International Journal of Digital Information and Wireless Communications: STUDY OF THE EFFECTED GENETIC WATERMARKING ROBUSTNESS UNDER DCT AND DWT DOMAINS

Abduljabbar Shaamala[1], Azizah A. Manaf[2]
[1] faculty of Computer Science and Information Technology, Universiti Teknologi Malaysia (UTM), Johor, Malaysia, hmsabduljabbar3@live.utm.my
[2] Advanced Informatics School (AIS), Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia, azizah07@ic.utm.my

ABSTRACT

Watermarking becomes the suitable technology to protect multimedia in digital world. Watermarking using genetic algorithm for the optimization of the tread-off between the watermarking requirements has attracted the attention of researchers; amongst the watermarking requirements, the robustness is an important one. Watermarking embedded in frequency domain using DWT or DCT can affect the robustness of watermarking, this paper studies the effect of embedding domain on the robustness in genetic watermarking. Results of attacks based on numerical correlation (NC) is analyzed through the paper sections, the DWT results showed more robustness than DCT in watermarking based on GA

KEYWORDS

Watermarking, genetic algorithm. DWT, DCT.

1 PAPER PREPARATION

With the explosive growth of the Internet in recent years have become progressively advanced in the rapidly growing field of internet application, data securities, including copyright protection and data integrity detection, have become a vast concern. One key for achieving information security is digital watermarking, which embeds hidden information or secret data in the image [1]. This technology works as a suitable tool for identifying the source, creator, owner, distributor, or authorized consumer of a document or image. Watermarking can also be used to detect a document or image is illegally distributed or modified [2].

Watermark techniques can be divided into two groups: Visible and invisible, the visible watermark is used if embedded watermark is intended to be seen by human eyes, For example, a logo inserted into corner of an image. While the invisible watermark is embedded into a host image by sophisticated algorithms and is invisible to the human eyes [3]. In digital right management (DRM) systems, encryption and robust watermarking are two major schemes for applications [4], the encrypted digital if one bit is received erroneously during transmission, part or whole of received data would not be decrypted, leading to the uselessness of such contents. For robust watermarking, the watermarked contents and their original counterparts look similar, or even identical from subjective point of view. During the transmission, if some parts are received in error, the received contents can partly be recognized and the copyright can be preserved [1].

Watermarking techniques also can be classified according to its robust as robust, semi-fragile and fragile [3], Robust watermarks are designed to survive intentional (malicious) and unintentional (non-malicious) modifications of the watermarked image [5],[7], Semi-fragile watermarks are layout for detecting any unauthorized alteration, and allowing in the same time some image processing operations [8],[9]. On the contrary, a watermarking technique that cannot robust against noise or attacks is called fragile technique [3]. Fragile watermarking techniques are concerned with complete integrity verification. Furthermore, watermarking techniques can be classified as blind and non-blind. Blind watermarking [10] techniques don't require access to the original unwatermarked data (image, video, audio, etc.) to recover the watermark. In contrast, non-blind watermarking technique requires the original data [3],[10] needed for extraction of the watermarked. In general, the non-blind scheme is more robust than the blind watermark as it is obvious that the watermark can be extracted easily by knowing the unwatermarked data.

According to the embedding, watermarking techniques divided into two embedding domain, spatial domain and frequency domain [3],[10]. The main concept of spatial domain [11] is to insert a watermark into an image by modifying the gray value of certain pixels in the image [12],[13]. The classical methods are to modify the last significant bits (LSB) of specific pixels of the host image based on the watermark bits [3].For frequency domain, the main concept to insert a watermark into frequency coefficients of the transformed image using the discrete cosine transform (DCT), the discrete wavelet transform (DWT) [14], or other kind of transforms techniques [3], [10].

There are requirements and constraints in design effective watermarking algorithms the three fundamental amongst it are,

- Imperceptibility: should the difference between the watermarked image and the original image not noticeable and visible by human eyes,
- Robustness: is the ability of watermarking to survive and withstand any intentional or unintentional attacks,
- Capacity: is the number of bits embedded into the original image.

The above watermarking requirements are conflicting with each other. If watermark is embedding bits into higher frequency coefficient would change the image as little as possible and achieve the imperceptibility. However, that would reduce the robustness since the watermarked image may experience filtering and the hidden watermark may be vanished. Also if watermark is Embedding bits into lower frequency coefficient would increase the robustness. However, this would sacrifice the imperceptibility [15],[4]. The watermarking problem can be viewed as an optimization problem. Therefore, genetic algorithm (GA) can be used for solving such problem [16] [17].

In this paper we present the effectiveness of embedding domain in the robustness of genetic watermarking. Section 2 briefly describes DWT and DCT embedding domain. Then an overview about genetic algorithm (GA) and some related watermark using genetic algorithm are briefly reviewed. In section 3 we disuse some result of previous works and compare attacks results of it in order to identify the robust embedding domain in watermarking using GA.

2 Digital Watermarking Applications

There are many application of digital watermarking as following:

i. Copyright protection. Digital watermark embedded within the host signal can be retrieved later to assert the owner's copyright over the marked media.

ii. Fingerprinting. The owner of a digital content can choose to embed distinct watermarks within the content supplied to different customers. This method helps in identifying the customers that break license agreements by supplying the content illegally to unauthorized parties.

iii. Copy control. A watermark can prevent illegal regeneration of copies of the marked data. The watermark can include a do-not-copy flag, and the watermark detector within the digital copying device detects this flag and therefore does not produce a copy of the marked media.

iv. Broadcast monitoring. Commercial advertisements and other broadcast signals could carry tracking information in the form of hidden watermarks to monitor and verify the number of times the data has been broadcast. Hence, the customer can be charged accordingly.

v. Unauthorized modification. Fragile watermarks could be used to detect and highlight unauthorized modification to the protected data. These are weak watermarks and are designed to be destroyed in case of alteration of the marked data in an unauthorized manner.

vi. Annotation and indexing. Watermarks can also be used to annotate and index digital data. These watermarks can be used by individuals as identifiers leading to the source of the marked data or by search engines to return the marked data in relevant Web searches.

vii. Medical applications. Based on the regulations set by the Health Insurance Portability and Accountability Act, patient data are considered secure and are to be viewed by first-tier care providers only. The secure data can be embedded as a watermark within medical images, which can be extracted only by the authorized parties.

viii. Covert communications. Watermarking can also be used as a means of transmitting hidden data. Since the actual evidence of hidden data transfer is missing in watermarking, this mode of covert data transfer can be highly effective. Some researchers believe that covert communication, also known as steganography, is a branch of digital data hiding all by itself.

3 WATERMARKING ATTACKS

A watermarked data may undergo certain types of attacks before being reached to the detector or extractor. The attacks can be either intentional or unintentional distortion of the watermarked data, removal of the watermark or addition of noise or extra information on the watermarked data. Different types of attacks can be found depending on the type of the watermarking algorithm. The most types of attacks as following:

Removal attacks aim at the complete removal of the watermark from the watermarked image without using the key (which was used for watermark embedding). No processing can recover the watermark from the attacked data [1]

In contrast to removal attacks, the geometric attacks do not actually remove the embedded watermark, but intend to distort the watermarked data prior to [2]. The filtering attacks are high pass filtering, low pass filtering, Gaussian filtering, sharpening filtering, median filtering, midpoint and mean filtering, the Wiener filtering, etc. Compression attacks are usually an unintentional attack which is the most common attack in multimedia applications. All the audio, video and images that are being distributed via Internet have to be compressed. The most common types of compression are JPEG, and JPEG2000.

Many watermarking techniques are sensitive to synchronization. The attacker may attempt to mask the watermark signal by disturbing synchronization that is Synchronization attacks [3]. Protocol attack is used to attack the concept of the watermarking application. Therefore it is also called system-level attacks. The protocol attacks are subcategorized into copy attacks, ambiguity attacks and scrambling 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.

4 WATERMARKING EMBEDDING DOMAIN:

4.1 Discrete Cosine Transform (DCT):

Discrete cosine transform (DCT) is a general orthogonal transform for digital image processing and signal processing, with such advantages, as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT is a widely used mechanism for image transformation and has been adopted by JPEG to compress images; discrete cosine transform (DCT) is a Fourier-related transform similar to the discrete Fourier transform (DFT)[4]. Discrete cosine transform (DCT) turn over the image edge to make the image transformed into the form of even function[5]. It’s one of the most common linear transformations in digital signal process technology. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that the most visual important parts of the image (low frequencies) is to be avoided without over-exposing it to removal through compression and noise attacks (high frequencies)[6].

In DCT domain, DC component is more suitable to embed watermark than AC component (AC) due to several reasons. Firstly, DC component has larger perceptual capacity. so, after embedding watermark it doesn’t cause obvious change for visual quality of original image; secondly, signal processing and noise interference have smaller influence for DC component than AC component[7].

$$T\left(u,v\right) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y). \cos\frac{(2x+1)u\pi}{2M} . \cos\frac{(2y+1)v\pi}{2N} \qquad (1)$$

The DCT coefficients for output image $T(u,v)$ are computed according to the input $f(x,y)$ as equation (1). Where f is the input image with size $M \times N$ pixels, M is the row and N is the column of the image, whereas $T(u,v)$ is the DCT matrix.

Where

$$\alpha_u = \alpha_v = \begin{cases} \sqrt{\frac{1}{M}} & u = v = 0 \\ \sqrt{\frac{2}{N}} & u \neq v \neq 0 \end{cases}$$

The image recreated by applying inverse DCT according to equation 2.

$$\alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} T(u,v).\cos\frac{(2x+1)u\pi}{2M}. \cos\frac{(2y+1)v\pi}{2N} \qquad (2)$$

4.2 Discrete Wavelet Transform (DWT):

The wavelet transformation is a mathematical tool that can examine an image in time and frequency domains, simultaneously [8]. Discrete wavelet transform (DWT) is simple and fast transformation approach that translates an image from spatial domain to frequency domain. The DWT provides a number of powerful image processing algorithms including noise reduction, edge detection, and compression [9]. The transformed image is obtained by repeatedly filtering for the image on a row-by-row and column-by-column basis. An example of decomposing an image by a 2-level wavelet transformation is shown in Fig. 1. Then after applying the 2-level analysis filter bank a four sub-band images will be obtained (LL, LH, HL, and HH),

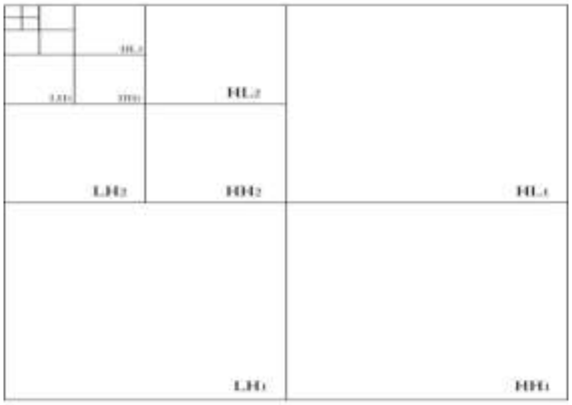

Fig.1 DWT decompose an image by 2-level

4.3 Advantages of DWT over DCT

According to[10] and [11], there is the DWT advantage over DCT as:

1. No need to divide the input coding into non-overlapping 2-D blocks, it has higher compression ratios avoid blocking artifacts.
2. Allows good localization both in time and spatial frequency domain.
3. Transformation of the whole image introduces inherent scaling
4. Better identification of which data is relevant to human perception higher compression ratio

5 GENETIC ALGORITHMS

Genetic Algorithms (GAs) introduced by Holland [12].GA is most widely used amongst the artificial optimization intelligent techniques. A GA is a stochastic searching algorithm based on the mechanisms of natural selection and genetics. GAs has been proven to be very efficient and stable in searching for global optimum solutions.

In general, GAs start with some randomly selected population, called the first generation. Each individual in the population called chromosome and corresponds to a solution in the problem domain. An objective called fitness function is used to evaluate the quality of each chromosome. The next generation will be generated from some chromosomes whose fitness values are high. Reproduction, crossover and mutation are the three basic operators used to repeat many time until a predefined condition is satisfied or the desired number of iteration is reached. According to the applications for optimization, designers need to carefully define the necessary elements for dealing with the GA. Then, the fitness function in addition to the terminating criteria is evaluated with the natural selection, crossover, and mutation operations [13].

5.1 Watermarking based on GA related works

Researchers used GA to optimize the watermarking requirements, Wang et al [14] presented watermarking based Genetic algorithm. They used bit substitution method. Huang et al [15] proposed watermarking method based on GA and DCT domain. They embedded watermark with visually recognizable patterns into image by selection modifying the middle frequency parts of the image. The GA is applied to search for the locations to embed into DCT coefficient block. In addition, Hsiang et al [16] proposed a robust watermarking based on DCT and GA. They tried to design a particle fitness function to solve the tread-off between the three watermarking matrices. On the other hand, they have considered the capacity to be constant. Moreover, Hsiang et al [17] have proposed watermarking based wavelet packet transform (WPT). They have assumed watermarked consists of 0's and 1's all bits of the watermark are embedded into host image. Also, Promcharoen and Rangsanseri [18] presented new approach for watermarking based on DCT. The authors used fuzzy C-mean (FCM) to classify the 8*8 block to texture or non-texture region. They used GA to find out the optimized parameter. As well as, Patra et al [19] proposed the digital watermarking scheme based on singular value decomposition (SVD). The authors used GA to optimize the conflict between quality and robustness. They used Sun et al algorithm for quantization embedding. Furthermore, Li et al [20] proposed watermarking based on DWT domain. They used Arnold transform and GA to improve the performance of watermarking algorithm.

6 RESULT ANALYSES

This section studies the effect of watermarking using GA on the embedding domains. Many of researchers have used Lena picture as the host image. They applied some types of attacks on that image after watermark embedding to prove the quality of their works. We chose some pervious works [21] [22] [23] [24] [25] [26] [18] [27] and analyzed their works and study how the attacks were affected by embedded domains. . The normalized correlation (NC) is used as measure of robustness. It calculates the difference between the embedded and extracted watermark defined as:

$$NC = \frac{\sum_{i=1}^{M} \ \sum_{j=1}^{N} w(i,j) w'(i,j)}{\sqrt{\sum_{i=1}^{M} \ \sum_{j=1}^{N} w(i,j)} \sqrt{\sum_{i=1}^{M} \ \sum_{j=1}^{N} w'(i,j)}}$$

where M and N are the numbers of row and column in the images, respectively. w(i,j) and w'(i,j) are the original and the watermarked image respectively.

Lena picture 516*516 (host image)

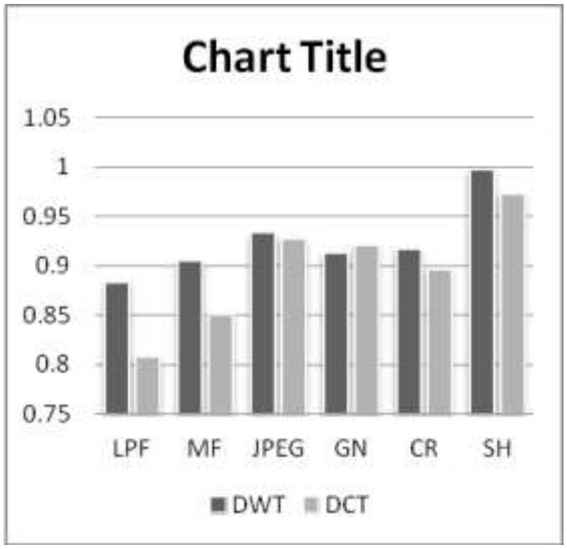

Fig.2 NC result after attack

The figure shows the attacks effect of on DWT and DCT domains. It shows in image processing operation like low-pass filtering (LPF) and medium filtering (MF) that the DWT domain is better than The DCT domain. Other attacks like JPGE, Cropping (CR) and sharpening (SH) almost have the same results with some advantages of DWT. Gaussian noise (GN) give DCT better result more than DWT.

In the brief, DWT domain is better than the DCT domain for embedding in watermarking based on Genetic algorithm.

7 CONCLUSIONS:

In this paper, we proposed watermarking based on genetic algorithm and studied the effect of DWT and DCT embedding domain on robustness of watermarking. As the result of the analysis obtained results by using NC measurement. It is clarify the DWT is better than DCT for robustness of watermarking using genetic algorithm. In future work will study the affect of others optimization techniques and watermarking requirements with some testing experiments.

6 REFERENCES

1. Voloshynovskiy, S., et al., Attack modelling: towards a second generation watermarking benchmark. Signal Processing, **81**(6): p. 1177-1214.(2001).
2. Hartung, F. and M. Kutter, Multimedia watermarking techniques. Proceedings of the IEEE, 1999. **87**(7): p. 1079-1107.(1999).
3. Miller, I.J.C.a.M.L., Facilitating Watermark Insertion by Preprocessing Media. EURASIP Journal on Applied Signal Processing, 2004. (14): p. 12.(2004)
4. Lam, C.-M.P.a.I.-T., Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright Ownership Authentication. INTERNATIONAL JOURNAL OF COMMUNICATIONS, **3**(1): p. 8.(2009)
5. Jiansheng, M., L. Sukang, and T. Xiaomei, A Digital Watermarking Algorithm Based On DCT and DWT. International Symposium on Web Information Systems and Applications (WISA'09), (2009).
6. El-Fegh, I., et al., Color image watermarking based on the DCT-domain of three RGB color channels, in Proceedings of the 10th WSEAS international conference on evolutionary computing2009, World Scientific and Engineering Academy and Society (WSEAS): Prague, Czech Republic. p. 36-39.(2009)
7. Eyadat, M. and S. Vasikarla, Performance evaluation of an incorporated DCT block-based watermarking algorithm with human

visual system model. Pattern Recognition Letters, **26**(10): p. 1405-1411.(2005)

8. Ouhsain, M. and A.B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform. Expert Syst. Appl. **36**(2): p. 2123-2129.(2009)
9. Chang, C.-Y., H.-J. Wang, and S.-W. Pan, A robust DWT-based copyright verification scheme with Fuzzy ART. Journal of Systems and Software, **82**(11): p. 1906-1915.(2009).
10. Hingoliwala H.A., m.S.J.a.N.B., An image comperession by using haar wavelet transform. Advances in Computer Vision and Information Technology,(2008).
11. V.Srinivasa rao, D.P.R.K., G.V.H.Prasad, M.Prema Kumar, S.Ravichand, Discrete Cosine Transform Vs Discrete Wavelet Transform: An Objective Comparison of Image Compression Techniques for JPEG Encoder. International Journal of Advanced Engineering & Applications,, Jan (2010).
12. Holland, J.H., Adaptation in Natural and Artifcial Systems,. The University of Michigan Press, Ann Arbor, MI, (1975).
13. Gen, M. and R. Cheng, Job-Shop Scheduling Problems. Genetic Algorithms and Engineering Design.: John Wiley & Sons, Inc. 190-233.(2007)
14. Wang, R.-Z., C.-F. Lin, and J.-C. Lin, Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition, **34**(3): p. 671-683.(2001)
15. Huang, C.-H. and J.-L. Wu. Watermark optimization technique based on genetic algorithms. SPIE.(2000).
16. Hsiang-Cheh Huang, C.-M.C.a.J.-S.P., The optimized copyright protection system with genetic watermarking. A FUSION OF FOUNDATIONS, METHODOLOGIES AND APPLICATIONS, (2008).
17. Hsiang-Cheh, H., C. Yueh-Hong, and L. Guan-Yu. DCT-Based Robust Watermarking with Swarm Intelligence Concepts. in Information Assurance and Security, IAS '09. Fifth International Conference on. (2009).
18. Promcharoen, S. and Y. Rangsanseri. Genetic watermarking based on texture analysis in DCT domain. in SICE Annual Conference, (2008).
19. Patra, J.C., J.E. Phua, and C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Digital Signal Processing, **20**(6): p. 1597-1611.(2010).
20. Li, H.-f., N. Chang, and X.-m. Chen, A study on image digital watermarking based on wavelet transform. The Journal of China Universities of Posts and Telecommunications, **17**(Supplement 1): p. 122-126.(2010).
21. Kumaran, T. and P. Thangavel. Watermarking in Contourlet Transform Domain Using Genetic Algorithm. in Computer Modeling and Simulation, EMS '08. Second UKSIM European Symposium on. (2008).
22. Ning, Z., et al. An Optimal Wavelet-Based Image Watermarking via Genetic Algorithm. in Natural Computation, ICNC 2007. Third International Conference on. (2007).
23. Yueh-Hong, C. and H. Hsiang-Cheh. Genetic Watermarking Based on Wavelet Packet Transform. in Hybrid Intelligent Systems. HIS '09. Ninth International Conference on. (2009).
24. Chu, S.-C., et al., Genetic Watermarking for Zerotree-Based Applications. Circuits, Systems, and Signal Processing, **27**(2): p. 171-182.(2008).
25. Lu, Y., et al., A Novel Color Image Watermarking Method Based on Genetic Algorithm and Hybrid Neural Networks, in Rough Sets and Current Trends in Computing, S. Greco, et al., Editors. Springer Berlin / Heidelberg. p. 806-814.(2006)
26. Huang, H.-C., C.-M. Chu, and J.-S. Pan, Genetic Watermarking for Copyright Protection. Information Hiding and Applications. **227**: p. 1-19.(2009).
27. Rafigh, M. and M.E. Moghaddam. A Robust Evolutionary Based Digital Image Watermarking Technique in DCT Domain. in Computer Graphics, Imaging and Visualization (CGIV), Seventh International Conference on. (2010).