Watermarking Techniques for Protecting Intellectual Properties in a Digital Environment

Isinkaye F. O*. and Aroge T. K.
Department of Computer Science and Information Technology
University of Science and Technology, Ifaki-Ekiti, Ekiti-State
***Corresponding Authour:niyikaye2002@yahoo.com**

Abstract

The protection and enforcement of intellectual property rights for digital media has become an important issue in many countries of the world. There is increase in the popularity and accessibility of the Internet to record, edit, replicate and broadcast multimedia content which has necessitated a high demand to protect digital information against illegal uses, manipulations and distributions. Digital watermarking technique which is the process used to embed proprietary information into multimedia digital signal provides a robust solution to this problem. This paper reviews different aspects and techniques of digital watermarking for protecting digital contents. It also explores different application areas of digital watermarking such as copyright protection, broadcast monitoring, integrity protection etc.

Keywords: Watermarking techniques, Digital properties, Content protection, Authenticity determination, Quantization

Introduction

The development and success of the internet has created a new challenge to protect digital content from piracy. Digital watermarking is a new technique that provides an ultimate and robust solution to this problem. It involves direct embedding of additional information into the original content or host signal without perceptible difference between the watermarked and the original content [1]. Such watermark is extremely difficult to remove without altering or damaging the original signal. Watermarking techniques consist of two parts: a part to embed a signal to the original content and a part to detect if a given piece of signal hosts a watermark and subsequently retrieves the conveyed signal. Digital watermarking is very important because it protects the rights of owners of a signal; it also provides copyright identification, user identification, authenticity determination and automated monitoring. This paper reviews different watermarking application and techniques to protect digital contents such as text, video, image and audio.

Digital watermarking is a new research area which is becoming popular. It provides robust solution to the problem of copying and modifying digital content by protecting it from piracy. [2, 3] observed that, the focus of most digital watermarking research is on data objects such as still images, video and audio. Digital watermarking technique is used to ensure the truthfulness and integrity of document content [4], and to embed information which can either be a unique code specifying the author or the originator of the host content [5] (user identification). Due to this, Digital watermarking techniques are often evaluated based on their invisibility, recoverability and robustness. Digital watermarking can be achieved in three ways: fragile, semi-fragile and robust watermarking. Fragile watermarks are the set of watermarking method that can be completely destroyed after any modification to an image [6]. They are not applicable for copyright protection because they are easily removed without seriously degrading the signal. They are heavily used in signal authenticity determination. Semi-fragile on the other hand are used for detecting any unauthorized modification to a digital signal [7]. They have more applicability because they assure that only non-malicious modification will occur in the host signal. Robust watermarking has the best applicability for watermarking than the two previous methods in that they are designed to withstand arbitrarily malicious attacks [8] and are usually used for copyright protection. According to [9], robust watermarking is seen as a communication channel multiplexed into original content in a non-perceptible way and whose capacity degrades as a smooth function of the degradation of the marked content. Watermark embedding scheme can either embed the watermark into the host signal or to a transformed version of the host signal. Transform domain watermarking is a scheme that is used to transform image frequency domain in such a way to modify the transform coefficient. Some common transform domain watermarking for image data can be Discrete Cosine Transform (DCT) based [10, 11] or Discrete Wavelet Transform (DWT) based [12]. This scheme is very useful for taking advantage of perceptual criteria in the embedding process for designing watermark techniques. Spatial domain watermarking on the other hand has the capability of performing some transformation directly on image pixels. The use of perceptual models is also an important component in generating an effective and acceptable watermarking scheme for audio just as it is used in image watermarking [13, 14]. Each watermarking application has its own features that determine the required attributes of the watermarking system and drive the choice of techniques used for embedding and detecting the watermark. These features such as transparency, effectiveness, security, reversibility and complexity as well as possibility of verification allow digital watermarking algorithms to be efficiently evaluated to know if it has enough ingredients that can be used for certain application area.

Watermarking Techniques

Watermark embedding techniques are designed to insert the watermark directly into original signal or into some transformed versions of the original signal in order to take advantage of the perceptual properties or robustness to a particular signal manipulation. Watermarking techniques should have two basic steps: one step that inserts a digital signal using an embedding algorithm and an embedding key. Another step uses a detection algorithm and an appropriate detection key to retrieve the watermark signal. In most techniques, the embedding and detection key are secrete as shown in the figure below.

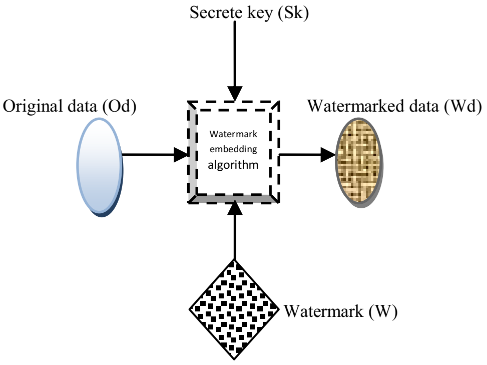

Fig. 1: Watermark embedding process

In Fig. 1, *(Od)* is the original data in which *(W)* will be inserted, *(W)* may require a secret key *(Sk)*. The watermarked data *(Wd)* which is normally generated with the help of a generating function (*fg*) is the output of the embedding process.

$$Wd = fg(Od, Ws, Sk) \qquad \textbf{(Eq. 1)}$$

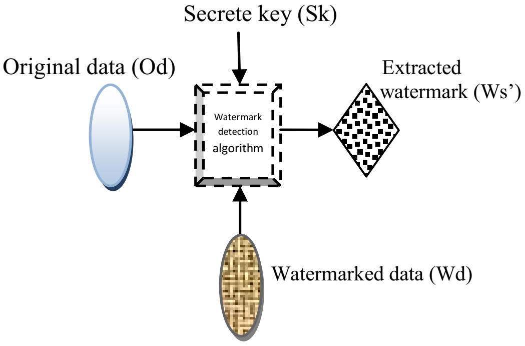

Fig. 2: Watermark detection process

In Fig. 2, the watermarked data *(Wd),* which is distorted, together with the secret key *(Sk)* and the original data *(Od)* are all input to the detection algorithm. The extracting function (*fh*) recovers the embedded watermarked signal (*Ws'*) at the receiving end. The secrete key (*Sk*), used in the embedding process should be available at the receiving end along with the original data (*Od*). If the watermark data was not attacked, it returns the watermark or an indication of its presence (Eq. 2) [15]. In the contrary case, nothing is returned (Eq. 3).

$$Ws' = fh\ (Od, Wd', Sk) \qquad \textbf{(Eq. 2)}$$

$$Ws' = fh(Od,\ Sk) \qquad \textbf{(Eq. 3)}$$

Digital Audio Watermarking

Digital audio watermarking involves embedding special signals within a discrete audio file. The signal can be extracted by detection mechanisms. The use of perceptual models is an important component in generating an effective and acceptable watermarking scheme for audio [16]. The requirements for audio watermarking are imperceptivity, robustness to signal alteration such as conversion, compression and filtering [17]. There are different watermarking techniques for audio which includes echo coding, phase coding, spread spectrum and quantization based watermarking. *Phase encoding* breaks an audio signal into frames and performs spectra analysis on each of the broken frames, once the spectrum has been completed, the magnitude and phase of consecutive frames are compared and an artificial phase signal is created to transmit signal. The artificial phase is modulated in with the phase from each frame and new frames are combined to form the watermarked signal. This technique is very effective in the presence of noise. *Spread spectrum watermarking technique* depends on direct sequence spread spectrum to spread the watermark signal over an entire audible frequency spectrum. It is an example of a correlation method which embeds pseudorandom sequence and detects watermark by calculating correlation between pseudorandom noise sequence and watermark audio signal. SSW is very easy to implement but it requires time-consuming psycho-acoustic shaping to reduce audible noise and susceptible to time-scale modification attack [18]. *Echo watermarking* allows the original audio signal to be copied into two kernels, one which leads the original in time and one which lags. Each kernel represents either a zero or a one bit for watermark data transmission. The bit stream of watermark data is used to mix the two kernels together. The signals are mixed with gradually slope transition to reduce distortion. *Quantization based watermarking technique* quantizes a sample *a* and assigns new value to the sample *a* based on the quantized sample value. The watermarked sample value *b* is described as:

$$\boldsymbol{b} = \{\boldsymbol{qz(a, C)} + {}^{\boldsymbol{C}}\!/_{\boldsymbol{4}}\} \qquad \boldsymbol{if\ a = 1} \qquad \textbf{(Eq. 4)}$$

$$\boldsymbol{b} = \{\boldsymbol{qz(a, C)} - {}^{\boldsymbol{C}}\!/_{\boldsymbol{4}}\} \qquad \boldsymbol{if\ otherwise} \qquad \textbf{(Eq. 5)}$$

In Eq (4&5), *qz*(.) is a quantization function and C is a quantization step. The quantization function *qz(a)* is given as *qz(a,C)=[a/C].C.* The technique is simple to implement and it is robust against noise attack so long as the noise margin is below *C/4.* It also has the ability to achieve provably better rate-distortion-robustness trade-offs than other watermarking techniques such as spread spectrum and low-bits modulation against worse-case square-error distortion-constrained intentional attacks which may be encountered in a number of copyright, authentication and convert communication multimedia application.

Image Watermarking

Images in watermarking are represented as pixels in frequencies transform domain or in spatial domain and they are expected to go through signal processing operations such as compression, filtering, rescaling, cropping, geometric distortion and additive noise which they must survive. In image watermarking, watermark embedding is applied directly to the pixels values in the spatial domain or to transform coefficients in a transform domain [19] such as discrete cosine transform (DCT) or discrete wavelet transform (DWT). The watermarked image (I') is obtained by embedding the watermark *(W)* in the original image ***I, I' = f (I g) w),*** where *f()* is a function denoting the embedding operation and g() is a gain function that depends upon *(w)* and local global image properties. The function can be linear or non-linear. *Discrete Wavelet Transform* allows the simultaneous apparition of both temporal and frequency information. It separates an image into lower resolution approximation image *LL* as well as horizontal *HL*, vertical *LH* and diagonal *HH* detail components. The process can then be repeated to compute scale wavelet decomposition as in the two scale wavelet transform shown in the Fig. 3 below.

<table>
<tr><td>LL_2</td><td>HL_2</td><td rowspan="2">HL_1</td></tr>
<tr><td>LH_1</td><td>HH_2</td></tr>
<tr><td colspan="2">LH_1</td><td>HH_1</td></tr>
</table>

Fig. 3: Two scale 2-dimensional DWT

The benefit of this technique is that it accurately models aspects of the human visual system (*HVS)* as compared to the DCT. This helps to use higher energy watermarks in regions that the *HVS* is known to be less sensitive to, such as high resolution detail bands like *LH*, *HL, H.* when watermark is embedded in these regions, there is increase in the robustness of watermark at little to no additional impact on image quality. *Discrete Cosine Transform* allows an image to be broken into different frequency bands making it easier to embed watermarking information into the middle frequency bands of the image. The basic idea is to represent the image as a sum of sinusoid at different frequencies and magnitudes. An image is divided into 8x8 blocks and the coefficient for each block is calculated. For most images, most of the visually significant information is concentrated in a few coefficients. The DCT is used frequently in JPEG compression. The steps are highlighted below.

Divide the image into non-overlapping blocks of 8x8
apply forward DCT to each of the blocks
apply some block selection criteria
apply coefficient selection criteria
embed watermark by modifying selected coefficient
convert the inverse DCT for 8x8 blocks after modifying the largest coefficient in step 5.

Discrete Fourier Transform watermarking is of two types, one allows the watermark to be directly embedded by modifying the phase information within the DFT. The other is a template based embedding which embeds a template in the DFT domain to estimate the transformation factor. Anytime the watermarked image is transformed, the template is searched to resynchronize the image. A detector is now used to extract the embedded spread spectrum watermark. DFT offers robustness against geometric attacks such as scaling, cropping and rotation.

Digital Video Watermarking

Digital watermarking refers to embedding watermarks in a multimedia documents and files in order to protect them from illegal copying and identifying manipulations [20]. Ideally, a user viewing the video cannot perceive a difference between the original video and the watermarked video, but a watermark extraction application can read the watermark and obtain the embedded information. Video watermarking approaches can be classified into two main categories based on the method of embedding watermark information bits in the host video. The two categories are: spatial domain watermarking and transform-domain watermarking [21]. In spatial domain watermarking techniques, embedding and detection are performed on spatial pixels values such as luminance, chrominance, color space or on the overall video frame. Spatial-domain techniques are easy to implement, however they are not robust against common digital signal processing operations such as video compression. Transform-domain techniques, on the other hand, alter spatial pixel values of the host video according to a pre-determined transform. Commonly used transforms are the Discrete Cosine Transform (DCT), the Fast Fourier Transform (FFT) and the Discrete Wavelet Transform (DWT). Watermarking algorithm optimizes for three separate factors which are: Robustness, which is the ability to resist attempts by attackers to destroy it by modifying the quality, size, rotation and other visual aspect of video. Security, which is the ability of the watermark to resist attempts by a sophisticated attacker to remove it through cryptanalysis without modifying the video itself and Perceptual fidelity**,** which is the perceived visual quality of the watermarked video compared to the original video.

Text watermarking

Text watermarking involves embedding watermark information into the layout and formatting of the text directly. It was designed for watermarking electronic versions of text document which may be in some formatted versions such as postscript or PDF. Text watermarking technique consist of *line shift coding,* here, each of the even lines is slightly shifted up or down according to the bit value in the payload [22]. If the bit is one, the corresponding line is shifted up else it is shifted down. The odd lines are control lines. *Word shift coding,* this technique allows each line to be divided into groups of words which has enough number of characters. Each even group is shifted to the right or left according to the bit value in the payload. At decoding, the odd groups are used as references for measuring and comparing the distances between the groups [23]. Spread spectrum technique makes watermark bit to be mixed with Pseudo Random Noise [PRN] generated signal, the signal is then embedded in the original signal where the PRN acts as the secrete key. A particular PRN signal can later be detected by correlation receiver. All these techniques are based on watermarking the binary-valued text region of a text document. Text watermark detection technique involves post processing steps to try to remove noise.TW techniques are effective against common attacks such as multigenerational photocopying.

Application of Watermarking Techniques

Content Authentication: The advances in computer technology has made it easier to manipulate digital multimedia content as well as making it extremely difficult to determine the originality of such content. Content authentication is the process which confirms the integrity of watermarked data to make sure that the data is not tampered with. The use of watermarking related authentication consists of digital rights management systems, video surveillance and remote sensing applications, digital insurance claim evidence and trusted cameras. In security monitoring, watermark is used to make sure that all video inputs are from authorized sources. In these applications, a watermark which describes the work is sometimes used. It is important that the description of the file is unique and hard to obtain by an attacker.

Privacy Protection: Electronic health programs allow personal health information to be collected and stored in a digital form. Most of these records consist of personal information which should be highly protected. Personal information on medical images are normally stored in a separate file that can be easily accessed at the same time with the images. However, this information are not always protected, hence it can be accessed anytime by intruders. The issues of privacy protection and access control were triggered by a recent incidence that involved accessing patient information for jobs screening in the university Health Network in Toronto [24]. Digital watermarking can be used to embed sensitive information into the cover files. The advantage of watermarking is that the information stays with the original file, which reduces the chance of it being deleted or changed accidentally. Moreover, since watermarking introduces only small distortions, it will not cause difficulties for physicians who do not have the authority to access the personal file.

Ownership assertion and identification: watermarking can be used to prevent unauthorized copying and distribution of a digital content. Intellectuals can make use of watermark to prove ownership of the work they created in case of dispute [25]. The ownership can be ascertained by extracting the embedded information from the watermarked document. In this application, Robustness is critical because the embedded watermark should not be easily removed by little transmission imperfections.

Broadcast Monitoring: It is usually performed by automated monitoring stations and it is one of the watermarking applications that has found its way toward successful commercialization. Applications such as data monitoring and tracking require a higher level of robustness in order to detect or identify stored or transmitted data. Examples are automatic monitoring of radio broadcast for billing purposes or identification of images on the World Wide Web with the help of web crawlers. For such applications, the watermarks have to be easily extractable and must be reasonably robust against standard data processing like format, conversion and compression [26]. Broadcast monitoring allows the embedded information to be utilized for various functions that are related to digital media broadcasting. The embedded data can be used to verify whether proper airtime allocation occurred, for devising an automated royalty collection scheme for copyrighted material that is aired by broadcasting operators or to collect information about the number of people who listened to a certain broadcast.

Transaction tracking: This consists of hidden and imperceptible information about the user which can be detected by a watermark detector hence; tracing illegal copies of a digital property when distributed is made easier. Also, licensed copies which belong to an individual user are ascertained thus resolving the possible conflicts as regards the ownership of a particular intellectual property. Identification of movie theatres where illegal recording of a movie with a handheld camera took place is a scenario that belongs to this category of application.

Conclusion

The paper reviews basic watermarking techniques as applied to different media types. Watermarking is an important technique that has the potential of incorporating an embedding process and preventing easy separation of watermark from content. It also has an enabling technology for a number of applications which imposes different requirements on the watermarking system. Owing to these strengths, digital watermarking is suggested as the ultimate solution to protect digital properties from piracy and copyright infringement.

References

[1] R.B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual Watermarks for digital images,” Proc. IEEE, No 7, 1999, pp. 1108-1126.

[2] V.Potdar, S. Han and E. Chang, “A Survey of Digital Image Watermarking Techniques”, Proc. of the 3rd International IEEE Conference on Industrial Informatics. IEEE Xplore Press, USA, 2005, pp. 709-716.

[3] A. Lemma, J. Aprea and L. Kherkhof, “A Temporal-Domain Audio Watermarking Technique”, IEEE Trans. Signal Process, Vol 51, 2003, pp1088-1097.

[4] J. Ingermar Cox, L. Matthew Miller, and A. Jerey Bloom, Digital watermarking, Morgan Kaufmann Publishers, Inc., San Francisco, 2001

[5] S. Katzenbeisser, A.P. Fabien Peticolas, “Information Hiding Techniques for and Digital Watermarking”, Security Technology for World Wide Web, Artech House Computer Security Series, 2000.

[6] G. Caronni, “Assuming Ownership rights for digital images”, Proc of Reliable IT systems, 1995, pp 251-263.

[7] Q. Sun, S. Chang, “Semi-fragile image Authentication Using Generic Wavelet Domain Features and ecc,” Proc of IEEE International Conference on Image Processing, 2002, pp. 901-904.

[8] N. Nicholaisdis, I. Pitas, “Robust Image Watermarking in the Spatial domain”, Signal Processing, Vol.66 No 3, 1998, pp. 385-403.

[9] T. Kalker, “Considerations on Watermarking Security. Proc. MMSP, Cannes, France, Oct. 2001, pp. 201-206.

[10] F. M. Boland, J. J. K. O’Ruanaidh, and C. Dautzenberg, “Watermarking Digital Images for Copyright Protection,” In IEEE Int. Conf. Image Processing and Applications. 1995, pp. 321-326.

[11] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Trans. Image Processing, Vol.6, 1997, pp. 1673-1687.

[12] J. Huang, Y. Shi, “Embedding Image Watermarking in DC Components”, IEEE Trans. CSVT Vol.10 No 6, 2000, pp. 974-979.

[13] N. F. Johnson, S. C. Katzenbeisser, “A Survey of Steganographic Techniques” In Information Techniques for Steganography and Digital Watermarking, S. C. Katzenbeisser et al., Ed. Northwood, MA: Artech House, Dec. 1999, pp. 43-75.

[14] W. Bender, D. Gruhl, and N.Morimoto, “Techniques for Data Hiding,” IBM Syst. Journal, Vol.35, Nos 3-4, 1996, pp. 313-336

[15] I. B. Ismail, I. R. Farah and M. B. Ahmed, “Satellite Watermarking based on Wavelet Techniques,” IEEE 2nd International Conference on Information and Communication Technologies ICTTA ’06 SYNA, 2006.

[16] L. Boney, A. Tewfik, and K. Hamdy, “Digital Watermark for Audio Signals,” IEEE Proc. Multimedia, 1996, pp. 473-480.

[17] M. Swanson, B. Zhu, A. Tewfik and L. Boney, “Robust Audio Watermarking using Perceptual Masking,” Signal Process; Special Issue on watermarking, 1997, pp. 337-355.

[18] J. Seok, J. Hong, and J. Kim, “A Novel Audio Watermarking Algorithm for Copyright Protection of Digital Audio,” ETRI Journal, Vol. 24, 2002, pp. 181-189.

[19] S. Guan-Ming, “An Overview of Transparent and Robust Digital Image Watermarking”, Available online at www.watermarkingworld.orgLWMMLArchive/0504/pdf00000.pdf

[20] L. Qiao, K. Nahrstedt, "Watermarking Schemes and Protocols For Protecting Rightful Ownership and Customer's Rights", Journal of Visual Communication and Image Representation Vol. 9, 1998, pp.194–210.

[21] R. Shah, A. Argawal, and S. Ganesan, "Frequency Domain Real Time Digital Watermarking", in Proc. of the IEEE 2005 Int. Conf. on Elector Info. Tech, 2005, pp. 1-6.

[22] A. Micic, D. Radenkovic, and S. Nikolic, “ Autentification of Text Document Using Digital Watermarking”, Telecommunication in Modern Satellite, Cable and Broadcasting Services, 2005, 7th International Conference, Vol. 2. 2005, pp. 503-505.

[23] J.T Brassil, S. Low, N.F Maxemchuk, L.O’Gorman, “Electronic Marking and Identification Techniques to Discourage Document Copying”, Selected Area in Communications, IEEE Journal on Vol. 13, No 8, Oct. 1995, pp. 1495-1504.

[24] M. Arnold, M. Schumucker and S. Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”, Artech House, Boston, MA. ISBN:10:1580531113, 2003, pp. 274.

[25] I. Pitas, “A method for Signature Casting in Digital Images”, Proc. IEEE Int. Conf on Image Processing, 1996, pp. 215-473.

[26] F. Hartung, M. Kutter, “Multimedia Watermarking Techniques”,4 Proceeding of the IEEE, Vol. 87 No 7, 1999, pp.1079-1107.

Received: November 2011. Accepted: March 2012.