International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 06 (NOVEMBER -DECEMBER, 2017)

Gray Scale Image Authentication System Based on Discrete Cosine Transforms Against Different Attack: A Survey

Dolly Sakare [1], Prof.Ratan Singh Rajput[2]
Department of Computer Science & Engineering
RGPM, Bhopal, M.P., India
dolly.sakre92@gmail.com, mr.ratan.proff@gmail.com

Abstract- *A secure image watermarking against different attack and digital watermarking is weak to various attacks in spatial domain, thus in most of the watermarking technique's transform domain is used. Digital watermarking has applications in several areas like broadcast monitoring, copy right protection etc. digital Image Watermarking is that the method .the owner of a copyright holder in a digital image watermarking works for copyright protection. Digital image watermarking quality is effect of DWT. Discrete cosine transforms based totally image watermarking technique; classification and analysis of distinct cosine transform based watermarking techniques. A secure image watermarking technique has proposed a bit replacements technique based on the method of watermark embedding and extraction is also given host image. It's not visible watermark .Digital watermarking will be used to protect digital info from illegal and it's additionally good robust in digital image.*

Keywords—*Watermarking, Visibility, Frequency domain, Robustness, Discrete cosine Transform, Reversible data hiding, PSNR.*

I. Introduction

The digital communication technology, like internet technology confronts various troubles related to the privacy and security of the data. Security techniques are required because of illegal access of data without permission. Therefore, it is necessary to protect data in the internet technology. For providing the security of digital data various techniques are used like encryption, decryption, cryptography, steganography and digital watermarking. In this paper discusses about the digital watermarking. The digital watermarking is an application of the digital image processing. The digital watermarking is a process of information hiding. There are various techniques for hiding the information in the form of digital contents like image, text, audio and video. Basically digital watermarking is a method for embedding some secret information and additional information in the cover image which can later be extracted or detected for various purposes like authentication, owner identification, content protection and copyright protection, etc. Sometimes the scaling factor is also used for embedding the watermark in the cover image. The digital watermarking is used for the security of the digital content and to protect the data from illegal users and provides the ownership right for the digital data. An important characteristic of digital watermarking is robustness and imperceptibility against various types of attacks or common image manipulation like rotation, filtering, scaling, cropping and compression. The efficiency of digital watermarking algorithms is totally based on the robustness of the embedded watermark against various types of attacks. Digital watermarking is a method used to improve the ownership over image by replacing low level signal directly into image. Digital watermarking method is also used for the tamper proofing and authentication [1].

1.1 Process of Digital image Watermarking

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself [2].

1.2 Requirements of Digital image Watermarking

The major requirements for digital watermarking are:

1. Robustness: This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and intentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks [3].

2. Data Load: This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the watermark during extraction.

3 Reliability: Watermark should be able to provide complete & reliable information for proving ownership of copyright products. The watermarking technique should be giving the reliability of recovery of watermark. The robustness of the watermarking technique is dependent upon how securely and intelligently the watermark is embedded into the host signal without any noticeable change. Robustness of the algorithm to attacks and quality of the watermarked image are related properties that are indispensable. All applications presupposing protection and use in verification of the watermarking systems require this type of marking in order to survive any kind of alterations or intentional removal introduced by standard or malicious processing and attacks [4].

4. Perceptual Transparency: The main requirement of watermarking is perceptual transparency. The watermark which has embedded as the owner's information should not degrade the quality of the host signal. The watermark cannot be seen by human eye. It can be detected by special processing or dedicated algorithms [5].

1.3 Applications of Watermarking

1. Authentication: Watermark is used to provide authentication. Providing an incorrect watermarked image can either destroy the watermark or leads to incorrect watermark after extraction.

2. Digital Signatures*:* Watermarks may be used to identify the owner of the content. By having this information the user may contact the owner for acquiring the legal rights to copy or using the content [6].

3. Copy Control*:* Watermark may contain information required by the content owner that decided the policy of copying the digital content. The information contained by the watermark may specify „content may not be copied" or „only one copy" etc. subsequently, the devices used for copying the content may be required by law to contain watermark detector, which follows directives given by the content owner [7].

4. Broadcast Monitoring*:* Automatic identification of owners of data may be required to be done and used in systems responsible for monitoring the broadcasts. This may help in deciding the royalty payments. It also helps in ensuring that commercials of a particular advertiser are played at right time and for a right duration.

1.4 Attacks on Watermarked Image

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing soft ware's made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under.

1. Geometric Attacks: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack. 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.

2. Noise Attack: In this attack, add noise to the watermark image were 0.002, 0.01, 0.08, 0.1, 0.005, 0.4, and 0.3. The extracted watermarks are affected Confuses the mark detector.

3. Smoothing Attack: Smoothing filters tend to blur an image, because pixel intensity values that are significantly higher or lower than the surrounding neighborhood would "smear" across the area [8].

1.4 Limitations of DCT

1. DCT is main a Block effect
2 .Effect of picture cropping
3. The main problems and the analysis of the DCT is the blocking effect. In DCT images are broken into blocks 8x8 or 16x16. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking effect [9].

II. Literature Survey

Bartolini F et al. [10]. Have developed an improved wavelet-based watermarking through pixel-wise masking. It is based on masking watermark according to characteristics of HVS. The watermark is adaptively added to the largest detail bands. The watermark weighing function is calculated as a simple product of data extracted from HVS model. The watermark is detected by correlation.

S. Hong et al. [11]. A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents. In this paper, algorithm for embedding watermarking is presented. Firstly, the original image is compressed into JPEG image and generates the

watermark by using the 2D barcode and scrambling. Secondly, JPEG image is decayed into 3 sub bands: H, V and D by using 2D DWT. Thirdly, the DFRNT (discrete fractional random transform) are performed on the sub-band coefficients. And then, watermark image is embedded into the sub-band coefficient value using quantization technique. Fourthly, the inverse DFRNT and inverse DWT is performed and lastly watermark JPEG image is obtained. The proposed algorithm has good invisibility and extraction performance, and ensures robustness

Guzman, Meana et al. [12]. Have developed an algorithm that relies upon adaptive image watermarking in high resolution sub-bands of DWT. Weighting function is the product expression of data extracted from the HVS model.

K.R. Rao et al. [13]. Developed a wavelet based image adaptive watermarking scheme. Embedding is performed in the higher level sub-bands of wavelet transform, even though this can clearly change the image fidelity. In order to avoid perceptual degradation of image, the watermark insertion is carefully performed while using HVS.

Ching-Chin Tsai et al. [14]. Proposed Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. A hybrid image-watermarking technique based on DWT and SVD has been presented, where the watermark is embedded on the singular values of the cover image's DWT sub band. The main objective of developing this technique is to satisfy both imperceptibility and robustness.

Li Na et al. [15]. Have proposed a DWT based method in which watermark was embedded in middle frequency coefficient using α as flexing factor with $\alpha = \beta |m|$, where m is mean value of all coefficients watermarking embedded. But this method doesn't provide enough security.

Amitav Mahapatra et al. [16]. described a survey on digital watermarking techniques, the idea behind this survey is to study different kind of watermarking techniques and present a robust watermark data using DWT and introduce fragile and semi-fragile watermarking techniques.

Ali Al-Haj et al. [17]. Combined DWT-DCT Digital Image Watermarking In this paper, Watermarking is done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of the two transforms improves the watermarking performance considerably when it is compared to the DWT-Only watermarking approach.

D. Vinita Gupta et al. [18]. Robust and Secured Image Watermarking using DWT and Encryption with QR Codes [4]. In this Paper, algorithm for embedding watermarking is presented by using DWT and encrypted with QR codes. Here cover image is selected and DWT is applied on it. A key K is selected to generate the QR code as secret key. QR code and watermark image is encrypted by using XOR operation. Then the encrypted watermark is embedded into the cover image and inverse DWT is applied on the embedded watermark image. For extraction, simply apply the DWT on the cover image. This algorithm is quite simple because of the use of simple X-OR operation for encryption. This algorithm is suitable on different kind of attacks on watermarked images like JPEG Compression, Possion Noise Attack, Salt & Pepper Noise and Gaussian Noise.

Kim et al. [19]. Proposed a watermarking method using the human visual system based on wavelet transform. The number of watermark elements is proportional to the energy contained in each wavelet transform bands. To estimate the characteristic of the image, the changing rate of a sinusoidal pattern per subtended visual angle in cycles per degree is calculated. The result is used as the visual weight of watermarks in each wavelet transform band.

III. Expected Outcome

Digital watermarking method provides a reliable digital image. It is providing good protected digital image. It is good robustness and ownership. It is providing secures in data hiding in digital image.

VI. Conclusion

In study of digital watermarking like indication, framework, techniques, applications, challenges and limitations. In search focuses on data hiding and this paper focuses on digital image in frequency domain and digital watermarking techniques like DCT, DWT their advantages, disadvantages and applications. Both embedding and extraction of watermark is being done using the techniques. For checking the robustness of these methods various attacks on watermarked images are performed Noise, Rotation, noise and unshipping watermark embedded. Hence we have concluded that if genetic algorithm is being applied in the digital watermarking, the image becomes low robust and the watermarked quality is also improved. DCT-DWT shows better results among these methods compared in terms of PSNR after attack on watermarked image.

Reference

[1]. N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE 2013.

[2]. Sasmita Mishra, Amitav Mahapatra, Pranati Mishra, "A Survey on Digital Watermarking Techniques", International Journal of

Computer Science and Information Technologies, Vol. 4 (3), 451-456, 2013.

[3]. T.H. Chen, D.S. Tsai, Owner–customer right protection mechanism using a watermarking scheme and a watermarking protocol, Pattern Recognition 39 (8) 1530–1541, 2006.

[4]. P. Loo, N. Kingsbury, Watermark detection based on the properties of error control codes, IEE Proc. Vis. Image Signal Process. 150 (2) 115–121, 2003.

[5]. P.W. Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Trans. Image Process. 10 (10) 1593–1601, 2001.

[6]. Tribhuwan Kumar Tewari, VikasSaxena, Prof. J P Gupta "Audio Watermarking: Current State of Art and Future Objectives" IJCTA, Volume 5, Number 7, July 2011.

[7]. I. Cox, M. Miller, et al. "Digital watermarking and Steganography", Morgan Kaufmann, 2008.

[8]. 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.

[9]. Anu Bajaj, "Robust And Reversible Digital Image Watermarking Technique Based On RDWT-DCT-SVD", IEEE International Conference on Advances in Engineering & Technology Research (ICAETR), 2014.

[10]. Barni M, Bartolini F, Piva, "An Improved Wavelet Based Watermarking Through Pixel wise Masking", IEEE transactions on image processing, Vol. 10, pp.783-791, 2001.

[11]. M. Kim, D. Li, and S. Hong, —A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents‖ :Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I WCECS 2013, 23-25 October, San Francisco, USA, 2013.

[12]. Victor V., Guzman, Meana, "Analysis of a Wavelet-based Watermarking Algorithm", IEEE Proceedings of the International Conference on Electronics, Communications and Computer, pp. 283-287, 2004.

[13]. N. Kaewkamnerd and K.R. Rao, "Wavelet Based Image Adaptive Watermarking Scheme", IEEE Electronic Letters, Vol. 36, pp.312-313, Feb. 2000.

[14]. Chih-Chin Lai, Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transaction on Instrumentation and Measurement", vol. 59, no. 11, November 2010.

[15]. Wang Hongjun, Li Na," An algorithm of digital image watermark based on multi-resolution wavelet analysis", International Workshop on VLSI Design and Video Technology, Proceedings, pp: 272- 275, 28-30 May 2005.

[16]. Sasmita Mishra, Amitav Mahapatra, Pranati Mishra, "A Survey on Digital Watermarking Techniques", International Journal of Computer Science and Information Technologies, Vol. 4(3), 451-456, 2013.

[17]. Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science 3 (9): 740-746, 2007.

[18]. Vinita Gupta, Atul Barve, "Robust and Secured Image Watermarking using DWT and Encryption with QR Codes, International Journal of Computer Applications (0975 – 8887)Volume 100 – No.14, August 2014.

[19]. Kim, Y.S., Kwon, O.-H., and Park, R.-H., "Wavelet Based Watermarking Method for Digital Images Using the Human Visual System," IEE Electronics Letters, Vol. 35, No. 6, pp. 466-468, 1999.