Literature Survey on Digital Image Watermarking

Er-Hsien Fu
EE381K-Multidimensional Signal Processing
8/19/98

Abstract

This paper conducts a literature survey of digital watermarks used for images. It describes the previous work done on digital watermarks, including the analysis of various watermarking schemes and their results. Potential applications are discussed, and an implementation plan of the project is presented.

1. INTRODUCTION

Over the past few years, there has been tremendous growth in computer networks and more specifically, the World Wide Web. This phenomenon, coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images. Publishers, artists, and photographers, however, may be unwilling to distribute pictures over the Internet due to a lack of security; images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this tough issue. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image.

This paper is a literature survey of digital watermarks. Its objective is to summarize the previous work done on digital watermarks and to detail the implementation plan of the project. The paper is organized as follows: Section 2 gives a general description of a digital watermark. Section 3 summarizes the watermarking methods performed in the literature and presents its results. Section 4 explains the potential applications of watermarking, and section 5 presents the implementation plans for the project. Finally, section 6 gives a conclusion of the literature survey.

2. THE DIGITAL WATERMARK—A BRIEF DESCRIPTION

In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Ideal properties of a digital watermark have been stated in many articles and papers [1-3]. These properties include:

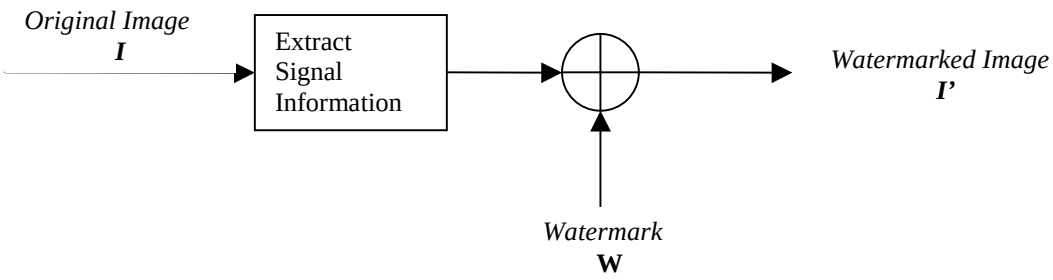
1) A digital watermark should be perceptually invisible to prevent obstruction of the original image.
2) A digital watermark should be statistically invisible so it cannot be detected or erased.

3) Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation.
4) Watermark detection should be accurate. False positives, the detection of a non-marked image, and false negatives, the non-detection of a marked image, should be few.
5) Numerous watermarks can be produced. Otherwise, only a limited number of images may be marked.
6) Watermarks should be robust to filtering, additive noise, compression, and other forms of image manipulation.
7) The watermark should be able to determine the true owner of the image.

Figure 1 shows a general watermarking scheme. For transmission, the watermark W is generated as a pseudo-random sequence to ensure statistical invisibility. Signal information, such as DCT coefficients, are extracted from the original image I and embedded into the information. The watermarked image I' is formed with no visible differences between I and I'.

For watermark detection, a suspected image J is taken and its signal information is obtained. A suspected watermark V is extracted based on knowledge of the original image I and the watermark W. A similarity measure S is performed on V and W. Popular measures include the cross-correlation and correlation coefficient. Finally, S is compared to a threshold τ. If S is larger than the threshold, then the watermark W is detected. Otherwise, no watermark is detected.

Watermark Transmission:



Watermark Detection:

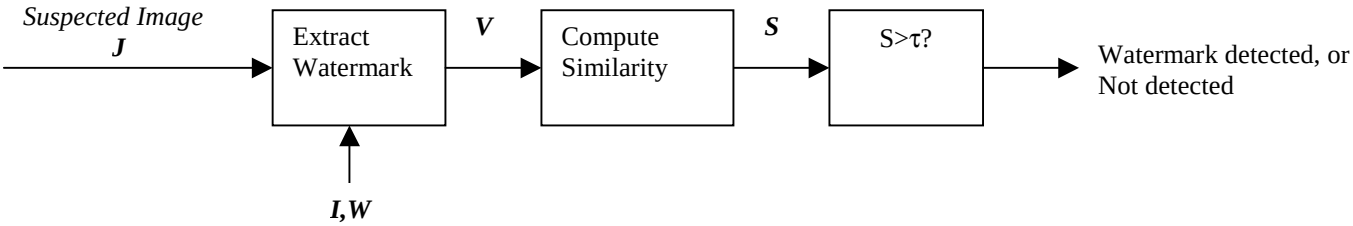


Figure 1.

3. WATERMARKING TECHNIQUES

Many watermarking methods have been proposed in the literature. Schyndel, Tirkel, and Osborne [4] generated a watermark using a m-sequence generator. The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. Schyndel *et al*. showed that the resulting image contained an invisible watermark with simple extraction procedures. The watermark, however, was not robust to additive noise.

Cox *et al*. [1] noted that in order for a watermark to be robust to attack, it must be placed in perceptually significant areas of the image. The watermark was based on 1000 random samples of a N(0,1) distribution. These samples were added to the 1000 largest DCT coefficients of the original image, and the inverse DCT was taken to retrieve the

watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient was computed and set to a threshold. If the correlation was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping, and rescanning.

Xia, Boncelet, and Arce [5] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method [1] when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images.

Improvements on the above schemes were possible by utilizing properties of the Human Visual System. Bartolini *et al.* [6] first generated a watermarked image from DCT coefficients. Then spatial masking was performed on the new image to hide the watermark. Kundur and Hatzinakos [7] embedded the watermark in the wavelet domain. The strength of the watermark was determined by the contrast sensitivity of the original image. Both techniques showed resistance to common signal processing operations.

Delaigle *et al*. [8] proposed a unique watermarking scheme based on the Human Visual System. Binary m-sequences were generated and then modulated on a random

carrier. This image served as the watermark, and then it was masked based upon the contrast between the original signal and the modulated image. The masked watermark was added to the original image to form the watermarked image. Their technique was robust to additive noise, JPEG coding, and rescanning.

Craver *et al* [9] noted that certain watermarking techniques were susceptible to counterfeit attacks. They showed that the method proposed by Cox et al. can be attacked by creating a fake original image and fake watermark that is indistinguishable from the true original image and watermark. To prevent this scenario, they modified the Cox *et al.* algorithm by making the watermark dependent on the original image. This new scheme was less susceptible to counterfeiting and still maintained robustness.

Bas, Chassery, and Davoine [10] introduced a watermarking system using fractal codes. A collage map was composed from 8x8 blocks of the original image and from the image's DCT. The watermark was added to the collage map to produce a marked image. Results showed that fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique was robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.

5. APPLICATIONS

Many potential applications exist for digital watermarking. Artists and photographers could mark their images to secure ownership rights. Publishing companies who commercially distribute their images could watermark them to prevent unauthorized distribution. Digimarc Corporation already has a software package that searches the Internet for web pages containing specific watermarks.

Watermarking could also apply to other multimedia data such as audio and video. Compact disks and digital video disks are extremely susceptible to bootlegging via the internet. Digital watermarks might take part in diminishing this potential underground market.

6. PROJECT IMPLEMENTATION PLANS

Since a watermark is merely a sequence of pseudo-random numbers, error free detection may be possible by using linear block codes. With the exception of [11] most watermarking schemes do not employ error-correction. My project will attempt to implement a new watermarking method using error-correction techniques. Tests will be performed to see if the watermark satisfies the desired properties mentioned in section 2. Image processing and other computations will be handled by MATLAB. Furthermore, this project seeks to determine if the error-correcting watermark scheme will hold any advantages over traditional watermarking methods.

7. CONCLUSION

A large variety of watermarking techniques is currently available in the literature. Recent work has shown that digital watermarks can be fairly successful in achieving the desired properties mentioned in section 2. These watermarks, however, are not perfect, and more could be done to improve a watermark's robustness or accuracy in detection. Furthermore, the question of copyright infringement remains a legal issue. Courts need to determine which methods may or may not be used. Until these legal standards are set, the Internet continues to be unsafe for images.

REFERENCES

1. I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.
2. M. Swanson, B. Zhu, and A. Tewfik, "Transparent Robust Image Watermarking," *Proc. IEEE Int. Conf. on Image Processing*, Sept. 1996, vol. III, pp. 211-214.
3. I. Pitas, "A Method for Signature Casting on Digital Images," *Proc. IEEE Int. Conf. on Image Processing*, Sept. 1996, vol. III, pp. 215-218.
4. R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," *Proc. IEEE Int. Conf. on Image Processing*, Nov. 1994, vol. II, pp. 86-90.
5. X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," *Proc. IEEE Int. Conf. on Image Processing*, Oct. 1997, vol. I, pp. 548-551.
6. F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," *Proc. Int. Conf. on Image Processing*, Oct. 1998, vol. I, pp. 450-454.
7. D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," *Proc. IEEE Int. Conf. on Image Processing*, Oct. 1997, vol. I, pp. 544-547.
8. J. Delaigle, C. De Vleeschouwer, and B. Macq, "Psychovisual Approach to Digital Picture Watermarking," *Journal of Electronic Imaging*, vol. 7, no. 3, pp. 628-640, July 1998.
9. S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573-586, May 1998.
10. P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," *Proc. IEEE Int. Conf. on Image Processing*, vol. I, Oct. 1998, pp. 469-473.
11. L. Marvel, C. Retter, and C. Boncelet, "Hiding Information in Images," *Proc. IEEE Int. Conf. on Image Processing*, vol.II, Oct. 1998, pp. 396-398.