A Study on Digital Watermarking Techniques

[L. Robert, Department of Computer Science, Government Arts College, Coimbatore, Tamilnadu, INDIA]
[T.Shanmugapriya, Research Scholar, Bharathiar University, Coimbatore, Tamil Nadu, India]

Email: {robert_lourdes@yahoo.com, shpriya_2k@yahoo.com, }

***Abstract*—With the widespread use of networks, intellectual properties can be obtained and reproduced easily. This creates a high demand for content protection technique like watermarking, which is one of the most efficient ways to protect the digital properties in recent years. This paper reviews several aspects and techniques about digital watermarking.**

***Index Terms*— content protection, watermarking, digital properties.**

I. Introduction

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. This paper provides a survey of techniques to watermark data files like text, images, audio and video.

II. Review on Digital Watermarking

Digital Watermarking technique [1] refers to the process of embedding the given watermark information

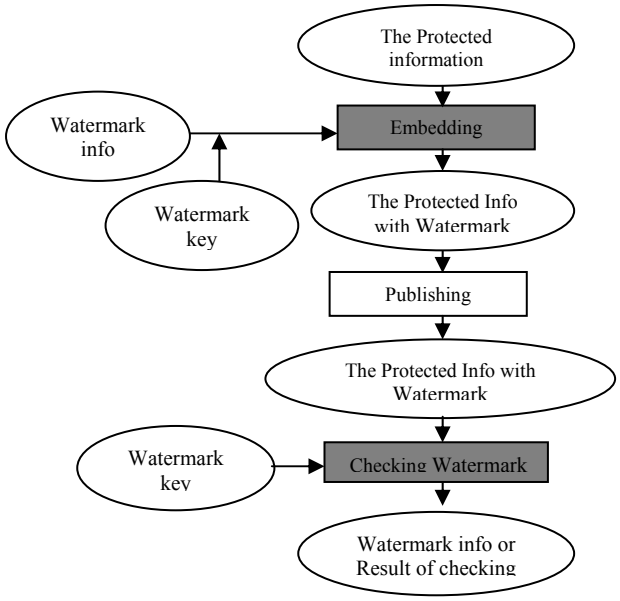

Fig 1: Fundamental Process of digital Watermarking

(such as prossessory name, symbol, signature etc.) into the protective information (such as picture, sound, video) and picking the given watermark information from the protective information, which is not perceived by human perceptual system. Fig.1 shows the fundamental process of digital watermarking technique. "Ref. [1, 2]" gives sufficient detail about watermarking requirements and its type like robust and fragile watermarking.

III. Three Stages in Watermarking

A. Generation and Embedding

Pseudo Random Sequence, M- Sequence and Chaotic Sequence are some sequences used for watermark generation [5]. The embedding process can be understood as the combination of watermark signal and original image.

B. Distribution and Possible Attacks

The distribution process can be seen as the transmission of the signal through the watermark channel. Possible attacks in the broadcast channel may be intentional or accidental.

C. Detection

Detection process allows the owner to be identified and provides information to the intended recipient. There are two kinds detection: Informed detection and Blind detection.

IV. Text Watermarking Techniques

A. Spread Spectrum Technique of Watermarking

Watermark bits (b) are mixed with PRN (Pseudo Random Noise) generated signal and then this signal is inserted in the host signal (X). This PRN signal functions as a secret key. Fig. 2 shows such mechanism [3].

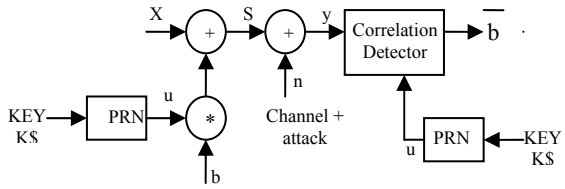

Fig 2: Spread spectrum based watermarking - b bit to be embedded

The watermarked signal's amplitude is much less then 1% of the host's amplitude. This specific PRN signal can later on be detected by correlation receiver or match filter.

B. Line-Shift Coding

Here each even line is slightly shifted up or down according to the bit value in the payload [7]. If the bit is one, the corresponding line is shifted up; otherwise, the line is shifted down. The odd lines are considered as control lines and used at decoding.

In the context of standardization activities, objective performance metrics are needed to evaluate whether one of the established are emerging watermarking technique is superior to

Fig 3: Example of line-shift coding. The second line has been shifted up by 0.085 mm

C. Word-Shift Coding

Here each line is first divided into groups of words. Each group has a sufficient number of characters. Then, each even group is shifted to the left or the right according to the bit value in the payload. The odd groups are used as references for measuring and comparing the distances between the groups at decoding [8].

D. Feature Coding

In this method, certain text features (e.g., vertical end lines) are altered in a specific way to encode the zeros and ones of the payloads. Watermark detection is achieved by comparing the original document with the watermarked document [8].

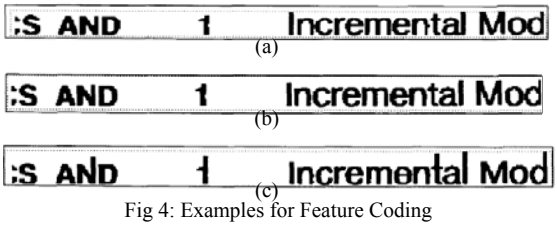

Fig 4: Examples for Feature Coding

In Fig. 4 feature coding is performed on a portion of text from a journal table of contents. In (a), no coding has been applied. In (b), feature coding has been applied to select characters. In (c), the feature coding has been exaggerated to show feature alterations [8].

V. IMAGE WATERMARKING TECHNIQUES

Images can be represented as pixels in spatial domain or in terms of frequencies in transform domain. To transfer an image to its frequency representation we use reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT) [6]. Watermarks can be embedded within images by modifying these values, i.e. the pixel values or the transform domain coefficients [9].

A. DCT Domain Watermarking

In frequency domain the high frequency components are watermarked. The main steps are

1) Segment the image into non-overlapping blocks of 8x8

2) Apply forward DCTto each of these blocks

3) Apply some block selection criteria (e.g. HVS)

4) Apply coefficient selection criteria (e.g. highest)

5) Embed watermark by modifying the selected coefficients.

6) Apply inverse DCT transformn on each block

B. DWT Domain Watermarking

Here the underlying concept is the same as DCT however, the process to transform the image into its transform domain varies and hence the resulting coefficients are different. Wavelet transforms use wavelet filters like Haar Wavelet Filter, Daubechies Orthogonal Filters and Daubechies Bi-Orthogonal Filters to transform the image. Each of these filters decomposes the image into several frequencies. Single level decomposition gives four frequency representations of an image like LL, LH, HL, HH subbands.

C. DFT Domain Watermarking

DFT domain has been explored by researches because it offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. There are two different kinds of DFT based watermark embedding techniques. One in which watermark is directly embedded and another one is template based embedding. In direct embedding watermark is embedded by modifying the phase information within the DFT.

A template is a structure which is embedded in the DFT domain to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, and then use the detector to extract the embedded spread spectrum watermark.

VI. AUDIO WATERMARKING TECHNIQUES

The amount of data that can be embedded [4,5] into audio is considerably low than amount that can be hidden in images, as audio signal has a dimension less than two-dimensional image files. Embedding additional information into audio sequence is a more tedious than images, due to dynamic supremacy of HAS than HVS.

A. Least Significant Bit Coding

This simple approach in watermarking audio sequences is to embed watermark data by altering certain LSBs of the digital audio stream with low amplitude.

B. Phase coding

The basic idea is to split the original audio stream into blocks and embed the whole watermark data sequence into the phase spectrum of the first block.

C. Quantization Method

A scalar quantization scheme quantizes a sample value x and assign new value to the sample x based on the quantized sample value. In other words, the watermarked sample value y is represented as follows:

$$y = q(x, D) + D/4 \quad \text{if b} = 1,$$
$$y = q(x, D) - D/4 \quad \text{otherwise} \qquad (1)$$

In (1) q (·) is a quantization function and D is a quantization step. A quantization function q (x) is given as $q(x, D) = [x/D].D$, where [x] rounds to the nearest integer of x. A sample value x is quantized to $q(x, D)$. Let q (x, D) denote anchor. If the watermarking bit b is 1, the anchor is moved. Otherwise, the cross (×) stands for the watermarking bit 0.

D. Spread-Spectrum Method

This scheme [3] spreads pseudo-random sequence across the audio signal. The wideband noise can be spread into either time-domain signal or transform-domain signal. Frequently used transforms include DCT, DFT, and DWT.

E. Replica Method

Original signal can be used as an audio watermark. Echo hiding is a good example. Replica modulation also embeds part of the original signal in frequency domain as a watermark.

Echo Hiding

Echo hiding embeds data into an original audio signal by introducing an echo in the time domain. For simplicity, a single echo is added in Fig 5. However, multiple echoes can be added (Bender *et al.* 1996). Binary messages are

embedded by echoing the original signal with one or two delays, either a d_0 sample delay or a d_1 sample delay. Extraction of the embedded message involves the detection of delay *d*.

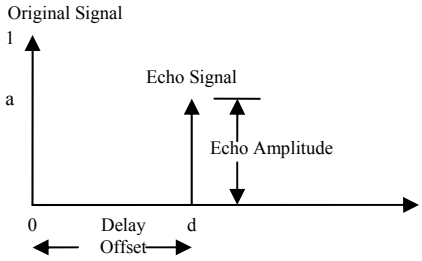

Fig 5: Kernels of Echo Hiding

VII. VIDEO WATERMARKING TECHNIQUES

A. *Embedding in the spatial domain*

Embedding in the spatial domain [4, 5] is one of the characteristics of JAWS video watermarking algorithm by Kalker et al. It embeds a watermark pattern W in the spatial domain by changing intensity values to guarantee robustness against color conversions. If the spatial correlation value C_τ exceeds a certain threshold τ, the watermark is detected otherwise no watermark. This allows the embedding of one-bit pay load.

B. *Embedding in the transformation domain*

Embedding in the transformation domain [5] can be similar to image watermarking in the transformation domain as realized in the SysCoP video watermarking algorithm by Busch et al. Real-time-capable implementations of the DCT and inverse DCT are used. The SysCoP algorithm is executed on a digital signal processor (DSP) board. Visual quality is increased by checking if the block that is used for watermarking contains textures or edges. Blocks identified as plain areas are watermarked with lower strength. Robustness against MPEG2 compression is achieved by maximum redundancy. Almost all blocks of a video frame are subjected to the watermark procedure.

C. *Embedding in the compressed domain*

Hartung and Girod proposed a method that is capable of embedding the information also in the compressed domain and retrieving the information from the decompressed domain. The general scheme of the proposed method is shown in Fig 6.Only the DCT coefficients of the MPEG 2 bit stream are modified. Before modification, MPEG 2 compression operations are inverted. Thus, this scheme is in fact embedded in the transformation domain. After adding the watermark, which is a two-dimensional signal and was transformed in the DCT domain, the new bit rate is compared with the original and, depending on the bit rate; the original DCT block is selected.

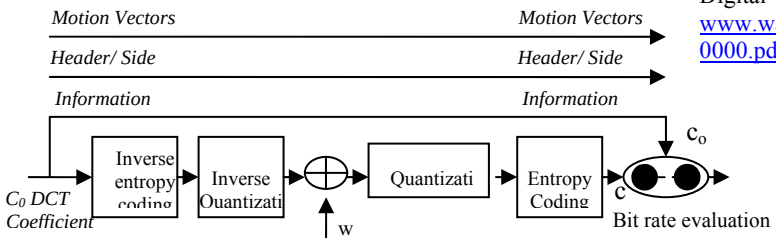

Fig 7: The Block diagram of compressed video marking

VIII. CONCLUSION

This paper reviews various techniques for watermarking data files like text, image, audio and video. According to the paper, we can conclude that watermarking is a potential approach for protection of ownership rights on digital properties. According to different applications, there are different requirements of the watermarking system. However, it is hard to satisfy all the requirements at the same time. So, benchmark is used to evaluate and compare the performance of different watermarking systems.

REFERENCES

[1] Jian Liu, Xiangjian He; "A Review Study on Digital Watermarking", Information and Communication Technologies, 2005. ICICT 2005. First International Conference, Page(s):337 – 341, 27-28 Aug. 2005.

[2] Cox, I.J., M.L. Miller, and J.A. Bloom, "Digital Watermarking.", 1st edition 2001, San Francisco: Morgan Kaufmann Publisher.

[3] I.J. Cox, J. Kilian. F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia." IEEE Transactions on Image Processing, Vol. 6, No. 12, pp. 1673-1687, Dec. 1997.

[4] Juergen Seitz, University of Cooperative Education Heidenheim, Germany, "Digital Watermarking for Digital Media", 1st edition May 2005, Information Science Publishing.

[5] Michael Arnold, Martin Schmucker, Stephen D.Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection", 1st edition July 2003, Artech House.

[6] Potdar V.M., Han, S., Chang, E.; "A survey of digital image watermarking techniques", Industrial Informatics, 2005. INDIN '05. 2005 3rd IEEE International Conference, Page(s):709 – 716, 10-12 Aug 2005.

[7] Micic, A.; Radenkovic, D.; Nikolic, S.; "Autentification of Text Documents Using Digital Watermarking", Telecommunications in Modern Satellite, Cable and Broadcasting Services, 2005. 7th International Conference on Volume 2, Page(s):503 – 505, 28-30 Sept. 2005.

[8] Brassil, J.T.; Low, S.; Maxemchuk, N.F.; O'Gorman, L.; "Electronic marking and identification techniques to discourage document copying", Selected Areas in Communications, IEEE Journal on Volume 13, Issue 8, Oct. 1995 Page(s):1495 – 1504

[9] Guan-Ming Su, "An Overview of Transparent and Robust Digital Image Watermarking". Available online at www.watermarkingworld.orgLWMMLArchive/0504/pdf00000.pdf