Improved Digital Watermarking Techniques and Data Embedding In Multimedia

Ajay Goel
Department of CSE
Singhania University, Rajasthan, India

Rupesh Gupta
Department of Mechanical Engineering, Singhania University, Rajasthan, India

O.P.Sahu
Department of ECE,
N.I.T. Kurukshetra, India

Sheifali Gupta
Department of ECE
Singhania University, Rajasthan, India

***Abstract*— Digital watermarking is a technology being developed to ensure security and protection of multimedia data. The purpose of digital watermarking is not to restrict use of multimedia resources, but rather to facilitate data authentication and copyright protection. In this paper, we discuss the general requirements on data hiding and digital watermarking. It includes topics in spatial watermarking; spread spectrum watermarking, spectral watermarking, and a brief survey of currently available commercial and public domain software are provided. The Improved technique is robust to image/video compression, and one can recover the hidden data without requiring the availability of the host signal. The new scheme enables signature images to be as much as 25% of the host image data, and hence could be used both in digital watermarking as well as in image data embedding.**

Keywords: Watermarking Techniques, robustness, DCT, Spread Spectrum Approach, Fractal Operations, Transform-Based Approaches, Lapped Orthogonal Transform

I. INTRODUCTION

The use of digitally formatted audio, video, and printed information is increasing rapidly with the expansion of multimedia broadcasting, networked databases, electronic publishing, etc. This progressive switch to digital representation of multimedia information (text, video, and audio) provides many advantages, such as easy and inexpensive duplication and distribution of the product. However, it also increases the potential for misuse and theft of such information, and significantly increases the problems associated with enforcing copyrights on multimedia information [5], [1], [2], [8] the protection and enforcement of intellectual property rights has become an important issue in the digital world. Well-established organizations are actively pursuing research into digital watermarking and are calling for proposals to incorporate these methods in current multimedia standards. There are various watermarking schemes applied to images and several methods applied to audio and video streams, among them; a large class of the watermarking schemes addresses invisible watermarks. We are currently in an evaluation phase of the technology in which researcher are developing general guidelines for effective watermarking algorithm design, improving reliability within the constraints of computational complexity and tailoring to the constantly changing needs of multimedia industries [5].

During the past few years, a number of digital watermarking methods have been proposed. The two basic modalities for image watermark encoding are: spatial domain techniques (spatial watermarks) and spatial frequency-domain techniques (spectral watermarks). The following paper describes several spatial watermarking algorithms that rely on some type of perceptual knowledge in the encoder. Many of the spatial watermarking techniques provide simple and effective schemes for embedding an invisible watermark into the original image but are not robust to common image alterations. Another way to mark an image is to transform it into the frequency domain- Fourier, DCT, wavelet, etc. - before marking it. The mark is incorporated directly into the transform coefficients of an image. The inverse-transform coefficients form the marked image. These types of algorithms are often called spectral watermarks, and commonly use frequency sensitivity of the human visual system to ensure that the watermark is invisible. Many of these techniques are private watermarks, which require the original image to verify the mark. Algorithms that do not require the original image for testing are called public watermarks [2].

II. APPLICATION AREAS

The basic components of any watermarking technique consist of a marking algorithm that inserts information, the watermark, into an image. The watermark is inserted into the image in the spatial domain or spatial frequency domain. As part of the watermarking technique, a testing algorithm must be defined that tests an image to see if a particular watermark is contained in the image. Depending on the desired properties of the data hiding scheme, we can classify data hiding applications into the following three categories:

(i) Watermarking for protecting intellectual property protection
(ii) Watermarking for tamper detection
(iii) Data hiding for multimedia delivery

It is also true that these applications vary greatly depending on the application, for instance, in the use of watermarking for protection of intellectual property, the watermark is used to supply digital objects on the Internet with an identification of origin. On the other hand, Fingerprinting attempts to identify individual copies of an object by means of embedding a unique marker in every copy that is distributed.

III. GENERAL REQUIREMENTS

Each watermarking application has its own specific requirements. Therefore there is no universal set of requirements as such that must be met by all watermarking techniques. There are some requirements mentioned below for watermarking techniques:-

1. Imperceptibility
2. Robustness
3. Resistance
4. Security
5. Computational Complexity
6. Modification and Multiple Watermarks
7. Scalability

IV. SPATIAL WATERMARKING APPROACHES

Among the earliest works in image watermarking proposed a digital watermarking method which substitutes the least significant bits of randomly selected pixels with bits from M-sequence generator, to represent the watermark. The original 8 bit gray scale image data is compressed to 7 bits by adaptive histogram manipulation, and then the LSB from the watermark sequence is combined to form the encoded image. The watermark can if be decoded by comparing the LSB bit pattern with a stored counterpart. This method is limited to those images containing relatively large areas of texture; the technique is also vulnerable to low-pass filtering. A similar system was proposed by Pitas, 1996 [7]. Much the same techniques can be used to mark digital audio as well. One way to attack such systems is to break up the synchronization needed to locate the samples in which the mark is hidden, for example, one can crop the image.

A. BASIC SPREAD SPECTRUM APPROACH

Most of the work on robust watermarking is based on spread spectrum (SS) principles In SS watermarking; the embedded signal is generally a low energy pseudo-randomly generated white noise sequence. It is detected by correlating the known watermark sequence with either the extracted watermark or the watermarked signal itself (if the host is not available for extraction). If the correlation is above a given threshold then the watermark is detected. The anti-jamming properties of SS signaling makes it attractive for application in watermarking since a low energy, and hence imperceptible, watermark, robust to narrow band interference, can be embedded. In most SS techniques the pseudo-random white noise watermark sequence is added to the host signal and is detected by correlating the known watermark with the watermarked signal. That is, the watermark is embedded in some domain of the signal using linear addition.

The shortcoming of such method is in the channel capacity estimate, where they used the capacity formula for a Gaussian channel, which is not the best model of the noise in a single image.

B. OTHER SPATIAL DOMAIN WATERMARKS

The watermark proposed in. [3],5] is known as the Constant and Variable two-dimensional Watermark respectively. The authors reshape an m-sequence into two-dimensional watermark blocks, which are added and detected on a block-by-block basis. Both schemes do not require the original for watermark detection. However, it can detect local alterations in a received image on a block-wise basis.

C. FRACTAL OPERATIONS

Darven and Scott [Dan in and Scott, 1996] presented an approach to image Steganography utilizing fractal image compression operations. An information bit is embedded into the Stego-image by transforming one similar block into an approximation for an. The data are decoded using a visual key that specifies the position of the range and domain regions containing the message. Unfortunately, the amount of data that can be hidden using this method is small and susceptible to bit errors. Moreover, the search for similar blocks in the encoder, and the decoder comparison process, are both computationally expensive operations.

D. PATTERN OVERLAYING

By interpreting watermarking as a key-dependent pattern overlaying, a new watermarking scheme was proposed by Fridrich [2]. The method is based on overlaying a pattern with its power concentrated mostly in low frequencies in order to guarantee robustness. The method is described as follow: The watermark is generated by choosing a string of bits (author's ID + image hash) which can be transformed into a smooth, almost transparent pattern to be overlaid over the carrier image. The pattern should not exhibit traces of any regular building blocks. Also, patterns generated by two different watermarks should be uncorrelated. To achieve these goals, the author proposed to seed a random number generator with the watermark to create an initial black and white two-dimensional random pattern. The pattern will then further processed to eliminate high frequencies, which is done by applying low pass filters to the initial pattern. The initial pattern was initialized with 0's and 1 's with the same probability 50%. To extract the watermark, the watermarked image is subtracted from the original and the correlation between the difference and the smoothed pattern is calculated. The advantage of this

method is that it avoids transformations, which results in a faster and easy implementation.

E. SPECTRAL WATERMARKING: A SPREAD SPECTRUM WATERMARK EMBEDDED IN THE DCT DOMAIN

Perhaps et. al. [5] is the first work utilizing DCT decomposition for data embedding. They argue that a watermark must be placed in perceptually significant components of a signal if it is to be robust to common signal distortions and attacks. To avoid the perceptual degradation because of watermarking those components, they propose to insert a watermark into the spectral components of the data using techniques analogous to spread spectrum communications, hiding a narrow-band signal in a wide-band. The watermark consists of 1000 randomly generated numbers. The length of the watermark is variable and can be adjusted to suit the characteristics of the data. The technique is very effective both in terms of transparency, robustness to signal processing, and attempt to remove the watermark. The types of image distortions to which the technique is robust include cropping, very low data rate JPEG compression, Printing and scanning, as well as collusion with several independently watermarked images. The limitation of this scheme is its | dependence on the original image for detection of the watermark, which makes it susceptible to multiple claims of ownership [3], [7], and [11].

F. A LINEAR COMBINATION OF MARKED AND UNMARKED IMAGES

The method by Piva, Barni, Bartolini, and Cappellini [1], [8], [10], and [2] is similar to Cox's method [5]. The DCT of the entire image I is computed, and the coefficients are ordered in the zigzag fashion of JPEG to form the coefficient vector ID. To decrease the chance of the watermark being perceptible, the first L coefficients are not marked. W is of length M pseudo-random sequence of numbers, which is added to DCT coefficients. Testing is similar to Cox's method, but the detection does not require the original image.

G. SUB-BAND WATERMARKING

The image watermarking technique in [1] first computes the DCT of an original image X on an 8 x 8 block-wise basis. Making thresholds, m, are defined and computed for each block based on the DCT coefficients; these thresholds are similar in theory to the JND values used in IA-DCT. The watermark for an individual block is a reshaped m-sequence and different watermarks are used for each block. To ensure that the addition of the watermark is imperceptible, spatial domain correction is employed on the marked blocks. The watermark verification is similar to the IA-W method and Cox's testing. A paper test is performed on the normalized cross-correlation coefficient computed between the extracted watermark, and original watermark. If the result is above a certain threshold, the image is authentic. As in previous techniques, the threshold is determined according to the desired probability of detection and probability of false alarm.

V. TRANSFORM-BASED APPROACHES

Another global method also modulates DCT coefficients, but uses a one dimensional bipolar binary sequence for the watermark [6] and [8]. The DCT of the original image is first obtained. The marking procedure consists of sorting the DCT coefficients according to their absolute magnitude. The owner then defines a percentage of total energy, P, and identifies the largest n coefficients that make up P percent of the total energy. The watermark sequence is then added to all the AC coefficients. A larger P increases the number of elements of W that can be embedded in I, but increases the chance that W will be perceptible and the list of selected coefficients must be kept secrete. The verification procedure first extracts the watermark from the marked coefficients in the received image and a procedure similar to Cox [5] can then be used to verify the watermark, but both this method and Cox's method require the original host image to extract the watermark. An early DCT-based technique was presented in [6] and used in the product SysCop, is similar to direct sequence and frequency hopping spread spectrum communications.

A. WATERMARKING USING THE LAPPED ORTHOGONAL TRANSFORM (LOT)

Periera[8] proposed a new approach based on Lapped Orthogonal Transforms (LOT) in which the watermark is inserted adaptively into the LOT domain. The motivation for using the LOT as the basis for embedding a watermark is that the DCT may produce blocking artifacts if the strength of the watermark is increased sufficiently. The drawback of the LOT is that it is not robust in itself to cropping, rotation or scaling. Consequently, the authors suggested adding to the LOT domain watermark a template in the discrete Fourier transform (DFT) domain. The template is used to increase robustness of the watermark. The original image is not needed for detecting the watermark [11].

B. MARKING TEXT DOCUMENTS

The applications and problems associated with text marking are unique. A text document consists of objects of different sizes, such as paragraphs, lines, words, characters, figures, and captions. The basic idea is to encode information by moving these objects by small amounts. For instance, a text line can be moved up to encode a "1" or down to encode a "0". The movements may be as small as a pixel, or 1/3 00th inch at 300 dot-per-inch (dpi) resolution. The motivation for encoding data in this manner is that moving an entire object is less perceptible than distorting the object. Encoding techniques that distort the object include dithering and modifying the transform components [9]. [10] described several invisible techniques for encoding information in text documents, the encoding they used for text marking was moving a paragraph vertically (or horizontally), move a text line vertically, move a block of

words or a single word horizontally, or move a character horizontally. The movement can be
nested or combined to encode more information.

C. COMMERCIAL SOFTWARE

Recently, there have been many commercial software packages for copyright authentication, (e.g. [PictureMarc] and [SureSign]), some of which could be used for multimedia data hiding. Duric[7] provide a comparative evaluation of several different commercial software. Most of these methods employ variations of least-significant bit encoding for data embedding. The shareware program is StegoDos. This program uses the least significant bit method to hide messages. Technical details of these commercially available software utilities are generally not available to the public. Furthermore, the embedding algorithms are generally not very robust. Even if the software is capable of hiding a large quantity of data, the embedded data can be easily removed with simple signal processing methods.

VI. IMPROVED WATERMARKING BASED ON IMAGE- ADAPTABILITY

A watermarking technique that is based on utilizing human visual systems (HVS) characteristics is presented in [4]. In this scheme, Watson [4] visual model was used to determine image dependent upper bound values on watermark insertion. The Watson model is based on the same image independent component utilizing frequency sensitivity as determined by measurements of specific viewing conditions. For watermark generation, the authors used bounded-normal (BN) distribution, which do not yield the value outside [-0.1, 1.0]. The reason was, watermarks which is generated from a normal distribution N (0,1), sometimes results in values that exceeds the JND which in turn makes image impairment. Watermark detection is performed by subtracting the original image from the received one, and the correlation between the signal difference and a specific watermark sequence was determined. The correlation value is compared to a threshold to determine whether the received image contains the watermark or not. Results were slightly higher than Podilchuk's scheme [5]. A revision to IA-DCT as applied to JPEG images [5][3] is proposed in [6], and avoids the use of the original unmarked image in the verification procedure. In this technique, it is assumed that the original image has already been JPEG compressed.

VII. CONCLUSION

Digital watermarking and data hiding has a very active research area. Methods for embedding data both in the spatial and in the frequency domain have been explored. The Spread spectrum allows detection of a known watermark, but the fundamentally large bandwidth requirement does not facilitate the extraction of a long bit sequence or logo from an audio signal or image. Spread spectrum approaches are vulnerable to inter-symbol interference caused by multi path -fading [2]. For watermarking this implies that if the energy of the watermark is reduced due to fading-like distortions on the watermark, any residual correlation between the host signal and watermark as discussed above can result in unreliable detection [3]. In Spatial Watermarking: Simple Systems one way to attack such systems is to break up the synchronization needed to locate the samples in which the mark is hidden, for example, one can crop the image. In Basic Spread Spectrum Approach the shortcoming of such method is in the channel capacity estimate, where they used the capacity formula for a Gaussian channel, which is not the best model of the noise in a single image. It assumes that the Gaussian channel has the same power at each frequency. But the host images do not have flat frequency characteristics, especially after compression. In Pattern Overlaying The robustness of the method with respect to filtering, JPEG compression, cropping, noise adding and collusion was studied and found that the watermark was resistant to all the above attacks. The watermarking method requires the original, un watermarked image in order to recover the watermark. In Spectral Watermarking: A Spread Spectrum Watermark Embedded in the DCT Domain: there is no mechanism for local spatial control in this particular framework. The limitation of this scheme is its | dependence on the original image for detection of the watermark, which makes it susceptible to multiple claims of ownership . In Transform-Based Approaches This watermarking scheme is difficult to implement in practice. The first difficulty is that both the log-polar mapping and the inverse logpolar mapping can cause a loss of image quality. The second difficulty is numerical, where the computation of the Fourier-Mellin transform somewhat problematic. In general, this method embeds watermarks, which resist rotation and scale transformations, however, with some loss in the robustness against JPEG compression. Also, the original image is needed for watermark extraction.

Improved Watermark detection is performed by subtracting the original image from the received one, and the correlation between the signal difference and a specific watermark sequence was determined. The correlation value is compared to a threshold to determine whether the received image contains the watermark or not. Results were slightly higher than other schemes. In this paper, we introduce several new techniques, which enable large quantities of data hiding in images and video and which implement channel codes such as block, convolution and concatenated codes. The Improved technique is robust to image/video compression, and one can recover the hidden data without requiring the availability of the host signal.

VIII. REFERENCES

[1] M. D. Swanson, M. Kobayashi, and A. Tawfik, "Multimedia Data-Embedding and Watermarking technologies," Proceedings of the IEEE, vol.86, no. 6, June 1998, pp. 1064-1087.

[2] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding- A survey," Proceedings of the IEEE, Special Issue on Protection of Multimedia Contents, vol. 87, no. 7, July 1999, pp. 1062 -1078.

[3] Bender W., Gruhl D., and Morimoto N., "Techniques for Data Hiding," Technical Report, MIT Media Lab, 1994.
[4] R. G. van Schyndel, A. Z. Tirkel and C. F. Osbome, "A Digital Watermark," Proceedings of IEEE International Conference on Image Processing, vol.2, pp. 86-90, Austin, Nov. 1994.
[5] Cox I., Kilian J., Leighton T., and Shamoon T.,"Secure spread-Spectrum watermarking for Multimedia," Technical Report 95-10, NEC Research Institute, 1995.
[6] 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, 1998, pp.357-372.
[7] D. Kundur, and D. Hatzinakos, "A Robust Digital Image watermarking Method using Wavelet-Based Fusion," Proceedings of the IEEE International Conference on Image Processing, Oct. 26-29, 1997,
Santa Barbara, CA, vol. 1, pp. 544-547.
[8] C. I. Podilchuck, and W. Zeng, "Image-Adaptive watermarking using Visual Model," IEEE Journal of selected Areas in Communications, Special Issue on Copyright and Privacy Protection, vol. 16, no. 4, May 1998, pp. 525-539.
[9] Linde Y., Buzo A., and Gray R. M., "AN Algorithm for vector Quantizer Design," IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 37, 1989, pp. 553-559.
[10] N. Abdulaziz and K. K. Pang, "Source and Channel Coding Approach for Data Hiding," Proceedings of SPIE, Visual Communications and
Image Processing 2000 Conference, 20-23 June 2000, Perth, Australia, pp. 1526-1535.
II1] N. Abdulaziz and K. K. Pang, "Performance Evaluation of Data Hiding System using Wavelet Transform and Error-Control Coding," In IEEE
International Conference on Image Processing 2000 , ICIP 2000, 10-13 September 2000, Vancouver, Canada.