International Journal of Innovation Sciences and Research
Vol.9, No, 11, pp.1559-1563, November, 2020
Available online at *http://www.ijisr.com*

RESEARCH ARTICLE

SECURING THE E-LEARNING MATERIALS USING DIGITAL WATERMARKING APPROACH

[1,*]Dr. Hamdy S. Heniedy, [2]Dr. Osama M. Ouda and [1]Prof. Mohamed Osama Khozium

[1]Department of Engineering and Applied Science - Computers, MCC, Umm Al-Qura University, Makkah, Saudi Arabia
[2]Department of Computer Science Faculty of Computer and Information Sciences, Mansoura University, Egypt

Accepted 19th October 2020; Published Online 30th November 2020

ABSTRACT

The creation of learning materials needs a substantial amount of human expertise. Since the materials are represented as digital data in eLearning systems, the user can make any number of copies without any loss of quality. Therefore, the copyright holders of these materials have a strong interest in protecting their learning objects from illicit use and distribution. One approach to protect intellectual property of such digital contents is digital watermarking. In this paper, a simple wavelet-based watermarking scheme is presented and a comparison of watermark embedding into high and low frequency bands is made. The difference between watermark embedding at first and second level decompositions is also investigated. And finally a framework for optimizing watermark embedding using genetic algorithms is proposed.

Key words: Embedding Watermark, Watermark Decomposition, Learning Materials, Genetic Algorithms, Digital Watermarking.

INTRODUCTION

ELearning refers to the use of the Internet technologies to deliver a broad array of solutions that enhance knowledge and performance (Rosenberg, 2001). Elearners access the learning from computers via the internet or an intranet, or through a hand-held device like a palm pilot. Some of the more obvious benefits of eLearning include consistency of content, ease of customization, learner control, and reduction or elimination of travel costs to attend learning events. Consistency of content is achieved by the same learning being made available to anyone, anywhere, anytime with no degradation to the quality or effectiveness of the content or presentation. Learner control lets each learner complete just the sections of the learning they need leaving them free to come back at any time for more or to review what they have already covered. Many types of materials used in eLearning are copyrightable such as music, text, graphics, films, photographs and animated sequences. Therefore, eLearning, as a form of digital work, faces many challenges related to intellectual property. This paper shows how to employ digital watermarking to solve some of the intellectual property problems of eLearning. Although watermarking cannot prevent the illicit distribution and usage of copyrighted material it is of utmost use once a copyright violation is to be proved. In this paper, we introduce a digital image watermarking scheme that is based on discrete wavelet transform (DWT) domain. A comparison of embedding the watermark into higher and lower frequency bands at first and second level decompositions is presented. This paper is organized as follows. In section 2, we present an overview of digital watermarking. Section 3 introduces a simple wavelet-based watermarking scheme. Experimental results are shown in section 4. Finally, the conclusions are made in section 5.

Corresponding author: **Dr. Hamdy S. Heniedy,**
Department of Engineering and Applied Science - Computers, MCC, Umm Al-Qura University, Makkah, Saudi Arabia.

Digital watermarking: One of the solutions to provide security in copyright protection is watermarking which embeds special marks in a host document. Digital watermarking has been proposed as a way to identify the source, creator, owner, distributor, or authorized consumer of a document or an image. There are many aspects to be noticed in watermarking design, for example, imperceptibility, robustness and capacity. Imperceptibility refers to the fact that we would like the watermark to be invisible. The watermark should also be robust against a variety of possible attacks such as compression attacks. Capacity means that the watermark should be able to carry a certain amount of information.

Today, almost all of the proposed schemes couldn't meet the above requirements simultaneously. In fact, the imperceptibility and robustness properties are mutually opposing requirements in most proposed schemes. There are two methods of performing watermarking, one in spatial domain, and the other in frequency domain. Each technique has its own advantages and disadvantages. In the spatial domain (Nikolaidis, 1998), we can simply insert watermark into a host image by changing the gray levels of some pixels in the host image, but the inserted information may be easily detected using computer analysis. In the frequency domain, we can insert the watermark into the coefficients of a transformed image, for example, using the discrete Fourier transform (DFT) (O'Ruanaidh, 1996), discrete cosine transform (DCT) (Lin, 2000), and discrete wavelet transform (DWT) (Xia, 1998). Transform domain methods have several advantages over spatial domain methods. First, it has been observed that in order for watermarks to be robust, they must be inserted into the perceptually significant parts of an image. For images, these are the lower frequencies which can be marked directly if a transform domain approach is adopted. Secondly, since compression algorithms operate in the frequency domain, it is possible to optimize methods against compression algorithms as will be seen in section 3.

In this work, we selected to use the discrete wavelet transform (DWT) since it has several inherent advantages to image watermarking. The data structure in the discrete wavelet transform is a scale-space representation. In this representation, the high and low frequency signals are located in pixels and frequency domain. The image features such as edges are located in high frequency sub bands of the transform domain. Since the human eyes are less sensitive to edge and texture information in image, it is difficult for human eyes to see changes to them. However, embedding in high frequency coefficients is fragile to many attacks such as compression attacks. Therefore, many watermarking schemes tend to embed the watermark into low frequency coefficients. In the next section, a simple wavelet-based watermarking scheme is presented. We use the algorithm to show the difference between watermark embedding into high and low frequency bands at first and second level decompositions.

Dwt Watermarking: In this section, we explain the embedding and extraction procedures of a simple wavelet-based watermarking scheme based on the work presented in (Mehul, 2003; Khozium, 2016; Ajlan, 2014; Fatek Saeed, 2018; Rohit singh, 2019; Abdallah soualmi, 2018).

Embedding Procedure

Cover Image: The original image ***I*** is represented as

$$I = x(i, j), 0 \le i \le M, 0 \le j \le N$$

where *x(i, j)* is the intensity pixel and *M, N* represent the size of the image.

Watermark: The mark is a binary visual image ***W*** with as much as 25% of the host image size. The watermark is represented as

$$W = w(i, j), 0 \le i \le M/4, 0 \le j \le N/4, w(i, j) \in \{0,1\}$$

The watermark *W* is permuted using a secret key, key_0, in order to improve the security of the algorithm and to defeat attacks of signal processing, such as image crops. Fig.1 illustrates the relationship between the watermark and the permuted one.

Fig. 1: The watermark and the permuted one

Decomposition: The host image is decomposed into four bands using 1-level DWT decomposition as illustrated in Fig.2. The wavelet domain representation of the host image is denoted by *f(m, n)*.

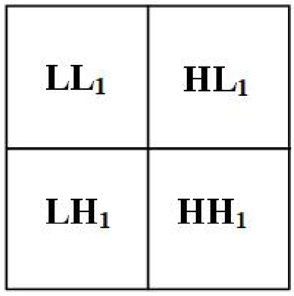

Fig.2. Decomposition of an image using 1-level DWT

LL_1 is the low frequency band that contains most of the image energy. The other bands HL_1, LH_1, and HH_1 are the high frequency bands which contains the detail information of the image.

Embedding: the watermark bits are inserted into the selected coefficients using the following simple additive formula:

$$f'(m, n) = f(m, n) + \sim .w(m, n)$$

where *f'(m, n)* is a watermark embedded DWT coefficient, *f(m, n)* is the original DWT coefficient value, and α is a scaling factor which determines the strength of the watermark. The inverse DWT will generate a watermarked image.

An objective measure of image quality should mirror the perceived image quality. We can compute the distortion introduced to the cover image after embedding the watermark according to a given image quality measure such as PSNR or WPSNR. Measured in HVS terms, PSNR is not a useful measure, weighted PSNR (WPSNR) take into account the local HVS sensitivity; it is a measure criterion which holds account of the neighbors of the studied pixels. Therefore, the WPSNR increases with variance increasing and decrease in the contrary case following this equation (Fourati, 2005):

$$WPSNR = 10Log_{10}\left(\frac{MAX^2}{WMSE}\right)(dB)$$

where weighted MSE (WMSE) is defined as:

$$WMSE = \frac{1}{M^2}\sum_{m=0}^{M-1}\sum_{n}^{N-1}\left(\frac{f_p - \hat{f}_p}{1+Var(m,n)}\right)^2$$

Watermark Detection: The forward 1-level decomposition of the watermarked, and possibly attacked, image and the original image is performed to recover the DWT frequency bands. Then, we apply the inverse embedding formula to extract the watermark bits.

$$w^*(m,n) = \frac{f''(m,n) - f(m,n)}{\sim}$$

The extracted watermark is a visually recognizable pattern. The viewer can compare the results with the reference watermark subjectively. Also a quantitative measurement defined as the Bit Correct Ratio (BCR) is used to compare the embedded and extracted watermark. The Definition of the BCR is (Pan, 2001):

Fig. 3. The original test image Lena (512 ò 512) (a) and The watermark used in experiments (128 ò 128) (b)

Table 1. WPSNR values and BCR values with different ~s under JPEG compression attacks with different quality factors while using LENA as the test image and embedding in low DWT subband LL_1

JPEG Quality factor	BCR (%)		
	~ = 5	~ = 10	~ = 15
WPSNR	48.4628	42.4422	38.9204
10	52.3621	53.8574	55.8533
20	55.2856	60.2539	66.9800
30	60.3333	66.1255	76.3733
40	64.1113	72.9614	83.2092
50	66.5527	77.3071	88.7573
60	72.2717	82.1533	93.4814
70	78.7476	88.9465	96.9666
80	85.0830	95.2637	99.4873
90	96.0510	99.7620	100

Table 2. WPSNR values and BCR values with different ~s under JPEG compression attacks with different quality factors while using LENA as the test image and embedding in high DWT subband HH_1

JPEG Quality factor	BCR (%)		
	~ = 5	~ = 10	~ = 15
WPSNR	54.2984	51.3706	43.1864
10	44.0796	44.5894	44.8025
20	44.0926	45.0837	45.2476
30	44.1040	45.3828	46.1987
40	44.3420	45.7015	46.6260
50	44.9697	45.3523	46.9083
60	45.4397	45.4866	47.1664
70	45.5618	45.6345	47.9758
80	45.6759	45.8562	52.3193
90	52.4536	66.7664	79.4678

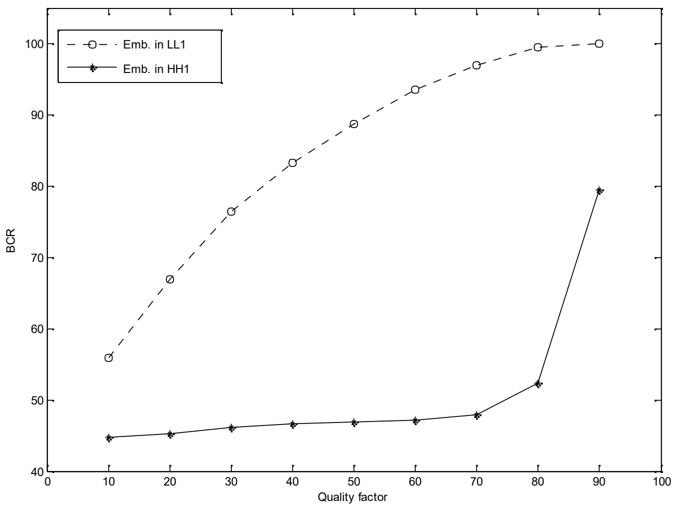

Fig. 4. The robustness of the scheme while embedding into LL_1 band versus robustness while embedding in HH_1 (~ = 15)

$$BCR(W,W^{'}) = (1 - \frac{\sum_{i=1}^{L_w}\left(w_i \oplus w_i^{'}\right)}{L_w}) \times 100\%$$

RESULTS

In our experiments, we employ the "classical" image *Lena*, Fig.3 (a) as our original image I_{org} and a binary-valued image, Fig. 3(b) as our watermark image *W*. These image sizes are 512 × 512 and 128 × 128 pixels, respectively.

First, we performed our experiments using the first level decomposition. We then applied the JPEG compression attack with different quality factors varied from 10 to 90 on the watermarked image. Table 1 shows the WPSNR and BCR values for embedding the watermark in the low frequency band LL_1 with different scaling factors (α). Table 2 shows the WPSNR and BCR values for embedding the watermark in the high frequency band HH_1 with different scaling factors (α). It is clear from the above tables that embedding into low frequency bands results in high robustness compared to

(a) (b)

Fig. 5: The quality of the watermarked images ~ = 15 using while embedding in HH_1 (a) and in LL_1 (b)

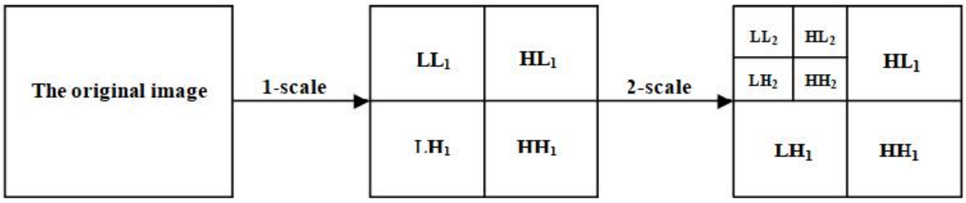

Fig. 6. The image is divided into seven sub-bands through 2-scale wavelet transform

Table 3. WPSNR values and BCR values with different $\sim_s$ under JPEG compression attacks with different quality factors while using LENA as the test image and embedding into the second level DWT subband LL_2

JPEG Quality factor	BCR (%)		
	~ = 5	~ = 10	~ = 15
WPSNR	48.4628	42.4422	38.9204
10	53.2532	59.5093	62.4146
20	56.2561	69.8853	76.3245
30	60.5530	80.4443	87.4146
40	64.1113	86.5234	93.3899
50	66.6870	91.6138	97.0520
60	68.8965	95.3369	98.8586
70	75.0427	98.4375	99.8779
80	85.0830	99.8718	99.9939
90	94.7449	100	100

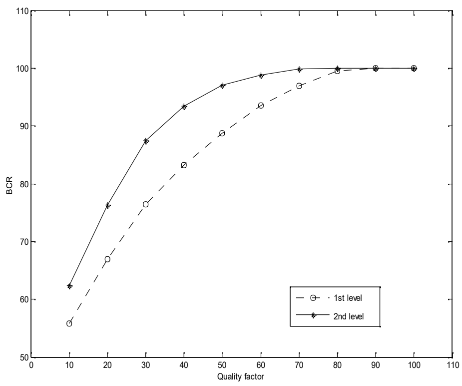

Figure 5. BCR results of the watermark recovered from LL1 and LL2 after JPEG compression attack using ~ = 10 in (a) and ~= 15 in (b)

embedding into high frequency bands. This result may be better illustrated in Fig. 4. On the other hand, embedding in high frequency band ensures high quality watermarked image whereas embedding into low frequency bands introduces noticeable quality degradation. Fig. 5 shows the difference between the watermarked image quality while embedding into the low frequency subband LL_1 and embedding into the high frequency subband HH_1 using $\alpha = 15$. In order to compare between watermark embedding at first and second level decompositions, we repeated the same experiments using the second level decomposition. Fig. 3 shows a 2-scale wavelet transform. In order to investigate the effect of the decomposition level on the performance of the watermarking scheme, we performed the two level decomposition of the cover image and then embed the watermark into the second level LL_2 and repeated the above experiments. Fig. 6 shows a 2-scale wavelet transform and the results are summarized in Table 2. It is obvious from Table 2 and Table 3 that embedding the watermark using the second level decomposition results in more promising values than that results from embedding in the first level of decomposition. Figure 7 shows the BCR values against JPEG compression attack for both levels of decomposition

Conclusion and future work

In this paper, digital watermarking is introduced as one of the solutions to protect intellectual properties of eLearning objects. A simple wavelet-based image watermarking scheme is presented. Simulation results showed that watermark data inserted into high frequencies doesn't affect the visual quality of the watermarked image although it is not robust to attacks such as JPEG compression. On the other hand, embedding the watermark into low frequencies is more robust to JPEG compression attacks but the visual quality of the watermarked image is relatively worse. Experimentation with two levels DWT decomposition helped us understand the optimal level for watermark embedding. The extracted watermarks are more robust while watermark embedding is performed at the second level of decomposition. However, a major drawback of higher level decompositions is that as we increase the level of decomposition, the area to embed the watermark becomes smaller. With the above results, many new research directions arise. We note that the advantages and disadvantages of low and high frequency watermarks are complementary. An interesting topic of further research is the optimization of the watermark embedding process in order to improve the performance of the conflicting requirements: robustness and imperceptibility simultaneously. An optimization technique such as genetic algorithms (GA) may be used to reach this goal. Work is currently under way to apply the ideas in (12, 13) in the wavelet transform domain.

REFERENCES

Abdallah soualmi, Alti adel and Lamri laouamer. 2018. "Toward a Secure and Robust Medical Image Watermarking in Untrusted Environment "The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA)

Ajlan S. Al-Ajlan, "E-Learning Certificate Using Digital Watermarking Technology", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 4, 2014.

Fatek Saeed, Anurag Dixit, "Digital Watermarking Techniques for Content Integrity on E-Learning Systems", International Conference on Computing, Power and Communication Technologies (GUCON),2018.

Fourati W. and Bouhlel, M. S. 2005. "A Novel Approach to Improve the Performance of JPEG2000", ICGST-ACSE journal.

Goldberg, D.E. 1989. "Genetic Algorithms in Search, Optimization and Machine Learning", Addison-Wesley.

Hammerman N. and Goldberg, R. 1998. "Algorithms to improve the Convergence of a Genetic Algorithm with a Finite State Machine Genome" In Practical Handbook of Genetic Algorithms Complex Coding System, L. D. Champers, ed, CRC Press.

Haupt, R. L. and Haupt, S. E. 2004. "Practical Genetic Algorithms", Second Edition, John Wiley & Sons Inc.

Holland, J.H. 1975. "Adaptation in Natural and Artificial Systems", Ann Arbor: University of Michigan Press.

Khozium, M. O. 2016. "Security Using Hiding Technique: EOB Case Study" International Journal in IT and Engineering, Volume 4 Issue 3, March.

Lin S. D. and Chen, C. 2000. "A Robust DCT-based Watermarking for Copyright Protection", IEEE Trans, Consumer Electron, 46 (3).

Mehul R. and Priti, R. 2003. "Discrete Wavelet Transform Based Multiple Watermarking Scheme", Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India.

Mitchell, M. 1999."An Introduction to Genetic Algorithms", MIT Press.

Nikolaidis N. and Pitas, I. 1998. "Robust Image Watermarking in the Spatial Domain", Signal Process, 66 (3).

O'Ruanaidh, J. J. K., Dowling, W. J. and Boland, F. M. 1996. "Phase Watermarking of Digital Images", Proceedings of the 1996 International Conference on Image Processing, Vol. 3, Lausanne, September.

Pan, J.S., Huang, H.C. and Wang, F.H. 2001. "Genetic Watermarking Techniques", Fifth Int'l Conf. on Knowledge-Based Intelligent Information Engineering System & Allied Technologies.

Rohit singh, Simrandeeps singh and Nitin sharma." A Review of Digital Watermarking Technique", IEEE Com-IT-Con, Jan 2019.

Rosenberg, J. M. 2001. "e-Learning". New York, NY: McGraw-Hill,

Sakawa, M. 2002. "Genetic Algorithms and Fuzzy Multi-objective Optimization", Springer.

Shieh, C.S., Huang, H.C., Wang F.H. and Pan, J.S. 2004. "Genetic Watermarking Based on Transform-Domain Techniques", Pattern Recognition, Vol. 37, No.3.

Xia, X.G., Boncelet, C. G. and Arce, G. R. 1998. "Wavelet Transform Based Watermark for Digital Images", Optics Express, Vol. 3, No. 12.

****