

A REVIEW ON DIGITAL IMAGE WATERMARKING USING DWT

Er. Pinki Tanwar¹, Er. Manisha Khurana²

Assistant professor¹, M.tech student².

Department of computer Science & Engg, Seth Jai Parkash Institute of Management and Technology. Radaur, (Haryana).

ABSTRACT

This paper presents a literature survey on Digital Watermarking within an image. It describes the early work carried out on digital watermarks, including the brief analysis of various watermarking schemes and its applications. This paper also makes a comparison between various watermarking schemes. This paper also gives us a brief introduction about the procedure of digital watermarking.

Keywords: Digital Watermarking, DCT, DWT, DFT, LSB, Watermarked Image

1. Introduction

In last years, due to the growth of technology, the distribution of multimedia data in digital form by internet became very popular. Such open access to multimedia data allows the internet users to change this data in a number of ways. This can be done by large scale duplication, changing or stealing the original data from the internet. Thus it has become difficult for the copyright owner to protect the originality of the data and prove their ownership over the data. is a type of such technique that hides owner's information, called digital watermark, in an image.

The covert watermark can be subsequently used for the purpose of copyright protection, image proof etc. Whenever there is a conflict over the ownership of an image, the covert watermark must be extracted from the suspected image to prove the rightful ownership. Watermarking can also be used to keep the integrity of the data by detecting any tampering done on data either deliberately or accident. In such a case a crisp watermark is embedded in the image, that gets damaged easily when image is tampered². The amount and type of destruction in the extracted watermark gives the information about the tamper made to the original image. In this paper we emphasize on the first type of watermarking, i.e., watermarking for copyright ward of user on image data.

The watermark can either be set in the host image itself or the host image can be encrypted with the watermark without set it explicitly in the host image. In, Balanced Neural Tree has been used to encrypt the secret image with host image, where as in, visual cryptography has been used. The technique (VC) encrypts the visual data by dividing it into multiple shares. These lot separately do not give any information about encrypted image but when stacked stable, the encrypted image is obtained. Visual cryptography has been worn by several researchers for lossless watermarking.

The benefit of this kind of watermarking is that it does not issue the texture quality of the host image so no visual evil is perceived in the watermarked image. Chang and Chung has proposed a project by using the combination of visual cryptography with a words called torus automorphism in⁹. The use of this combination protects the host image from any kind of alteration. In this issue, there is a control that the size of the watermark is dependent on the area of the host image. Later, Hsu and Hou¹⁰ have planned a new issue, where over there is no alteration in the host image during the process of watermark embedding.

They have lot the sampling distribution of many means and VC. In this scheme, multiple secret images can be inserted in the host image without changing it. Also the size of the watermark and host image are independent of each other resulting a extensibility to use a binary image of any size as a watermark. Hou and Huang¹¹ have proposed a watermarking issue based on comparison of pixel values in spatial domain

. The comparison of two pixels picked at random decides the area of master share and the ownership share is constructed using rules of VC codebook with master share and secret image. Their issue can toss a larger watermark in a smaller image and is able to withstand common image processing attacks. Wang and Chen¹² have advised a hybrid DWT-SVD based issue using VC for cop copyright protection. In their issue, first the features are extracted by executing DWT and SVD on host image. The extracted image features are then classified into two clusters using K-means clustering style, and a master share is generated according to the clustering results. Finally the master share and the covert image are used to generate the ownership share using VC good book. The issue is found safe and robust against common image processing attacks. Rawat and Balasubramanian have proposed a VC based style employing part fourier transform (FrFT) and SVD in⁷ First the features are extracted using FrFT and SVD, then a binary map is design using extracted features. Thus design binary map is used to generate master share using VC good book. Further ownership share is constructed using master share and the secret image using VC good book. The issue is found robust against many image processing attacks. The limitations with some of the VC based style is that, false alarms are not negligible for them¹³.

The other disadvantage of VC based techniques is the large area of ownership share (double of secret image), requiring extra storage space. In this paper, we have addressed this issue by avoiding use of VC for master share and ownership share design. Two issue have been developed using discrete wavelet transform (DWT) and singular value decomposition (SVD) in two different ways. A differential classification of SVD has been used to create a master share of random nature which is lot to generate ownership share using the secrete image by simple X-OR operation.

This arise the necessity of style for authentication and protection of the data area.

There are large amount of data that is distributed over the internet. This data are stored and transmitted in a digital arrangement and can easily be duplicate without loss of quality and efficiently distributed. That's why protection has become increasingly urgent.

Thus for hiding multimedia information, watermarking is a relative new style. Its application is broad, including data validation, safety of holding, broadcast monitoring etc. Basically watermarking can easily be defined as the process of inserting watermarks in digital media e.g. audio, video, image etc. using an correct algorithm. The purpose of watermark is vast including the identification of work and discourages its illigeal use etc. example, you may catch a digital picture of an event that you may consider selling to a p. However, since you are eager a human being, you might have sent the photos to bunch of different companies to make them go on a demand war. One individual that works at company may then modify the image a bit, claim that it's their original work, and actually steal it. So what are you left with? Nothing, unfortunately, because you did not know that you can protect your image even if it's in a digital format. How? You can embed extra information into digitized data to use as a protection—that is what digital watermarking is actually . It is very similar to Steganography in a number of respects. The main goal of digital image watermarking is to embed information imperceptibly and robustly in the spread data. Basically digital watermarking is lot for the security of the digital content and to protect the data from illegal use and lend the ownership right for the digital data. The efficiency of digital watermarking algorithms is totally based on the flesh of the embedded watermark against various types of attacks like cropping, low pass filter, Salt and Pepper noise and JPEG compression.

Applications of Digital Watermarking

1. **Owner ID:** It establishes ownership of the content.
2. **Copy prevent:** It prevent people from making illegal copies of copyright content.
3. **Validation of Content:** To detect modifications of the content as a sign of invalid validation.
4. **Fingerprinting:** Trace back illegal duplication and duplication of the content.
5. **telecast Monitoring:** Specially for display and in entertainment industries, to monitor content that is Telecast as declineand by the authorized source.
6. **Medical Applications:** Used to provide both validation and covertly without affecting the medical image in any way.

Literature Review of Digital Watermarking

There are many algorithms which are being used to hide the secret in-formation. These algorithms can be classified into two domains called:

- A. Spatial domain and
- B. Frequency domain.

Spatial domain watermarking slightly altered the dots of one or two randomly selected subsets of an image. On the other side, in frequency domain style the image is first shift to the frequency domain by the use of any shifting methods just as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT). Now the advised is joined to the values of its transform coefficients. After applying the inverse transform, the marked coefficients form the embedded image

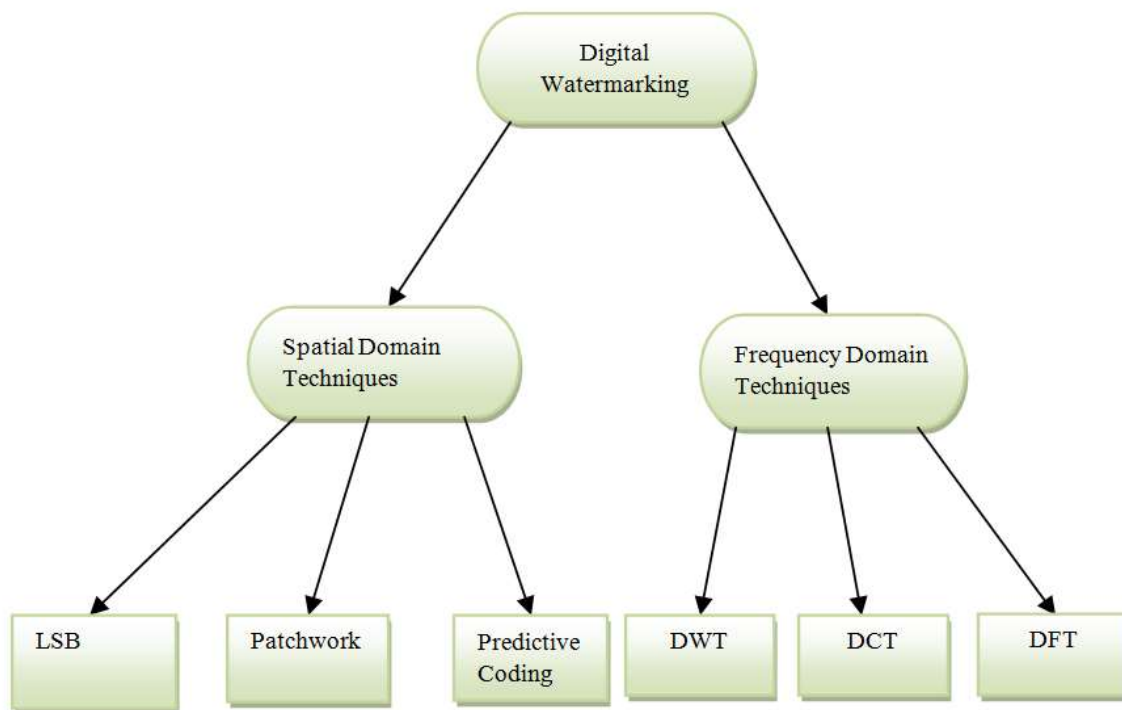


Figure 1. Classification of Digital Watermarking

A. Spatial Domain

A.1. Least Significant bit (LSB)

In this style watermark is inserted in the LSB of dot. Two types of LSB style are proposed. In the first method the LSB of the image was changed with a pseudo-noise (PN) sequence while in the second a PN sequence was joined to the LSB. This method is easy to use but not very flesh against attacks.

A.2. Patchwork Technique

In patchwork, n pairs of image points, (a,b) , were randomly chosen. The image data in a were lightened during that in b were darkened. High level of flesh against many types of attacks are lend in this style. But here in this style, very small amount of information can be hidden.

A.3. Predictive Coding Scheme

In this scheme, a pseudorandom noise (PN) pattern says $W(x, y)$ is join to cover image. It increases the flesh of watermark by increasing the gain factor. But due to high raise in gain factor, image quality may decrease.

B. Frequency Domain

B.1. Discrete Cosine Transforms (DCT)

First of all image disjointed into non overlapping slabs of 8x8. Then forward DCT is applied to each of these slabs. After that some slabs selection criteria is applied and then coefficient selection criteria is applied. Then watermark is inserted by modifying the selected coefficients and in the end inverse DCT transform is applied on each 8x8 slab.

B.2. Discrete wavelets transform (DWT)

It is more constant used due to its time/frequency characteristics. Here an image is cross through series of low pass and high pass filters which decompose the image into sub bands of different resolutions. Image is breakdown into four parts, one part is a low frequency of actual image, the one bottom left is vertical details of the actual image, the top right contains horizontal detail of the image, the bottom right slab contains high frequency of actual image. This style uses wavelet filters to transform the image.

B.3. Discrete Fourier Transforms (DFT)

It transforms a continuous function into its frequency components. Discrete Fourier transform is scaling, rotation and translation equal whereas the spatial domain DCT and DWT are not RST invariant. So DFT can be used to recover from various geometric

Watermarking Insertion and Extraction

Encoding an identifying code into a digitized signal, that signal may be music, video, picture or other file is known as digital watermarking. OR It can be defined as the case of hiding digital information in a carrier signal.

The case of watermarking insertion is as follows: First of all a suitable image is selected as a cover image. Similarly a watermark is also selected. After this that watermark is inserted in this cover image with the help of a applicable watermark embedding algorithm. We argue about various watermark embedding algorithm above in this paper. The result we obtain is the watermarked image.

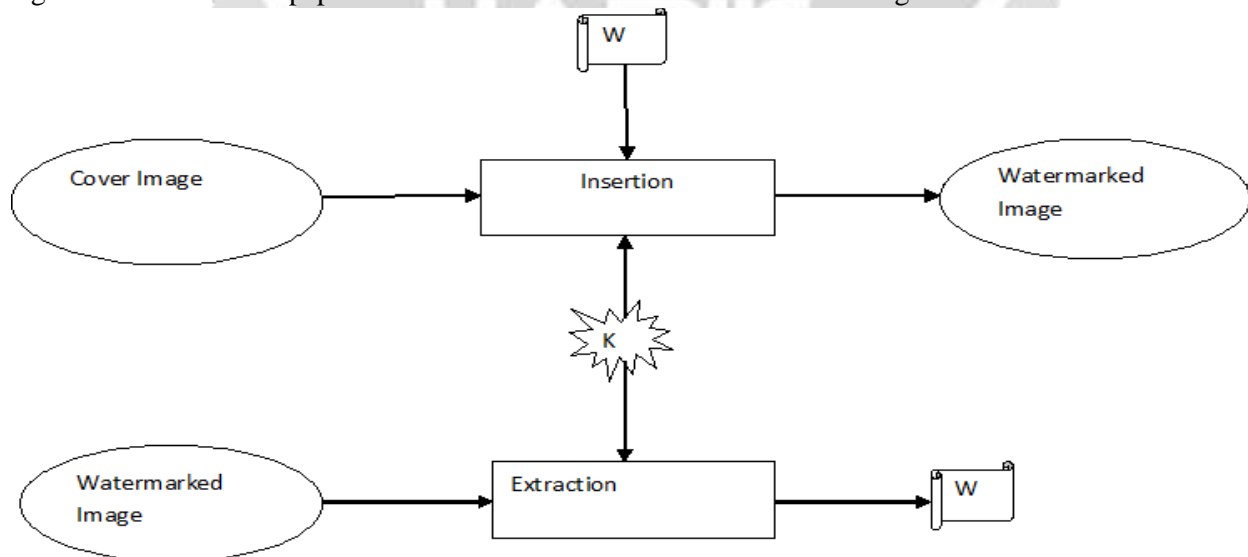


Figure 2. Insertion and Extraction of Watermarking

References

- [1] Digital Image Processing by Rafael C. Gonzalez and Richard E. Woods.
- [2] Digital Image Processing Using MATLAB by Rafael C. Gonzalez, Richard E. Woods and Steven L. Eddins.
- [3] N. Tiwari, M. K. Ramaiya and M. Sharma, “*Digital Watermarking using DWT and DES*”.
- [4] P. Mahajan and A. Kohl, “*CEET: A Compressed Encrypted & Embedded Technique for Digital Image Steganography*”, IOSR Journal Of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 vol. 16, no. 2, Ver. X (2014) March-April.
- [5] Moniruzzaman, A. K. Hawlader and F. Hossai, “*An Image Fragile Watermarking Scheme Based on Chaotic System for Image Tamper Detection*”, 3rd International Conference on Informatics, Electronics & Vision (2014).
- [6] G. V. Mane* and G. G. Chiddarwar, “*Review Paper on Video Watermarking Techniques*”, International Journal of Scientific and Research Publications, vol. 3, no. 4, (2013) April, 1 ISSN 2250-3153.
- [7] C.-C. Lai and C.-C. Tsai, “*Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition*”, IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, (2010) November.
- [8] J. Mei, S. Li and X. Tan, “*A Digital Watermarking Algorithm Based on DCT and DWT*”, IOSN 978-952-5726-00-8, Proceedings of the 2009 International Symposium on Web Information Systems And Applications (WISA'09) Nanchang, P.R. China, (2009), May 22-24, pp. 104-107.
- [9] G. S. Chandel and P. Patel, “*A Review: Image Encryption with RSA and RGB Randomized Histograms*”, International Journal of Advanced Research In Computer And Communication Engineering, vol. 2, no. 11, (2013), November.
- [10] M. Narang and S. Vashisth, “*Digital Watermarking using Discrete Wavelet Transform*”, International Journal of Computer Applications (0975 – 8887) vol. 74, no. 20, (2013) July.
- [11] N. Chaturvedi and S. J. Basha, “*Comparison of Digital Image Watermarking methods DWT & DWT-DCT on the basis of PSNR*”, International Journal Of Innovative Research in Science, Engineering and Technology, vol. 1, no. 2, (2012), December.
- [12] S. S. M. Ziabari, R. E. Atani, K. Keyghobad and A. Riazi, “*Digital Image watermarking using Edge Detection and Genetic Algorithm*”, International Journal of Scientific Engineering and Technology vol. 3, no. 1.
- [13] U. Yadav, J. P. Sharma, D. Sharma and P. K. Sharma, “*Different Watermarking Techniques And Its Applications: A Review*”, International Journal Of Scientific And Engineering Research, vol. 5, no. 4, (2014) April.
- [14] Barun Pandhwal, D S Chaudhari “*An Overview of Digital Watermarking Techniques*” International Journal Of Soft Computing And Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.
- [15] S.S.Bedi, Rakesh CAhuja, Himanshu Agarwal “*Copyright protection using video watermarking based on wavelet*”