MANTECH Publications

Journal of Digital Image Processing and Computer Vision
Volume3 Issue 1

A Review on Digital image Watermarking using DCT and DWT Techniques

Priyanka Jeswani[1], Manisha Kumari Rajoriya[2], Kanika Sharma[3]

Associate Professor[1], Assistant Professor[2, 3]

R.N Modi Engineering College, Kota

Corresponding authors' email id: *jess.priya85@gmail.com*

Abstract

In Internet world, there is a need for copyright protection of digital content. Even if it is a video files uploaded over websites. Watermarking algorithms have a basic requirement that the watermark should be imperceptible to avoid being detected and not cause visible distortion to the viewer. In this paper we aim to present a survey of two different techniques on digital image watermarking. Digital watermarking is used as a key solution to make the data transferring secure from illegal interferences. Digital watermark techniques are used in various areas such as copyright protection, broadcast monitoring and owner identification. In this paper we mainly discussed about two methods by frequency domain and spatial domain. In frequency domain such as DCT, DWT the watermark is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against watermarking attacks. In spatial domain, watermark is inserted directly by modifying the pixel values of host image.

Keywords: *Digital Image Watermarking, DCT, DWT, frequency domain, spatial domain and Algorithm*

INTRODUCTION

Digital watermarking is the embedding or hiding of information within a digital files without conspicuous ably improving the file itself. Now digital image watermarking is increasing attention because of the fast

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

developing in the internet traffic. Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data.

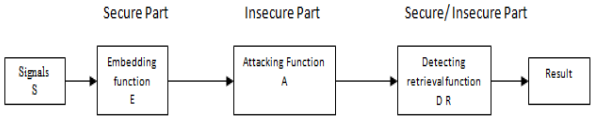


Fig – Block Diagram of Digital Watermarking

Watermarking technology can be used to embed unrestricted or restricted information. It is inserted invisible in host image so that it can be extracted for the evidence of rightful ownership [1]. Various digital watermarking techniques are purposed for copyright protection of multimedia data from being misused [2, 3]. Digital image watermarking techniques can be categorized into one of the two domains via spatial and transform. The spatial domain methods is to insert the watermark image pixels in the least significant bits (LSB) of the host image pixels [4]. Watermarking in transform domain is more secure and robust to various attacks. Watermarking using DWT and DCT methods are widely known to have gained much more popularity than any other methods. The robustness is increased by inserting in low valued coefficients with respect to attacks that have low pass characteristics such as filtering, lossy compression.

DIFFERENT TECHNIQUES OF DIGITAL WATERMARKING

In the modern era, providing authenticity is becoming increasingly important as most of the world's information is stored as readily transferable bits. Digital watermarking is a action where by inconsistent information is encoded into an image in such a way that the additional payload is undetectable to the image observer [5]. Watermarking algorithms are divided into two categories. Spatial-domain techniques work with the pixel values directly. Frequency-domain techniques employ various transforms, either local or global. Several widely recognized techniques are described subsequently [6].

A. Spatial Domain Techniques

In this technique, the watermark is inserted in the cover image changing pixels or image characteristics [33]. The algorithm should attentive weight the number of changed bits in the pixels against the possibility of the

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

watermark becoming visible [7]. Their method acted against unintentional attacks translation, rotation, arbitrary re-sectioning, scaling etc, and left artifact after intentional attacks of local and global number re-arrangement in a robust manner. This method has the ability to check the alteration of a single bit in every consecutive 8-bits length as it is parity enhanced. The robust nature of the novel method against image distortion and its significant superiority over Cox method[1] is illustrated by the results.

Lin et al [8] proposed a method to solve the problems of rotation, scale, and translation. They observed that the random transform can be employed for alternative implementation [9]. Their technique is resilient against mild jpeg compression as well.

Wei Lu and Hongtao Lu [10] provided a novel robust digital image watermarking scheme with the aid of subsampling and nonnegative matrix factorization. Originally, sub-sampling is employed to create a sub-image sequence. A Gaussian pseudo-random watermark sequence is embedded in the factorized decomposition coefficients.

Wei Lu and Hongtao Lu [10] provided a novel robust digital image watermarking scheme with the aid of subsampling and nonnegative matrix factorization. A Gaussian pseudo-random watermark sequence is embedded in the factorized decomposition coefficients.

B. Frequency Domain Techniques

Compared to spatial domain techniques, frequency domain techniques are more applied. The target of this technique is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). The discrete wavelet transforms (DWT) and the discrete cosine transforms (DCT) are implemented very effectively in numerous digital images watermarking scheme.

Al-Haj [11] presented a combined DWT-DCT digital image watermarking algorithm. Watermarking is carried out through the embedding of the watermark in the first and

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

second level DWT sub-bands of the host image sub-sequenced by the application of DCT on the selected DWT sub-bands. The most commonly used transforms are given below:

Discrete Cosine Transform

The Discrete Cosine Transform has been widely applied to solve numerous problems among the digital signal processing community and used for different application.

The most popular use of the DCT is in data compression, and it forms the basis for the well- known compression standards like JPEG image compression format for compression of still images, MPEG, for compression of motion video, MP3, for compression of audio streams and the H.263, for compression of video telephony and teleconferencing all employ the basic technique of the DCT. [12]

The Discrete Cosine Transform can be defined as the Discrete Fourier Transform of roughly twice the length, using real numbers data with even symmetry. Since DCT is real-valued, it provides a better approximation of a signal with fewer coefficients [15]. This DCT coefficients can also be used as a type of signature that is useful for recognition tasks, such as face recognition [13,14].

"The DCT decorrelates image data, after which each transform coefficient is encoded independently without losing compression efficiency."



Fig - Spatial (left) to frequency domain (right) conversion of an image

The recognition is performed using two dimensional Discrete Cosine Transform (2D -DCT) is an extension of the single dimensional discrete cosine transform (DCT) that is given by(1D-DCT)

$$c(u) = a(u)\sum_{x=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]$$

The series form of the 2D discrete cosine transform (2D DCT) is defined as:

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

$$c(u,v) = a(u)a(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos[\frac{\pi(2x+1)u}{2N}]\cos[\frac{\pi(2y+1)v}{2N}]$$

where (u) and (v) are given by=

$$a(u) = \begin{cases} \sqrt{\frac{1}{N}} & for\, u=0 \\ \sqrt{\frac{2}{N}} & for\, u\neq 0 \end{cases}$$

Discrete Wavelet Transform

Wavelet transform is a time domain localized analysis method with the window's size fixed and form convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed.

Discrete Wavelet Transform is a mathematical tool for hierarchically decomposing an image. The wavelet transform decompose the image in four channels (LL, HL, LH and HH) with the same bandwidth thus creating a multi-resolution perspective. Due to this advantage the watermark can embed in any of the frequency bands and on inverse transform the watermark will be distributed throughout the low and high frequencies as well as in the spatial domain. DWT is used a lot for watermarking and copyright protection by Shang-Lin Hsieh et al [16] [17] and many other like them [18] [19].

These algorithms are called the "wavelet based watermarking" [20]. Digital watermarking in wavelet domain presented by Taskovski et al. [21]. They implemented two watermarks using binary marks in LL2 and HH2 respectively, resulting in a mark which is robust against manipulations like compression and weak against cropping and rescaling.

G. Hai-ying et al [22] presented a watermark adapted to JPEG2000 using two algorithms to modify the wavelet coefficients of the LH2 band of the cover image, introducing only minimal differences between the watermarked image and the original.

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

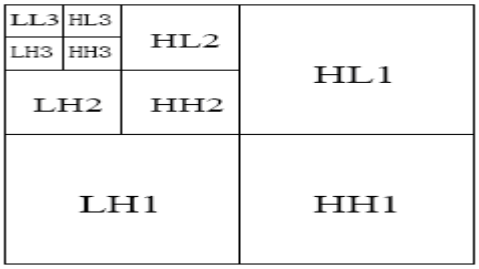


Fig : Sketch Map of Image 3 level DWT Decomposed

ATTACKS ON WATERMARKING

There are two main "reasons" or "purposes" for an attack against a watermark image:

- Hostile or malicious attacks, which are an attempt to weaken, remove or alter the watermark, and
- Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark. Lossy image compression is considered the most common form of attack a watermarking scheme has to withstand. A wide range of attacks has been described in this paper.

Removal attacks- Removal (simple) attacks attempt to separate and remove the watermark. If somebody tries to remove the watermark from the data, this is called a removal attack. Denoising the marked image through median or high-pass filtering as well as nonlinear truncation or spatial watermark prediction are methods considered very likely to succeed. The goal is to add distortion to the host image in order to render the watermark undetectable or unreadable [15].Many such attack operations have been proposed:

- Lossy image compression (JPEG, JPEG 2000)
- Addition of Gaussian noise
- Denoising
- Filtering
- Median filtering and blurring
- Signal enhancement (sharpening, contrast enhancement)

Compression: This is generally an unintentional attack, which appears very often in multimedia applications. The watermark is required to resist different levels of compression, it is usually advisable to perform the watermark embedding in the same domain where the compression takes

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

place. For instance, the Discrete Cosine Transform (DCT) domain image watermarking is more robust to Joint Photograph Expert Group (JPEG) compression than the spatial-domain watermarking. Also, the Discrete Wavelet Domain (DWT) domain watermarking is robust to JPEG 2000 compression.

Geometrical attacks-These attacks are not aimed at removing the watermark, but try to either destroy it or disable its detection. They attempt to break the correlation detection between the extracted and the original watermark sequence, where the image is subjected to translation, rotation, scaling and/or cropping. This can be accomplished by "shuffing" the pixels. The values of corresponding pixels in the attacked and the original image are the same. However, their location has changed. These attacks can be subdivided into attacks applying general affine transformations and attacks based on projective transformation. Cropping is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of video sequence.

Mosaic attack: This point is emphasized by a "presentation" attack, which is of quite general applicability and which possesses the initially remarkable property that a marked image can be unmarked and yet still rendered pixel for pixel in exactly the same way as the marked image by a standard browser. It consists of chopping an image up into a number of smaller sub images, which are embedded in a suitable sequence in a web page. Common web browsers render juxtaposed sub images stuck together, so they appear identical to the original image. Cryptographic attacks- Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is brute-force search for the embedded secret information. Practically, application of these attacks is restricted due to their high computational complexity. They cover, for example, direct attacks to find the secret key or attacks called collusion attacks. Cryptographic attacks are very similar to the attacks used in cryptography. There are the brute force attacks, which aim at finding secret information through an exhaustive search. Since many watermarking schemes use a secret key, it is very important to use keys with a secure length.

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

Protocol attacks- Protocol attacks neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather, they take advantage of semantic deficits of the watermark's implementation. The protocol attacks aim at attracting the concept of the watermarking application. The first protocol attack was proposed by Craveret al. They introduced the framework of invertible watermark and showed that for copyright protection applications watermarks need to be non-invertible. The idea of inversion consists of the fact that an attacker who has a copy of the stego-data can claim that the data contains also the attacker's watermark by subtracting his own watermark. This can create a situation of ambiguity with respect to the real ownership of the data. The requirement of non-invertability on the watermarking technology implies that it should not be possible to extract a watermark from non-watermarked image. As a solution to this problem, the authors proposed to make watermarks signal-dependent by using a one-way function. Consequently, a watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one image into another without knowledge of the secret key. It also belongs to the group of the protocol attacks.

CONCLUSION

In this paper, we have reviewed some recent algorithms, proposed a classification based on their intrinsic features, inserting methods and extraction forms. Many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with DCT and DWT. These marks are robust against several different attacks. In this paper we also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, properties of watermarking and its applications have been presented.

In future works, the use of coding and cryptography watermarks will be approached. There is a large amount of literature on these topics showing that the robustness increments can be gained through the addition of coding techniques.

REFERENCES

I. I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, "Secure Spread

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

Spectrum Watermarking for Multimedia", IEEE Transaction on Image Processing, 6(12), 1673-1687, December, 1997.

II. M.D.Swanson, M.Kobayashi and A.H.Tewfik, "Multimedia data embedding and watermarking technologies", Proc. IEEE, Vol.86, pp. 1064-1087, June 1998.

III. S.H.Low, N.F.Maxemchuk and A.M.Lapone, "Document identification for copyright protection using centroid detection", IEEE Trans. Commun., vol.46, pp. 372-383, Mar. 1998.

IV. C.I.Podilchuk and E.J.Delp, "Digital Watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, pp.33-46, July 2001.

V. Md. Mahfuzur Rahman and Koichi Harada, "Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data", IJCHNS International Journal of Computer Science and Network Security, Vol. 6, No. 2A, February 2006.

VI. M. Hamad Hassan, and A.A.M.Gilani, "A Fragile Watermarking Scheme for Color Image Authentication", International Journal of Applied Science, Engineering and Technology, Vol. 1, No. 3, pp.-156-160, 2005.

VII. M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection, Artech House, 2003.

VIII. C. Lin, M.Wu, Y.M. Lui, J.A Bloom, M.L. Miller, I .J. Cox, "Rotation, Scale, and Translation Resilient Public Watermarking for Images", IEEE Transactions on Image Processing, Vol. 10, No. 5, pp. 767-782, 2001.

IX. R. N. Bracewell, "The Fourier Transform and Its Applications", New York: McGraw-Hill, 1986.

X. Wei Lu, Hongtao Lu, "Robust watermarking based on sub-

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

sampling and nonnegative matrix factorization", Informatica, Vol. 19, No. 4, pp. 555- 566, December 2008.

XI. Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, Vol. 3, No. 9, pp. 740-746, 2007.

XII. The Discrete Cosine Transform, DCT for Compression. Retrieved 27 February 2007.

XIII. Shutao Li, James T. Kwok & Yaonan wang, "Combination of images with diverse focuses using the spatial frequency", Information Fusion, 2(3) pp,167-176,2001.

XIV. V.P.S Naidu, JR. Rao "Pixel-Level Image Fusion Using Wavelets and Principal components analysis," Defence Science Journal, pp 338-352,2008.

XV. Mahendra Kumar et.al., "Digital Image Watermarking using Fractional Fourier transform via image compression", In IEEE International Conference on Computational Intelligence and Computing Research 2013 (IEEE ICCIC-2013), 26-28 Dec., 2013.

XVI. Shang-Lin Hsieh and Bin-Yuan Huang, "A Copyright Protection Scheme for Gray-Level Images Based on Image Secret Sharing and Wavelet Transformation", Proceedings of International Computer Symposium, Dec. 2004.

XVII. Shang-Lin Hsieh and Lung-Yao Hsu, "A Copyright Protection Scheme for Color Image Using Secret Sharing and Wavelet Transform", Master Thesis, Tatung University, July 2005.

XVIII. Ju Liu, Xingang Zhang and Jiande Sun, "A new image watermarking scheme based on DWT and ICA", Proceedings of IEEE International Conference Neural Networks and Signal Processing, China, December 2003.

XIX. Wang Hongjun and Li Na, "An algorithm of digital image watermark based on multiresolution wavelet analysis", IEEE

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved

International workshop on VLSI Design and Video Technology, China, May 2005.

XX. V.M. Potdar, S.Han and E.Chang, "A survey of digital image watermarking techniques", 3rd IEEE International conference on Industrial Informatics, pp. 709-716, 2005.

XXI. D. Taskovski, S. Bogdanova, and M. Bogdanov, "Digital watermarking in wavelet domain", First IEEE Balkan Conference on Signal Processing, Communication, Circuits, and Systems, 2000.

XXII. G. Hai-ying, L.Guo-qiang, L.Xu, and X.Yin, "A robust watermark algorithm for jpeg2000 images", Fifth International Conference on Information Assurance and Security, 2009.

Page 1-7 © MANTECH PUBLICATIONS 2018. All Rights Reserved