Challenges of Multimedia Watermarking Techniques

E.Jayabalan R.Pugazendi
A. Krishnan

Abstract

Data transmitted through a network may be protected from unauthorized receivers by applying techniques based on cryptography. Only people who possess the appropriate private key can decrypt the received data using a public algorithm implemented either in hardware or in software. Fast implementation of encryption-decryption algorithms is highly desirable. Data-content manipulation can be performed for various legal or illegal purposes (compression, noise removal or malicious data modification). The modified product is not authentic with respect to the original one. The technology of multimedia services grows rapidly, and distributed access to such ser-vices through computer networks is a matter of urgency. However, network access does not protect the copyright of digital products that can be reproduced and used illegally. An efficient way to solve this problem is to use watermarks. A watermark is a secret code described by a digital signal carrying information about the copyright property of the product. The watermark is embedded in the digital data such that it is perceptually not visible. The copyright holder is the only person who can show the existence of his own watermark and to prove the origin of the product Reproduction of digital products is easy and inexpensive. In a network environment, like the Web, retransmission of copies all throughout the world is easy. The problem of protecting the intellectual property of digital products has been treated in the last few years with the introduction of the notion of watermarks.

Keywords : Multimedia Encryption, Watermarking, IPR, Copyrights

0. Watermarking Algorithm

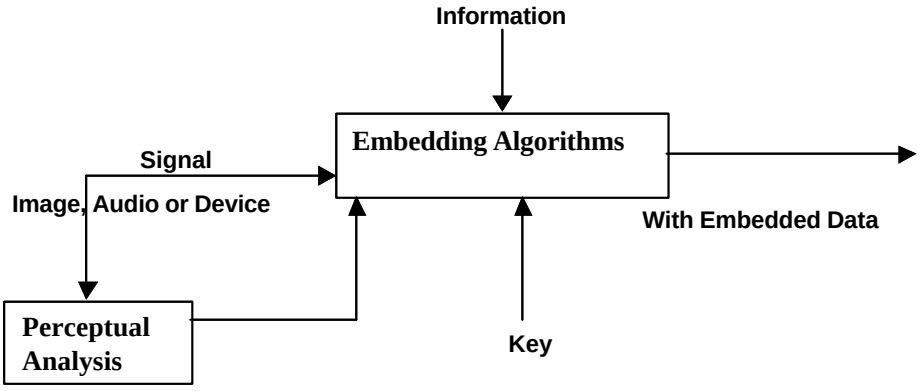
The following requirements should be satisfied by a watermarking algorithm

- Alterations introduced in the image should be perceptually invisible.
- A watermark must be undetectable and not removable by an attacker.
- A sufficient number of watermarks in the same image, detectable by their own key, can be produced.
- The detection of the watermark should not require information from the original image.
- A watermark should be robust, as much as possible, against attacks and image process-ing, which preserves desired quality for the image.

Watermarks slightly modify the digital data to embed non perceptible encoded copyright information. Digital data embedding has many applications. Foremost is passive and active copyright protection. Digital watermarking has been proposed as a means to identify the owner or distributor of digital data. Data embedding also provides a mechanism for embedding important control, descriptive or reference information in a given signal. A most interesting application of data embedding is providing different access levels to the data. Most data-embedding algorithms can extract the hidden data from the host signal with no reference to the original signal.

The first problem that all data-embedding and watermarking schemes need to address is that of inserting data in the digital signal without deteriorating its perceptual quality. We must be able to retrieve the data from the edited host signal. Because the data insertion and data recovery procedures are intimately related, the insertion scheme must take into account the requirement of the data-embedding applications. Data insertion is possible because the digital medium is ultimately consumed by a human. The human hearing and visual systems are imperfect detectors. Audio and visual signals must have a minimum intensity or contrast level before they can be detected by a human. These minimum levels depend on the spatial, temporal and frequency characteristics of the human auditory and visual systems. Most signal-coding techniques exploit the characteristics of the human auditory and visual systems directly or indirectly. Likewise, all data-embedding techniques exploit the characteristics of the human auditory and visual systems implicitly or explicitly. A diagram of a data-embedding algorithm is shown in figure. The information is embedded into the signal using the embedding algorithm and a key. The dashed lines indicate that the algorithm may directly exploit perceptual analysis to embed information. In fact, embedding data would not be possible without the limitations of the human visual and auditory systems.

Data embedding and watermarking algorithms embed text, binary streams, audio, image or video in a host audio, image or video signal. The embedded data are perceptually inaudible or invisible to maintain the quality of the source data. The embedded data can add features to the host multimedia signal, for example, multilingual soundtracks in a movie, or they can provide copyright protection



(Block diagram of a data-embedding algorithm)

1. Watermarking Techniques

Different watermarking techniques have been proposed by various authors in the last few years. The proposed algorithms can be classified into two main classes on the basis of the use of the original image during the detection phase: the algorithms that do not require the original image (blind scheme) [3.147, 3.148, 3.149] and the algorithms where the original image is the input in the detection algorithms along with the watermarked image (nonblind scheme). Detectors of the second type have the advantage of detecting the watermarks in images that have been extensively modified in various ways.

Watermarking embedding can be done either in the spatial domain or in an appropriate transform domain, like a DCT domain, a wavelet transform domain or a Fourier transform domain. In certain algorithms, the imposed changes take into account the local image characteristics and the properties of the human visual system (perceptual masking) in order to obtain watermarks that are guaranteed to be invisible.

The DCT-based watermarking method has been developed for image watermarking that could survive several kinds of image processings and lossy compression. In order to extend the watermarking techniques into video sequences, the concept of temporal prediction exploited in MPEG is considered. For intraframe, the same techniques of image watermarking are applied, but for non-intraframe, the residual mask, which is used in image watermarking to obtain the spatially neighboring relationship, is extended into the temporal domain according to the type of predictive coding. In considering the JPEG-like coding technique, a DCT-based watermarking method is developed to provide an invisible watermark and also to survive the lossy compression.

The human eyes are more sensitive to noise in a lower frequency range than its higher frequency counterpart, but the energy of most natural images is concentrated in the lower frequency range. The quantization applied in lossy compression reflects the human visual system, which is less sensitive to quantization noise at higher frequencies. Therefore, to embed the watermark invisibly and to survive the lossy data compression, a reasonable trade-off is to embed the water-mark into the middle-frequency range of the image. To prevent an expert from extracting the hidden information directly from the transform domain, the watermarks are embedded by modifying the relationship of the neighboring blocks of midfrequency coefficients of the original image instead of embedding by an additive operation.

For example, The original image is divided into 8x8 blocks of pixels, and the 2D DCT is applied independently to each block. Then, the coefficients of the midfrequency range from the DCT coefficients are selected. A 2D subblock mask is used in order to compute the residual pat-tern from the chosen midfrequency coefficients.

Let the digital watermark be a binary image. A fast 2D pseudorandom number-traversing method is used to permute the watermark so as to disperse its spatial relationship. In addition to the pixel-based permutation, a block-based permutation according to the variances of both the image and watermark is also used. Although the watermark is embedded into the mid-frequency coefficients, for those blocks with little variances, the modification of DCT coefficients intro-duces quite visible artifacts. In this image-dependent permutation, both variances of the image blocks and watermark blocks are sorted and mapped according to importance of the invisibility. After the residual pattern is obtained for each marked pixel of the permuted watermark, the DCT coefficients are modified according to the residual mask, so that the corresponding polarity of residual value is reversed. Finally, inverse DCT of the associated results is applied to obtain the watermarked image.

For example, The extraction of a watermark requires the original image, watermarked image and also the digital watermark. At first, both the original image and the watermarked images are DCT transformed. Then, we make use of the chosen midfrequency coefficients and the residual mask to obtain the residual values. Perform the EXCLUSIVE-OR operation on these two residual patterns to obtain a permuted binary signal. Reverse both the block and the pixel-based permutations to get the extracted watermark.

A video sequence is divided into a series of Group of Pictures (GOP). Each GOP contains an interframe (I-frame), forward-predicted frame (P-frame) and bidirectional predicted/interpolated frame (B-frame). P-frame is encoded relative to intraframe or another P-frame. B-frame is derived from two other frames, one before and one after. These non-intraframes are derived from other reference frames by motion-compensation that uses the estimated motion vectors to construct the images. In order to insert the watermark into such kind of motion-compensated images, the residual patterns of neighboring blocks are extended into the temporal domain and other parts of the image. Watermarking techniques can be applied directly into non intraframes.

For a forward-predicted P-frame, the residual mask is designed between the P-frame and its reference I- or P-frame, that is, the watermarks are embedded by modifying the temporal relationship between the current P-frame and its reference frame. For a bidirectionally predicted or interpolated B-frame, the residual mask is designed between the current B-frame and its past and future reference frames. The polarity of the residual pattern is reversed to embed the water-mark

2. Main Features of Watermarking

Watermarks are digital signals that are superimposed on a digital image causing alternations to the original data. A particular watermark belongs exclusively to one owner who is the only per-son that can proceed to a trustworthily detection of the personal watermark and, thus, prove the ownership of the watermark from the digital data. Watermarks should possess the following features

- ✍ Perceptual invisibility : The modification caused by the watermark embedding should not degrade the perceived image quality. However, even hardly visible differences may become apparent when the original image is directly compared to the watermarked one.
- ✍ Trustworthily detection : Watermarks should constitute a sufficient and trustworthily part of ownership of a particular product. Detection of a false alarm should be extremely rare. Watermark signals should be characterized by great complexity. This is necessary in order to be able to produce an extensive set of sufficiently well distinguishable watermarks. An enormous set of watermarks prevents the recovery of a particular watermark by trial-and-error procedure.
- ✍ Associated key : Watermarks should be associated with an identification number called watermark key. The key is used to cast, detect and remove a watermark. Subsequently, the key should be private and should exclusively characterize the legal owner. Any dig-ital signal, extracted from a digital image, is assumed to be a valid watermark if and only if it is associated to a key using a well established algorithm.
- ✍ Automated detection/search : Watermarks should combine easily with a search procedure that scans any publicly accessible domain in a network environment for illegal deposition of an owner's product .
- ✍ Statistical invisibility : Watermarks should not be recovered using statistical methods.For example, the possession of a great number of digital products, watermarked withthe same key, should not disclose the watermark by applying statistical methods.Therefore, watermarks should be image dependent.
- ✍ Multiple watermarkings : We should be able to embed a sufficient number of different watermarks in the same images. This feature seems necessary because we cannot pre-vent someone from watermarking an already watermarked image. It is also convenient when the copyright property is transferred from one owner to another.
- ✍ Robustness : A watermark that is of some practical use should be robust to image modifications up to a certain degree. The most common image manipulations are com-pression, filtering, color quantization/color-brightness modifications, geometric distor-tions and format change. A digital image can undergo a great deal of different modifications that may deliberately affect the embedded watermark. Obviously, a watermark that is to be used as a means of copyright protection should be detectable up to the point that the host image quality remains within acceptable limits.

3. Conclusion

Adapting signal compression to networked applications may require some changes in the fundamental approach to this problem. The compression and transmission aspects have generally been treated as separate issues. The first problem with this approach is that the resulting compression algorithms usually do not address the needs of networked transmission. A successful compression algorithm removes all the redundancy, and, hence, the compressed data must be delivered error free. Another consideration in designing compression techniques for network use is to identify the impact of losing different portions of a compressed stream. It is preferable to have the important parts of the compressed stream concentrate into a short and identifiable segment.

Signal-processing techniques can be valuable for hiding a watermark (or identifying information) in the media. Watermarks can play a number of roles. First, a watermark can mark or identify the original owner of the content, such as the image creator. Second, it can identify the recipient of an authorized single-user copy. Third, a watermark can be used to identify when an image has been appreciably modified. An appropriate solution for the watermarking problem requires understanding of both the signal coding and networking or security issues.

Multimedia processors that realize multimedia processing through the use of software include those for bit manipulation, arithmetic operations, memory access, stream data I/O and real-time switching. The programmable processors for multimedia processing are classified into media-enhanced microprocessors (CISC or RISC), embedded microprocessors, DSPs and media processors.

Many critical research topics remain yet to be solved. From the commercial system per-spective, there are many promising application-driven research problems. These include analysis of multimodal scene-change detection, facial expressions and gestures, fusion of gesture/emotion and speech/audio signals; automatic captioning for the hearing impaired or second language television audiences; multimedia telephone and interactive multimedia services for audio, speech, image and video contents.

From a long-term research perspective, there is a need to establish a fundamental and coherent theoretical ground for intelligent multimedia technologies. A powerful preprocessing technique capable of yielding salient object-based video representation would provide a healthy footing for online, object-oriented visual indexing. This suggests that a synergistic balance and interaction between representation and indexing must be carefully investigated. Another fundamental research subject needing our immediate attention is modeling and evaluation of perceptual quality in multimodal human communication. For a content-based visual query, incorporating user feedback in the interactive search process will be also a challenging but rewarding topic.

4. Reference

1 R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, “Perceptual Watermarks for Digital Images and Video”, submitted to the Proceedings of the IEEE, 1998.

2. F. M. Boland, J. J. K. ´ O Ruanaidh, and W. J. Dowling, “Watermarking digital images for copyright protection,” in Proc. Int. Conf. Image Processing and Its Applications, vol. 410, Edinburgh, U.K., July 1995.

3. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, “A DCT-domain system for robust image watermarking,” Signal Processing (Special Issue on Watermarking), vol. 66, no. 3, pp. 357–372, May 1998.

4. P. Bas and J.-M. Chassery, “Using fractal code to watermark images,” in Proc. Int. Conf. Image Processing (ICIP), vol. 1, Chicago, IL, 1998.

5. P. Bassia and I. Pitas, “Robust audio watermarking in the time domain,” in Proc. European Signal Processing Conf. (EUSIPCO 98), Rhodes, Greece, Sept. 1998.

6. W. Bender, D. Gruhl, and N. Morimoto, “Techniques for data hiding,” in Proc. SPIE, vol. 2420, San Jose, CA, Feb. 1995, p. 40.

About Authors

Mr. E. Jayabalan is a Research scholar in K.S.R. College of Technology, Tiruchengode, Tamil Nadu
Email : ej_ksrcas@rediffmail.com

Mr. R. Pugazendi is a Research scholar in K.S.R. College of Technology, Tiruchengode, Tamil Nadu
Email : pugazendi_r@rediffmail.com

Dr. A. Krishnan is Principal in R.R. Engineering College, Tiruchengode, Tamil Nadu
Email : a_krishnan26@hotmail.com