A REVIEW STUDY ON DIGITAL WATERMARKING TECHNIQUES

Vineet Raj Singh Kushwah[1], Sumit Tiwari[2], Manvendra Gautam[3]
[1]Prof., Dept. of CSE, IPS–CTM, Gwalior(M.P)
[2]PG Scholar,Dept. of CSE, SRCEM, Banmore, (M.P)
[3]Asst. Prof., Dept. of CSE, IPS –CTM, Gwalior, (M.P)
Email: vineetkushwah@yahoo.co.in[1], sumitgwalior23@gmail.com[2],manavgautam2010@gmail.com[3]

Abstract
With the fast development of web technology and the digital multimedia, the usage of multimedia (audio, video and image etc) has been widely spread. By increasing of these things, intellectual properties can be obtained and reproduced simply. So there is need of our content protection therefore to do so there is a technique like watermarking, which is one of the most effective ways to safeguards the digital properties of our object. This paper reviews various techniques and aspects about digital watermarking.

Index terms: content protection, watermarking, digital properties.

I. INTRODUCTION

Watermarking technique is used for information hiding which is used to conceal proprietary information in digital media as photographs, digital video, digital music etc. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Over peer-to-peer networks, copyrighted material can be easily exchanged, and this makes serious concerns to those content providers who produce these digital contents. This paper provides a survey of watermark techniques for files like video, text, images and audio.

II. REVIEW ON DIGITAL WATERMARKING

Digital Watermarking technique [1] means the process to embed the given watermark information

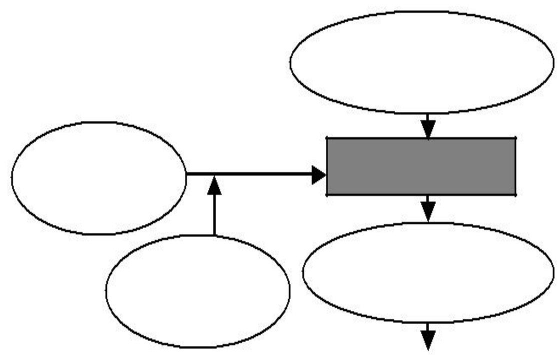


Fig 1: Fundamental Process of digital Watermarking

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

III. THREE STAGES IN WATERMARKING

A. Generation and Embedding

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

B. Distribution and Possible Attacks

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

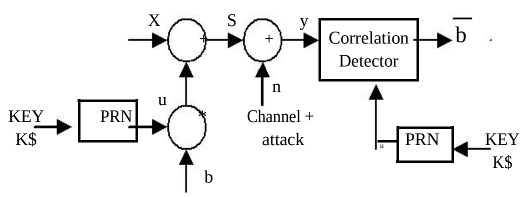
C. Detection

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

IV. TEXT WATERMARKING TECHNIQUES

A. Spread Spectrum Technique of Watermarking

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



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

B. Line-Shift Coding

Here each even line is slightly shifted down or according to the bit value in the payload [7]. The corresponding line is shifted up, if the bit is one; otherwise, the line is shifted down. The odd lines are act 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 we divide each line into group of words. Each group has a enough number of characters. Then, According to the bit value in the payload, each even group is shifted to the right or the left. The odd groups are treated as references for measuring and comparing the distances between the groups at decoding [8].

D. Feature Coding

Here certain text features (e.g., vertical end lines) are changed in a specific way to encode the ones and zeros of the payloads. To detect Watermark the original document is compared with the watermarked document [8].

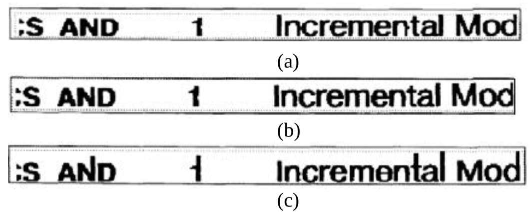


Fig 4: Examples for Feature Coding

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

V. IMAGE WATERMARKING TECHNIQUES

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

A. DCT Domain Watermarking

The high frequency components are watermarked in frequency domain. The main steps are

1) Divide 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 transform 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 changes and in this way the resulting coefficients comes different. Wavelet transforms use wavelet filters like Daubechies Orthogonal Filters, Haar Wavelet Filter and Daubechies Bi-Orthogonal Filters to transform the image. Each of these filters breaks the image into many frequencies. Single level decomposition yields four frequency representations of an image like LL, HH, LL, HH subbands.

C. DFT Domain Watermarking

DFT domain is favorite choice of researches because it provides robustness against geometric attacks like translation, rotation, cropping, scaling etc. There are two types of DFT based watermark embedding techniques. In first technique watermark is directly embedded and another technique is template based embedding. In direct embedding watermark is embedded by changing the phase information within the DFT.

A template is a structure which is used in the DFT domain to judge the transformation factor. First a transformation is made in image then to resynchronize the image this template is searched, and then employ the detector to extract the embedded spread spectrum watermark.

VI. AUDIO WATERMARKING TECHNIQUES

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

A. Least Significant Bit Coding

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

B. Phase coding

The basic idea is to divide the original audio stream into blocks and insert 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:

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

In (1) $q\ (\cdot)$ 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 transform-domain signal or time-domain signal. Frequently used transforms include DWT, DFT, and DCT.

E. Replica Method

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

Echo Hiding

The Echo hiding inserts data into an original audio signal by introducing an echo in the time domain. For example, 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. that 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.

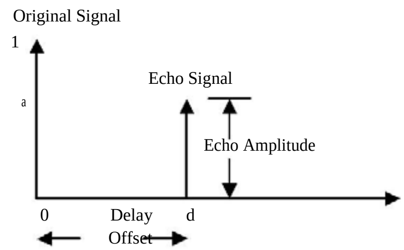


Fig 5: Kernels of Echo Hiding

VII. VIDEO WATERMARKING TECHNIQUES

A. Embedding in the spatial domain

Sspatial domain [4, 5] embedding is one of the characteristics of JAWS video watermarking algorithm by Kalker et al. It is used to embed watermark pattern W in the spatial domain by altering intensity values to guarantee robustness for color conversions. If the spatial correlation value C_τ goes more than a certain threshold τ, the watermark is found otherwise no watermark. This shows the embedding of one-bit pay load.

B. Embedding in the transformation domain

Transformation domain [5] embedding can be analogous to image watermarking in the transformation domain as seen in the SysCoP video watermarking algorithm by Busch et al. Real-time-capable implementations of the inverse DCT and DCT are used. The SysCoP algorithm is run on a digital signal processor (DSP) board. If the block comprises edges or textures visual quality can also be increased. The Blocks which are found plain areas, they are watermarked with lower strength. Robustness against MPEG2 compression is accomplished by maximum redundancy. Almost watermark procedure is deployed to all blocks of a video frame.

C. Embedding in the compressed domain

A method was proposed by Girod and Hartung that is used to embed the information in the compressed domain also and getting back the information from the decompressed domain. The general diagram of the that method is shown in Fig 6. DCT coefficients of the MPEG 2 bit stream are altered only. Before modification, MPEG 2 compression operations are inverted. Hence, After adding the watermark, this scheme is really embedded in the transformation domain,

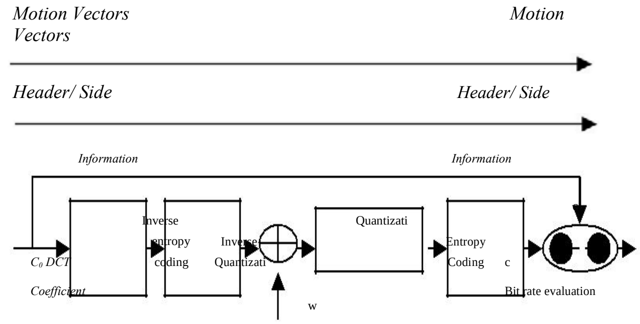


Fig 7: The Block diagram of compressed video marking

VIII. CONCLUSION

This paper reviews many techniques for watermarking data files like audio, text, image and video. So, we can conclude that watermarking is a significant approach for protection of copyrights on digital properties. Different watermarking techniques are used for various types of requirements. However, it is difficult to satisfy all the requirements at the same time. So, benchmark is used to compare the performance of different watermarking systems and evaluate.

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/pdf0 0000.pdf