researchers. To embed a watermark, the frequency or wavelet transformation can be applied to the host data. Therefore, modifications are made to the transform coefficients. The possible frequency image transformations include the Discrete Fourier Transform and Discrete Cosine Transform. Usually in the wavelet domain, the Discrete Wavelet Transform (DWT) is being used by the researchers.

I. Discrete Cosine Transform (DCT)

The character of discrete Fourier transform (DFT) and discrete cosine transform (DCT) turn over the image edge to make the image transformed into the form of even function. It's one of the most common linear transformations in digital signal process technology. The first efficient watermarking scheme was introduced by Koch. He pointed out that the image is first divided into square blocks of size 8x8 for discrete cosine transform 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. 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. Cox developed the first frequency domain watermarking scheme. After that lots of watermarking algorithms in frequency domain have been developed.

The watermarking concept has been elaborated through block diagram which is shown in figure 4. Insert watermark into the block, transformed block back into spatial domain and move on to the next block, write the watermarked image out to a file and finally separate the watermark from the image using DCT block. To compare the watermark extracted image from the original image, and if the change is less than threshold then the image is not distorted.

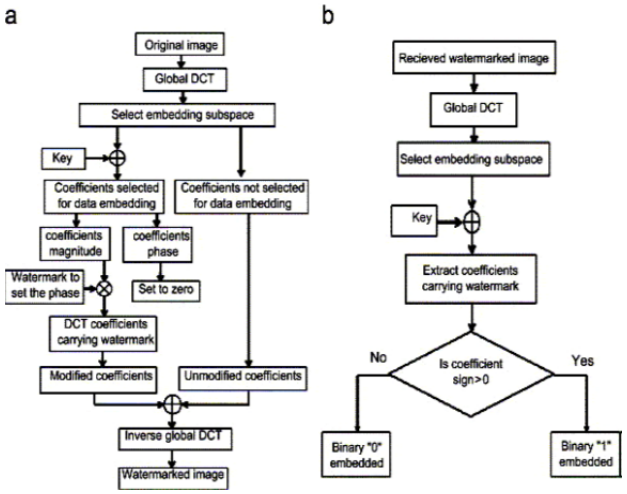

Fig.4 DCT Domain Watermarking Technique: (a) Embedding process and (b) Extracting process of an image

II. Wavelet Domain Watermarking Technique

The wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is rather good time differentiated rate in high frequency part of signals discrete wavelet transform. Also there is rather good frequency differentiated rate in its low frequency part of signals. It can distil the information from signal effectively. The basic idea of discrete wavelet transform in image process is to multi-differentiated decomposing the image into sub-image of different spatial domain and independent frequency district and after that transforms the coefficient of sub-image. When 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. A two-dimensional image after three-time DWT decomposed can be shown in Fig.5, where L represents low-pass filter, H represents high-pass filter. An original image can be decomposed into frequency districts of HL1, LH1, and HH1. Also the low-frequency district information can be decomposed into sub-level frequency districts information of LL2, HL2, LH2 and HH2. By following this original image can be decomposed into *n* level wavelet transformation.

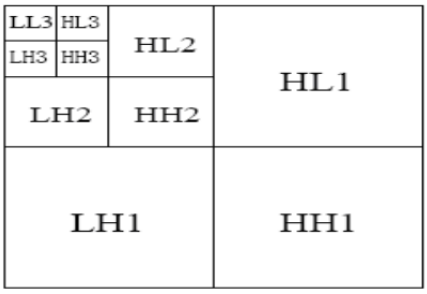

Figure 5. 2-D Image after DWT Decomposed

The information of low frequency district is an image close to the original image. Most of the signal information of original image is in this frequency district. The frequency districts of LH, HL and HH represent the level detail, the upright detail and the diagonal detail respectively of the original image.

Experimental Analysis: In the following experiments, a binary image "logo" is used as the watermark which is shown in fig. 6. Another image "Lena" is used as host image to embed watermark. The original host image and watermarked image are shown in Fig.7 (A) and (B). It is very difficult to recognize the transformed watermark image. This watermarked image is rather close to the original image in vision impression. There are no easily seen differences between these two images only with eyes. One major reason why frequency domain watermarking schemes are attractive is their compatibility with existing image compression standards, particularly, in JPEG standard. The compatibility ensures those schemes when the watermarked image is subject to lossy compression, which is the one of the most common image processing methods today. Therefore, those schemes become particularly useful in practical applications.

Figure 6 Original watermark and DCT transformed watermark

A. Original Image B. Watermarked Image
Fig.7 (A) & (B) Wavelet Domain Watermarking Technique

This recovery process then iterates through the entire pseudo noise sequence until all the bits of the watermark have been recovered. Furthermore, as the embedding uses the values of the transformed, the embedding process should be quite adaptive and storing the majority of the watermark in the larger coefficients. This technique would prove resistant to JPEG compression, cropping, and other various attacks.

7. CONCLUSION

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

REFERENCES

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

[2] 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.

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

[4] Vaishali S. Jabade, Dr. Sachin R. Gengaje,”Litrature Review of Wavelet Based Digital Watermarking techniques”, International Journal of Computer Applications, Volume 31, No.1,pp-28-35.

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

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

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

[8] 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.

[9] 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

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

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

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

[13] 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.

[14] Prabhishek Singh, R S Chadha ,“A Survey of Digital Watermarking Techniques, Applications and Attacks”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013

[15] Mei Jiansheng, Li Sukang, “A Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[16] Http://cameo.mfa.org/wiki/Watermark.