International Journal of Innovative Research in Technology & Science
ISSN: 2321-1156 Volume VIII Issue III, May 2020

A Survey on Digital Image Watermarking Method DCT and DWT

Akhaleshvari Jhade[1], Kedar Nath Singh[2]; *Computer Science and Engineering Department, TITS, Bhopal, M.P., India;*
[1]akhaleshvarijhade@gmail.com, [2]cseknsingh@gmail.com

Abstract--improvement in imaging technology and the ease with which digital content can be reproduced and manipulated, there is a strong need for a digital copyright mechanism to be put in place. There is a need for authentication of the content as well as the owner. It has become easier for malicious parties to make scalable copies of copyrighted content with any compensation to the content owner. Digital Watermarking is being seen as a potential solution to this problem. Different watermarking schemes have been proposed, but attacks on a watermarked image are distortions in the watermarked image. These attacks may be intentional or unintentional; the attacks are classified as geometric attacks. This paper presents a comprehensive survey of the current techniques that have been developed and their effectiveness. Digital watermarking was developed to provide the copyright protection and owners' authentication. Digital image watermarking is a method for embedding some data into digital image sequences. E.g. Text image, image data, in this paper, the survey on image watermarking and its methods, Attacks on watermarking, classification of watermarking, and applications. We aim to produce a comprehensive review of the existing literature available on DCT and DWT based mostly on digital image watermarking, to develop a useful digital image watermarking methodology.

Keywords: Watermarking, Transform Domain Technique, DCT, DWT, Visibility, Security, Robustness.

I. Introduction

The rapid development of computer communication and the Internet makes it very easy to lose exchange data via networks. On the other hand, it also becomes crucial to protect the digital copyright of various digital media. Watermarking has been studied for more than ten years as a possible solution for the issue. In addition to copyright protection, watermarking can also be designed for other purposes such as hiding communication, data authentication, data tracing). Many data types can be used as the cover data for watermarking, e.g., digital image, audio, video, text, bar-code, 3D model, CAD data, 2D vector data, software, VLSI [1]. The field of digital watermarking is rather new; indeed, at this point, many of its terms are not well defined. They define watermarking to be a process that embeds data, called a watermark into a multimedia object, to help protect the owner's rights to that object. A digitally watermarked image is obtained by invisibly hiding signature information into the host image. The signature is recovered using an appropriate decoding process. The challenge is to ensure that the watermarked image is perceptually indistinguishable from the original and that the signature is recoverable even when the watermarked image has been compressed or transformed by standard image processing operations. This paper describes various digital watermark algorithms studying their strengths and weaknesses, considering texture, luminance, corner, and edge information in the image to generate a mask that makes the addition of the watermark less perceptible to the human eye. The operation of embedding and extraction of the watermark is done in both the spatial and the frequency domain, thereby providing us information about the robustness against frequent attacks, including image compression and filtering. We use pseudo-random sequences to embed the watermark. Weighted Peak Signal to Noise Ratio is used to evaluate the perceptual change between the original and the watermarked image [2].

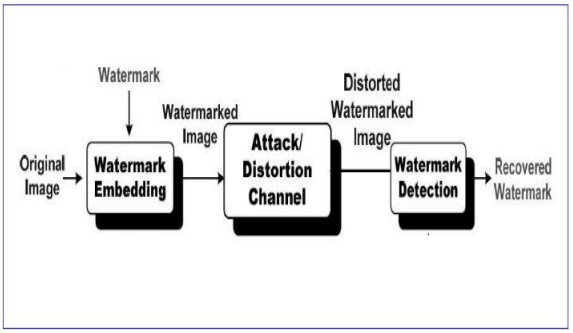

Fig1: Watermarking Diagram

Types of Transform Domain Technique: There are several transform domain watermarking Technologies available in the literature

1. Discrete Cosine Transform -The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation. A pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. Bors and Pitas developed a method that modifies 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, a lot of watermarking algorithms in the frequency domain have been proposed. The popular block-based DCT transform segments image non-overlapping blocks and apply DCT to each block. These results in giving three frequency sub-bands: low-frequency sub-band, mid-frequency sub-band, and high-frequency sub-bands. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band, which contains the most important visual parts of the image. The second fact is that high-frequency components of the image are usually removed through compression and noise

attacks. The watermark is therefore embedded by modifying the coefficients of the middle-frequency sub-band so that the visibility of the image will not be affected, and the watermark will not be removed by compression [3].

2. Discrete Wavelet Transform- the DWT (Discrete Wavelet Transform) separates an image into four components, a lower resolution approximation image (LL), a horizontal (HL), a vertical (LH) and a diagonal (HH) detail component. The process can then be repeated to computes multiple "scale" wavelet decompositions. Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for the processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike a conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses the suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. For 2-D images, applying DWT corresponds [4].

3. Singular Value Decomposition-SVD as a general linear algebra technique, is used in a variety of applications. SVD is optimal matrix decomposition in a least-square sense packing the maximum signal energy into a few coefficients as possible. The SVD theorem decomposes a digital image A of size $M \times N$, as: $A = USVT$, (1) where U and V are of size $M \times M$, and $N \times N$, respectively. S is a diagonal matrix containing the singular values. In the watermarking trial, SVD is applied to the image matrix; then, watermark resides by altering singular values (SVs)" [5].

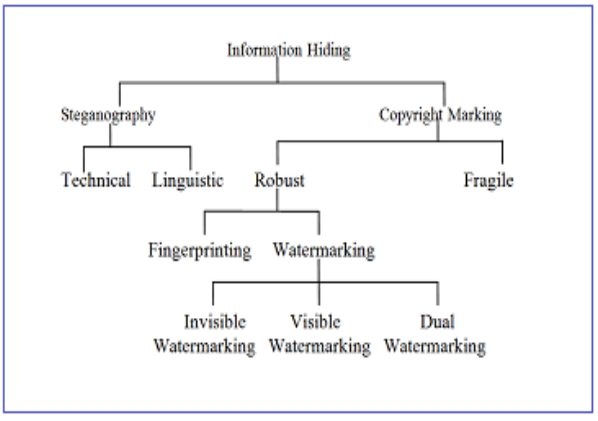

Fig2: Types of Watermarking

Category of Watermarking: Digital image watermarking has constituted into three classes, consequently supported the various watermarks.
1. Visible Watermarking -These are the logos concept enlargement. These sorts of watermarks are solely applicable to the pictures. A transparency criterion evolves once these logos are embedded into the still pictures. The watermarks happiness to the current class is exhausting to get rid of or alter once cropping attack falls.
2. Invisible Watermarking -As the name clears its which means the watermark should be hidden from the surface world. The detection of those sorts of the watermark will solely be done by the upper authority or agencies. The watermarks happiness to the current class is utilized by the author authentication or creator or possession and for locating the unauthorized person.
3. Fragile Watermarking- These are known as by the name of the tamper-proof watermarks. The watermarks hapless to the current class are shattered by the info management. The image, while not watermark, indicates that a trial has been created on the initial image, and forgery has evolved within the absence of watermark.

Applications of watermarking
1. Integrity Verification or Copyright Protection -When a new image is created, copyright information can be inserted as a watermark. In case of a dispute of ownership, this watermark can provide evidence.
2. Corrupt detection -Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates the presence of tampering, and hence digital content cannot be trusted.
3. Content Authentications: Content authentication is able to detect any change in digital content. This can be achieved through the use of a fragile or semi-fragile watermark, which has low robustness to modification in an image.
4. Content Descriptions: This watermark can contain some detailed information on the host image, such as labeling and captioning. For this kind of application, the capacity of the watermark should be relatively large, and there is no strict requirement of robustness.
5. Communications Authentications -It includes the exchange of messages secretly embedded within images. In this case, the main requirement is that hidden data should not be identified [6].

Attacks on Watermarking
Fragile watermarks are ready to be destroyed by random Image processing methods. The change in the watermark is easy to be detected, thus can provide information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from the heavily attacked watermarked image. Thus it is preferred in copyright protection. Attacks on a watermarked image are distortions in the watermarked image. These attacks may be intentional or unintentional. An image watermarking method can be judged against such relevant attacks. The attacks are broadly classified as geometric attacks.
Geometric Attacks: Geometric attacks include basic geometric transformations in an image. These include geometrical distortions like rotation, scaling, translation, cropping, row-column blanking, warping, etc. Geometric attacks attempt to destroy

synchronization of detection, thus making the detection process difficult and even impossible [7].

II. Literature Survey

A literature survey is the most significant step in the software improvement process. Before developing the tool, it is necessary to define the time factor economy and company power. Once these things are satisfied, then the next step is to define which operating system and semantic can be used for developing the tool; once the programmers start building the tool, the programmer wants a lot of external support. This support can be achieved from senior programmers, from the book or from websites. Before constructing the system, the above thoughts are taken into account for developing the proposed system

In Paper [8], T. K. Leung et al. present a new Steganography technique based on the spatial domain for encoding additional information in a picture by making small alterations to its pixels. The proposed technique concentrations on one specific popular technique, Least Significant Bit (LSB) Embedding. In place of using the LSB-1 of the cover for embedding the message, LSB-2 has been used to increase the robustness.

In paper [9] X. Li et al., examines the opportunity of usage of Genetic Algorithms (GA) for data hiding in digital images. Two spatial domain data hiding approaches are planned where GA is used distinctly for (i) improvement in discovery and (ii) optimum imperceptibility of secreted data in digital pictures, respectively.

In paper [10], Ankur Goyal et al. developed a technique for hiding information using LSB steganography and cryptography where the secret information is encrypted first using RSA or Diffie Hellman algorithm and then the encrypted ASCII value is converted to binary form. Here even the cover image is converted from pixels to binary form, and then the secret message is embedded in the cover image using the LSB technique, and the stego image is formed. With the proposed method, the time complexity is increased, but high security is achieved at that cost.

In paper [11], Ali Al-Ataby et al. developed a modified LSB method in which text message to be hidden is treated as 8 bit ASCII codes. Using encryption algorithms, these codes are then converted into 5-bit codes and then hidden in a cover image using LSB. As the encryption algorithm used, if anyone extracts bits from an image, he won't understand until he decrypts it. So with this technique, more information can be hidden with a level of protection.

In paper [12], Tanmay Bhattacharya et al. proposed a DWT based Dual steganographic technique. Using DWT, a cover image is decomposed into four sub-bands. Two secret images are hidden within HL and HH sub-bands, respectively, by using a pseudo-random sequence and a session key. After embedding the secret data, all four sub-bands, including two modified sub-bands, are combined to produce the stego image using IDWT. By this method, a large amount of information is transferred in a more secure way and also has an acceptable level of imperceptibility.

In paper [13] Amritha G. et al. proposed method steganography is object-oriented as it is based on one of the features of an image. Here the feature used is the skin region of the image. Instead of using a full cover image, embedding data only within the skin regions provide an excellent secure location for data hiding. Encrypt secret image using the RC4 algorithm before embedding enhances the security level. In this cover image is converted to HSV form to detect the skin color. After that skin segment is detected and cropped. That region is transformed into a DWT form and secret image encrypted with the RC4 cryptography algorithm. This encrypted data embedded within the high-frequency sub-band of the cover image and IDWT is performed. At last, by merging this segment stego image is generated.

In paper [14], Raval and Rage et al. introduced a multiple marking algorithm. In which DWT is applied after the decomposition of the main image. To achieve a high level of robustness, multiple watermarks are inserted into the high-frequency subbands and low-frequency sub-bands. However, this plan is extremely robust against many malicious attacks, but achieving a watermark is not up to the mark. This method is visible to all, and the main image is mandatory to be present during the extraction process.

In paper [15], Ghazy et al., has proposed the method which divides the image into non-overlapping blocks, and then SVD is applied on these blocks. Only singular values of these bocks were used to implant the watermark n the main image. The implementations of this algorithm provides better result against different attacks like compression, filtering, noise but are not efficient against the attacks like cropping and geometric attacks.

In paper [16], Chandra et al., proposed a non-blind digital image watermarking scheme using the spatial domain technique. The singular values of the watermark images are inserted into the singular values of the original image. On the other hand, this scheme proposed by the author does not hold good transparency and is not strong against the geometric attacks.

III. Expected Outcome

Our main objectives in research visually undetectable, achieving the desired robustness through PSNR values, are better in DCT watermarking method. It is a reliable digital image and authentication. It is a good robustness and ownership.

VI. Conclusion

In this paper, I have introduced some basic concepts in Digital watermarking, including its foundation, properties, requirements as well as the comparison

between digital watermark techniques. Schemes in the frequency domain and wavelet domain and digital watermarking techniques like DCT, DWT, and SVD their advantages, disadvantages, and applications. Both embedding and extraction of a watermark is being done using the techniques. For checking the robustness of these methods, various attacks on watermarked images are performed, Noise, Rotation, Gaussian noise, and unsharing. The existing method shows not better results among these methods compared in terms of PSNR after an attack on the watermarked image. Different techniques for digital image watermarking have been introduced, which are very efficient and robust in the sense of image quality after the watermark is extracted from the image. The techniques used are DCT, DWT, and SVD. The work can be extended in the proposed method and overcome the effect of various attacks such as Gaussian noise on the watermarked images.

Reference

[1]. A. Bors and I. Pitas, "Image watermarking using DCT domain constraints." in *Proc. IEEE. Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, pp. 231-234

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

[3]. N Chaturvedi, 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, Issue 2, Page no 147, December 2012.

[4]. Perez-Gonzalez, F.; Hernandez, J.R.;" A tutorial on digital watermarking" Security Technology, Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on. Oct. 1999, Page(s):286 – 292, 1999.

[5]. A Mansouri, A Mahmoudi Aznaveh And F Torkamani Azar ,"SVD-based digital image watermarking using complex wavelet transform'Vol. 34, Part 3, June 2009, pp. 393–406.

[6]. Amitava Nag, Sushanta Biswas, Debasree Sarkar, and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Human Encoding," International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6).

[7]. W. H. Lin, Y.R. Wang, And S.J. Horng, A wavelet tree-based watermarking method using distance vector of binary cluster, Expert System with Applications, vol. 36, no. 6, pp. 9896-9878, 2009.

[8]. A. A. Efros and T. K. Leung, "Texture synthesis by non-parametric sampling," Sep.1999.

[9]. X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogram shifting-based reversible data hiding," June 2013.

[10]. Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography," International Journal Modern Education and Computer Science, Vol. 6, pp. 27-34, June 2012.

[11]. Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform," The International Arab Journal of Information Technology, Vol.7, October 2010.

[12]. Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, "A Novel Session-Based Dual Steganographic Technique Using DWT and Spread Spectrum" International Journal of Modern Engineering Research, Vol.1, pp. 157- 161, 2012.

[13]. Amritha G., Meethu Varkey, "Biometric Steganographic Technique Using DWT and Encryption," International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 3, pp. 566-572, March 2013.

[14]. M.S. Raval and P.P. Rege, Discrete Wavelet Transform based multiple watermarking scheme. *Proc. Of the IEEE TENCON conf. for Convergent Technologies for Asia-Pacific Region*, Bangalore India, Vol.3, pp. 935-938, 2003.

[15]. Ghazy R A, El-Fishawy N A, Hadhoud M M, Dessouky M I, and El-Samie F E A 2007 An efficient block by -block SVD-based image watermarking scheme. *Radio Science Conference*, NRSC 1–9.

[16]. D.S. Chandra, Digital image watermarking using singular value decomposition, proc. Of 45th Midwest Symposium on circuits and systems (MWSCAS'02), Tulsa, OK, USA, Vol. 3, pp. 264-267, 2002.