International Journal of Information Technology and Knowledge Management
January June 2009, Volume 2, No. 1, pp. 195-197

REVIEW OF DIGITAL WATERMARKS

Jasvinder Kaur[*], Manoj Duhan[**] & Ashok Kumar[***]

Introduction

The applications accessing multimedia systems and content over the Web have grown immensely in the past five years. Furthermore, many end users can easily use tools to synthesize and edit multimedia information. Thus, security has become one of the most significant problems for distributing new information technology. It is necessary to prevent illegal copying, misappropriation, and misrepresentation of digital audio, images, and video because they can be so easily copied and multiplied without information loss. It's also important to determine where and how much a multimedia file differs from its original. Thus, a need exists for developing technology that will help protect the integrity of digital content and secure the intellectual-property rights of owners.

Watermarking is becoming the key method for protecting digital elements such as image, video, and sound. Digital watermarking embeds a signal into the original element, and the signal uniquely identifies the owner. This requires security solutions for such fields as distributed production processes and e-commerce because the producers seek to provide access control mechanisms to prevent their material's misuse and theft. Many authors, publishers and providers of multimedia data are reluctant to put their work on internet because the ease of reproducing digital data in their exact original form is likely to encourage copyright violation, data misappropriation and abuse. Therefore, creators and distributors of digital data are actively seeking reliable solutions to the problems associated with copyright protection of multimedia data. Watermarking can be one of the best solutions of this problem.

Watermarking Development

The rapid growth of digital imagery, coupled with the intensive network activity on the web, have generated interest in the development of effective protection mechanisms. But the development of watermarking is rather new: despite important efforts, the terminology is not yet completely established [1], even the purpose of watermarking is not identical in many different domains [2]. Therefore several propositions have been made which may look as competing but are indeed addressing different problems. Even more, as many as modern uses of multimedia documents are still in their infancy, many of the possible attacks against property of images and video documents are still to be invented(it is the case for instance with new audio-visual objects).

The challenge of the evolution of watermarking is related to the information-preserving transformations. Watermarks and attacks on watermarks are two sides of the same coin. A watermark's goal is to be secured and robust enough to preserve the digital data's value. However, watermark protection's goal is to be robust enough to resist attack but not at the expense of altering the value of the data being protected. On the other hand, the goal of the attack is to remove the watermark without destroying the protected data's value. From the communication viewpoint, a watermark can be defeated in two ways : erasure/alteration and jamming. In the first case, an attacker estimates a portion of the watermark and removes or alter enough of it so that it cannot be reliably detected. The second case, jamming refers to document alterations that do not remove the watermark but make it more difficult to detect.

Current Watermarking Techniques

Digital watermarking is a technology capable of solving important practical security problems. It's a multidisciplinary field that combines media and signal processing with cryptography, communication theory, coding theory, signal compression, and the theory of human perception. Interest in this field has recently increased because of the wide spectrum of applications it addresses. Although researchers have proposed a wide variety of techniques, it's difficult to classify the approaches and measure their quality.

In[3], a system is purposed to authenticate images by an authentication agent. The most significant bits are signed and the signature with name of owner and privacy enhanced data are placed into least significant bit plane. A similar approach is used in [4], where a checksum is computed for the seven most significant bit planes and then hidden in randomly chosen least significant bits.

In [5], authors add a signal in spatial domain by slightly modifying the intensity level of randomly selected pixels.

[*] Darsh Institute of Engineering & Technology, Gohana.
E-mail: jkharabanda@yahoo.com

[**] DCR University of Science & Technology, Murthal.
E-mail: duhan_manoj@rediffmail.com

[***] Kurukshetra University, Kurukshetra.
E-mail: parvinder23@rediffmail.com

In[6-11] digital equivalent of microdot and human visual system approach is used.

A method in which attacker can attempt to construct an approximation to watermark by taking advantage of inter-pixel correlation is described in [12]. The attack is applicable to watermarking techniques based on the addition of pseudo noise signal. The common design requirements applied in all digital watermarking techniques is explained in [13]. Current Watermarking techniques also make use of Wavelets, Curvelets, DCT coefficients, Fourier transforms and Spread spectrum techniques [14-19].

WATERMARKING CLASSIFICATION

To better manage digital content security, researchers have evolved watermark processing in three categories according to specific applications' requirements: robust, fragile, and semifragile watermarks.

Robuts watermarking resist attempts to remove or destroy the watermark. Primary applications are copyright protection and content tracking. Fragile watermarks can be easily destroyed. Authentication applications use such kinds of watermarks. The semifragile approach combines the properties of robust and fragile watermarks to tolerate some degree of change (quantization noise from lossy compression) to the watermarked digital content. The semifragile watermark can localize regions of digital content that have been tampered, and it distinguishes them from regions that are still authentic. Thus, a semifragile watermark can distinguish between localized tampering and information-preserving, lossy transformations.

Application-Based Classification

We have identified the following, general watermarking classes based on application areas for digital watermarking.

- *Copyright watermarks* mark the data with an owner or producer identification.
- *Fingerprint watermarks* mark the data with customer identification to track and trace legal or illegal copies.
- *Copy control or broadcast watermarks* ensure copyrights with customer rights protocols (for example, for copy or receipt control).
- *Annotation watermarks* embed annotations or descriptions of the data's value of content..
- *Integrity watermarks* ensure the data's integrity and recognize manipulations.

What Next ?

No single standard has prevailed for digital watermarking, and it remains to be seen whether one standard or open standards will in fact triumph. Proponents for a single technology standard argue that this focus would allow standardization across the industry and sufficient effort dedicated to developing a secure, reliable technology. Proponents of open standards feel that competition in research and development is necessary to keep the technology progressing. With competition, firms and researchers will need to keep innovating and improving their technologies to beat competitors. Thus, consumers would benefit from the best, most evolved, and innovative digital watermarking technologies.

References

[1] Frederic Andres: Multimedia and Security, *IEEE Multimedia*, (Oct-Dec 2001), 20-21.

[2] F. Mintzer, G. W. Braudway and M. M. Yeung: Effective and Ineffective Digital Watermarks *IEEE ICIP*, Santa-barbra, Cal, **III,** (Oct 1997), 9–12.

[3] Fragile Imperceptible Digital Watermark with Privacy Control, Don Coppersmith, Frederick C. Mintzer, Charles P. Tresser, Chai W. Wu, *Proceedings of SPIE*, **3657**, (1999), 79-84.

[4] Steve Walton, "Image Authentication for a Slippery New Age", *Dr. Dobb's Journal of Software Tools*, **20**, (4), (April 1995), (1995), 18–26.

[5] N. Nikolaidis and I. Pitas, Copyright Protection of Images using Robust Digital Signatures, *Proc. ICASSP '96* Atlanta, GA, (May 1996).

[6] C. I. Podilchuk and W. Zeng, "Digital Image Watermarking using Visual Models," in *Human Vision and Electronic Imaging II*, **3016**.

[7] B. E. Rogowitz and T. N. Pappas, Eds. San Jose, CA: IS&T and *SPIE*, (1997), 100–111.

[8] A. Herrigel, J. J. K. O'Ruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure Copyright Protection Techniques for Digital Images," in *Information Hiding: Second Int. Workshop (Lecture Notes in Computer Science),* D. Aucsmith, Ed. Berlin, Germany: Springer-Verlag, **1525**, (1998), 169–190.

[9] M. D. Swanson, B. Zu, and A. H. Tewfik, "Robust Data Hiding for Images," in *Proc. IEEE 7th Digital Signal Processing Workshop (DSP 96)*, Loen, Norway, (Sept. 1996), 37–40.

[10] J. F. Delaigle, C. De Vleeschouwer, and B. Macq, "Watermarking Algorithm based on a Human Visual Model," *Signal Processing*, **66**, (3), (May 1998), 319–335.

[11] Min Wu, Bede Liu, Data Hiding in Binary Image for Authentication and Annotation, *IEEE Transactions on Multimedia*, **6**, (4), (August 2004), 528–538.

[12] Matthew Holliman, Nasir Memon, Minerva M. Yeung, Watermarking Estimation through Local Pixel Estimation, *Proceeding of SPIE* **3657**, (1999), 134–146.

[13] Frank Hartung, Martin Kutter, Multimedia Watermarking Techniques, *Proceedings of IEEE*, **87**, (7), (July 1999), 1079–1107.

[14] Chune Zhang, L. L. Cheng, Zhengding Qiu, L. M. Cheng, Multipurpose Watermarking Based on Multiscale Curvelet Transform, *IEEE Transactions on Information Forensics and Security*, **3**, (4), Dec 2008, 611–619.

[15] G. Kai Wang Lavoue, F. Denis, A. Baskurt, Hierarchical Watermarking of Semiregular Meshes Based on Wavelet Transform, *IEEE Transactions on Information Forensics and Security*, **3**, (4), (Dec 2008), 620–634.

[16] M. U. Celik, A. N. Lemma, S. Katzenbeisser, M. van der Veen, Lookup-Table-Based Secure Client-Side Embedding for Spread-Spectrum Watermarks, *IEEE Transactions on Information Forensics and Security*, **3**(3), (Sep 2008), 475–487.

[17] Tsz Kin Tsui, Xiao-Ping Zhang, D. Androutsos, Color Image Watermarking Using Multidimensional Fourier Transforms, *IEEE Transactions on Information Forensics and Security*, **3**, (1), (March 2008), 16–28.

[18] Xiangyang Wang, Jun Wu, Panpan Niu, A New Digital Image Watermarking Algorithm Resilient to Desynchronization Attacks, *IEEE Transactions on Information Forensics and Security*, **2**, (4), (Dec 2007), 655–663.

[19] F. Frattolillo, Watermarking Protocol for Web Context, *IEEE Transactions on Information Forensics and Security*, **3**, (1), (Sep 2007), 350–363.