

International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X Impact factor: 4.295

(Volume3, Issue1)

Available online at: www.ijariit.com

Dwt based Invisible Watermarking on Images

Rashmi Srivastava M.Tech Scholar SIIT Gorakhpur, UP.

Abstract: The imaging technology is being enhancing day by day, there are a lot of possibilities of reproduction and manipulation of digital data such as digital image, digital audio and digital video, hence a strong digital copyright mechanism must be produced in place. So the protection of digital data content from unauthorized users and the problem of copyright management plays very vital role. The Digital watermarking is being used to protect and safe the data of researchers and to keep secret information inside a signal which cannot be easily detected by unauthorized person or users. The digital watermarking is a field of data hiding which hide the crucial information or data in the original data for protecting illegal duplication and to restrict disturbance of multimedia data. This research paper presents a survey on the digital image watermarking techniques. The output of various digital image watermarking methods has been compared on the basis of the results. A digital watermarking can be described as a stream of bits embedded in a digital file that offers features such as IPM (Intellectual Property Management) and proof of authority of ownership. The digital watermarking has two basic ideas - first is content protection and second is the copyright management. There are various methods to hide information inside an image, audio/video, document etc. But the Image Steganography has its own importance and is most popular among the others. This paper gives a review of various techniques such as image domain and transformation domain algorithms available for implementing Image Steganography. In this paper, an overview of some Digital Watermarking methods are discussed such as Discrete Cosine transform (DCT) and Digital Wavelet Transform (DWT) and its purpose ,techniques, limitations and applications.

Key Terms: Digital Watermarking, Image Steganography, Encryption, DCT, DWT

I. INTRODUCTION

The Digital watermarking is the act of hiding information related to a digital signal (i.e. an image, song, or video) inside the signal itself. It is a concept relatively closed to the steganography, in that they both hide a message or information within a digital signal. The Digital watermarking is a burgeoning field that wants continuous efforts to search best possible way in protecting multimedia content its security related [1]. The Digital Watermarking is a technique that embeds secret data into a multimedia files to protect the owner's authority to the objects. The Digital Watermarking applies to embed a message related to the original content of the digital signal, while in the steganography the digital signal has no relation to the information, and it is generally used as a cover to hide its existence. The Digital watermarks are drawn to be completely invisible, or in the case of audio clips, it is inaudible [2]. Now a day, because of internet connection it has become very easy to download any data worldwide through web. So watermarking is a useful method to reduce piracy problem.

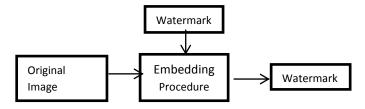


Fig1.Functional block diagram of Digital Watermarking

Srivastava Rashmi, International Journal of Advance Research, Ideas and Innovations in Technology.

The Digital watermarking is a very progressing field and is used in number of applications which have been proved to be very successful. The digital watermarking has been used in a number of image processing methods. The objective of every application is to provide security of the digital data content. The application of digital watermarking are Broadcast Monitoring [3], Data Hiding [4], Transaction Tracking [5], Copyright protection [6], Digital Fingerprinting [7], Temper Detection [8], and Content Authentication [9] etc.

Since from the rise of the Internet, one of the most important terms of information technology and communication has been the security of the data or information. Cryptography was created as a method for securing the secrecy of communication and various techniques have been introduced to encrypt and decrypt data in order to keep the information secret. Unfortunately, sometimes it is not enough to keep the details of a message secret, it may also be very important to keep the existence of the secret message. The method used to implement this, is known as steganography. The Steganography is the science and art of the invisible communication. This is achieved through hiding information or message in other information, thus also hiding the existence of the communicated information or message. The word steganography is found from the Greek words "stegos" which means "cover" and "grafia" means "writing" [10] defining it as "covered writing". In the image steganography the information is hidden exclusively in the form of images. A Steganography and watermarking differ in a number of ways including purpose, specification and detection/extraction methods. The most fundamental difference is that the object of communication in watermarking is the host signal, with the embedded data providing copyright protection. The Digital watermarking is the process of embedding auxiliary information into a digital cover signal with the aim of providing authentication information. Watermarking and fingerprinting related to steganography are basically used for intellectual property protection.

In order to keep effective watermarking, different properties are being followed such as, robust, unobtrusive, secure and high capacity and protect intellectual property. These properties are described below [11]:

- 1. Robust- The watermark should be resistant to distortion introduced during normal use or in a continuous attempt to remove the present watermarking.
- 2. Unobtrusive- The idea watermark should be completely invisible
- 3. Secure & High Capacity- The identification of the owner should be degrading gracefully in the face of attack.
- 4. To Protect Intellectual Property-Watermark must service image modification.

II. TECHNOLOGY USED IN DIGITAL WATERMARKING

The Watermark in Frequency domain and wavelet domain are more robust and compatible to image compression standards as compared to the spatial-domain techniques. Hence the frequency and wavelet domain watermarking is being spread more by researchers. For embedding watermark, the frequency or wavelet transformation is used by the host data. The different 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 technique was introduced by Koch [12]. He finds out that first the image is divided into square blocks of size 8x8 for DCT computation. The pair of mid-frequency coefficient is selected for modification from 12 pre-determined pairs. Bores and Pitas introduced a method that modified the DCT coefficients satisfying the block site selection constraints [13]. After integrating the image into blocks of size 8x8, the certain blocks are chosen based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then changed, using either a linear DCT constraint or a circular DCT detection constraint region. A DCT domain watermarking scheme based on the frequency masking of DCT blocks was developed by Swanson [14].

The DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. The DCT has been used in many fields such as data compression, pattern recognition, image processing, and so on. The Discrete Cosine Transform (DCT) applied for the signal processing. It converts a signal from the spatial domain to the frequency domain. The DCT is used in many fields like pattern recognition, data compression, and every field of image processing. The DCT watermarking is more robust as compared to the spatial domain watermarking methods. For embedding the watermark information in DCT, we divide the image into different frequency bands.

2) Discrete Wavelet Transform (DWT) Domain Watermarking Technique: The Discrete wavelet transform (DWT) of the image generates multi resolution representation of an image. The multi resolution representation gives a simple framework for interpreting the digital image information. The DWT examines the signal at multiple resolutions. The DWT splits the image into high frequency quadrants and low frequency quadrants. The low frequency quadrant is again divided into two more parts of high and low frequencies and this method is repeated until the signal has been entirely reduced.

The digital wavelet transform (DWT) are scalable in nature. The DWT frequently applied in digital image watermarking due of its excellent spatial localization and multi resolution scheme. The excellent spatial localization property is very convenient to identify the area in the cover or original image in which the watermark is embedded efficiently.

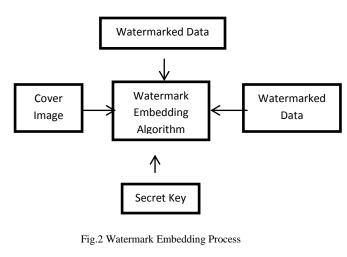
III.OBJECTIVES OF DIGITAL WATERMARKING

The key objectives of this research work are as below:

- To study and analyze the various watermarking techniques which exist and to develop an inference from them.
- To implement data hiding in various kinds of images.
- Testing and performance evaluation of the technique based on various factors like Peak to Signal Noise Ratio (PSNR), Mean Square Error (MSE) etc.

IV. PROCESS OF DIGITAL WATERMARKING

The Every digital watermarking method includes two algorithms: one for the embedding algorithm and other as the detecting algorithm. These two processes are similar for all the type of watermarking methods. The Fig 2 shows the watermark embedding process. in which watermark is embedded in the cover or original image by using the embedding algorithm. And in the Fig 3,it shows the watermark detection process in which the embedded watermark is recovered or reconstruct by using the detection algorithm.



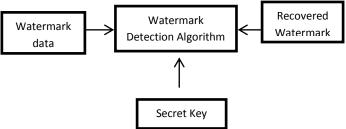


Fig.3 Watermark Detecting Process

V. Results

The watermarking Technique was implemented using MATLAB R2010a software tool on a number of images. The results are compiled as shown below. Several standard test images such as boat, baboon, Lena, peppers, couple, cameramen etc are referred to in the present paper for watermark embedding and watermark detection. The technique is not limited to the use these cover images but we have used them as they are standard images widely used by other researchers working on watermarking. They all are gray scale images with size 256x256.

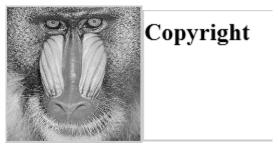


Fig 4: a) Baboon Image b) Key Image(hidden)

Fig 5: a)2D-DWT Result b) Watermarked Image



Fig 6: Extracted Watermark

The below table represents the values of PSNR and MSE for various images:

Table 1: MSE and PSNR values of Images

IMAGE	MSE	PSNR
BABOON	1.1683E-005	224.3994
Воат	3.2393E-005	214.2008
LENA	2.1659E-005	218.2261
PEPPERS	1.5276E-006	1.5276Е-006

CONCLUSION AND FUTURE WORK

The Digital watermarking is very useful technique for providing security to the digital multimedia on the internet technology. In this reasearch paper, survey of different techniques based on the transform domain (i.e. DCT & DWT). This survey examines the limitations and strengths of the watermarking methods.

The Digital watermarking is still a more challenging field for researchers with many interesting problems and issues, like it does not remove copying or distribution and also cannot overcome in every possible attacks. One future research point is the development of more robust, transparent and secure watermarking method for various digital media including images, video and audio etc.

REFERENCES

- [1] R.C. Gonzalez, R.E. Woods, "Digital Image Processing", Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002.
- [2] DhruvArya, "A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques"
- [3] L. Li and X. Li," Watermarking Protocol for Broadcast Monitoring", International Conference on E business and E-Government (ICEE) (2010).
- [4] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 4.
- [5] S. Emmanuel, A. P. Vinod, D. Rajan and C.K. Heng, "An Authentication Watermarking Scheme with Transaction Tracking Enabled", Digital Ecosystem and Technologies Conference, 2007.DEST'07 Inaugural IEEE-IES.
- [6] Y.-C. Wang and J.-f.Niu, "Research on Digital Content Copyright Protection System", IEEE International Conference on Network Infrastructure and Digital Content, 2009. IC-NIDC (2009).

Srivastava Rashmi, International Journal of Advance Research, Ideas and Innovations in Technology.

- [7] D. Zhang, S. Xu, Y. Wang, J. Zhang and Y. Li, "A Digital Fingerprinting Scheme of Digital Image", International Conference on Computational Intelligence and Software Engineerin (CISE) (2010).
- [8] S.-L. Hsieh, C.-P.Yeh and I-J. Tsai, "An Image Copyright Protection Scheme with Tamper Detection Capability", Symposia and Workshops on Ubiquitous, Autonomic and trusted Computing, 2009.UIC-ATC'09
- [9] J. Zhu, Q. Wei, J. Xiao and Y. Wang," A Fragile Software Watermarking Algorithm for Content Authentication", IEEE Youth Conference on Information, Computing and Telecommunication, 2009.YC-ICT'09.
- [10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", *Proceedings of the 2nd International Workshop on Digital Watermarking*, October 2003
- [11] 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.
- [12] 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.
- [13] 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 of Minnesota September 1996
- [14] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure sprea spectrum watermarking for multimedia"