WATERMARKING TECHNIQUES

[1]A.Manikandan
Research Scholar
Department of Computer Science & Engineering
Alagappa University
Karaikudi.

[2]Dr. T. Meyyappan,
M.Sc., M.Phil.,M.B.A.,Ph.D.,
Associate Professor
Department of Computer Science & Engineering
Alagappa University
Karaikudi.

Abstract:- Embedding a hidden stream of bits in a file is called Digital watermarking. The file could be an image, audio, video or text. Nowadays, a digital watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control and file reconstruction. It is intended to complement cryptographic processes. It is a visible or preferably invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. The focus of this paper will detail digital watermarking for multimedia applications and covered by definition of digital watermarking, purpose, techniques and types of watermarking attacks briefly discussed.

Index Terms: Digital watermarking, Watermarking Requirements, Advance Techniques.

A. Introduction

Digital watermarking technology is now drawing the attention as a new method of protecting copyrights for digital images. It is realized by embedding data that is insensible for the human visual system. Embedding a hidden stream of bits in a file is called Digital Watermarking. The file could be an image, audio, video or text. Nowadays, digital watermarking has many applications such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control and file reconstruction.

A digital watermark is a visible or perfectly invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. The digital watermark is then introduced to solve this problem. Covering many subjects such as signal processing, communication theory and Encryption, the research in digital watermark is to provide copyright protection to digital products, and to prevent and track illegal copying and transmission of them. Watermarking is embedding information, which is able to show the ownership or track copyright intrusion, into the digital image, video or audio.

Now the digital watermarking technologies can be divided into two types. By the embedding position spatial domain and transform domain watermark. Spatial domain techniques developed earlier and is easier to implement, but is limited in robustness, while transform domain techniques, which embed watermark in the host's transform domain, is more sophisticated and robust. With the development of digital watermarking, spatial techniques, due to their weakness in robustness, are generally abandoned, and frequency algorithm based on DCT or DWT becomes the research focus. Another tendency in watermarking is blind extraction, which means the host is not need when extracting the watermark otherwise it is hard to avoid the multiple claims of ownerships.

B. The Foundation of Digital Watermarking

It should be noted that he reason why digital watermarking is possible is that human vision system (HVS) is not perfect. Digital watermark utilizes the limitation of HVS to make it invisible, thus avoiding degrading original digital products, as well being hard to get identified or destroyed.

C. Watermarking Requirements

Security: The security requirement of a watermarking system can differ slightly depending on the application. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks [7].

Imperceptibility: The imperceptibility refers to the perceptual transparency of the

Watermark. Ideally, no perceptible difference between the watermarked and original signal should exist [4, 5]. A straightforward way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host signal [5].

Capacity: Watermarking capacity normally refers to the amount of information that can be embedded into a host signal. Generally speaking, capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness. Higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.

Invisible A watermarking system is of no use if it distorts the cover image to the point of being useless, or even highly distracting. Ideally the watermarked imaged should look indistinguishable from the original even on the highest quality equipment.

Robust The watermark should be resistant to distortion introduced during either normal use (unintentional attack), or a deliberate attempt to disable or remove the watermark present (intentional, or malicious attack). Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing, contrast enhancement...etc.

Unambiguous Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

D. Classification of Digital Watermarking

According to the domain for watermark embedding

Spatial Domain Watermarking: The image is considered to be a two-dimensional array and manipulating certain pixels based on their spatial locations in the array embeds the watermark. Techniques may be as simple as flipping the least significant bit (LSB) or may be a complex superposition of watermarking symbols over an area of the image. In the latter technique, a lot of flexibility exists in terms of placement, size, and intensity of the watermark. Spatial-domain watermarking technologies change the intensity of original image or gray levels of its pixels. This kind of watermarking is simple and with low computing complexity, because no frequency transform is needed. However, there must be tradeoffs between invisibility and robustness, and it is hard to resist common image processing and noise.

Frequency Domain Watermarking: The image is considered to be a sampled-digitized data of an analog signal. The analog signal can be obtained by various transforms like the DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform), FFT (Fast Fourier Transform) etc. and hence represented as a series of signals of increasing frequencies. The watermark can now be embedded in the coefficients of the various frequency components. The watermark is not embedded in the high frequency components, as they are usually lost on compression or scaling. Frequency domain watermarking disperses the watermark over the whole image thus rendering it less visible (or detectable) than spatial domain watermarking. However, it is more difficult to decode a watermark applied in the frequency domain. Another novel method is to embed the watermark in the phase component of the DFT. It has been demonstrated quite conclusively that the phase is more important than the magnitude of the DFT values, so a watermark embedded in the phase will be robust to tampering as any noise deliberately introduced will have to be sufficiently large to destroy the watermark thus damaging the image. It has also been shown that angle modulation possesses superior noise immunity when compared to amplitude modulation. Also, a phase-based watermark is robust to changes in image contrast. Frequency-domain watermarking embeds the watermark into the transformed image. It is complicated but has the merits which the former approach lacks.

According to how watermark is detected and extracted

Blind-extracting watermarking means watermark detection and extraction do not depend on the availability of original image. The drawback is when the watermarked image is seriously destroyed; watermark detection will become very difficult.

Non-blind extracting watermark can only be detected by those who have a copy of original image. It guarantees better robustness but may lead to multiple claims of ownerships.

According to the ability of watermark to resist attack

Fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from heavily attacked watermarked image. Thus it is preferred in copyright protection.

E. Techniques used for watermarking

Numerous methods for watermarking exist and they can be classified based on various parameters like the embedding algorithms and the detection algorithms used. We shall study them based on the data they watermark.

I) watermarking for Images:

Image data is binary in nature i.e. all image files are a combination of zeros and ones. Thus they are easily manipulated, processed, and tampered with. Hence, robust and standard watermarks for image files are a challenge. Images, being digital in nature, can be visualized in two forms either they can be thought of as a two-dimensional array of zeros or ones or they can be considered to be the digital representation of an analog signal. Watermarking techniques for images are based on these methods of representation.

II) Watermarking Audio Data:

It is relatively tough to watermark audio data as the human ear can detect even the slightest change in tone or delay. Watermarks for audio data, in addition to the existing conditions, must not tend to accumulate in particular time intervals. If the signal energy is concentrated in a time interval, then it may happen that the watermark is not watermarked in that time interval. One method that has been proposed is to generate sequences with filters approximating the human auditory system's frequency masking characteristics. To prevent audible distortion, the watermark is weighed or attenuated in the time domain with the relative energies of the signal. It has also been observed that the human auditory system is insensitive to phase distortion. Hence a variety of phase based watermarks can be explored. However, as of now watermarks for audio data are far away.

III) Watermarking Video Data:

Video clips on the computer are displayed at the rate of thirty frames per second. A movie of one and half-hours will thus have about sixteen lakh frames. The very magnitude rules out watermarking each frame. A constant standard watermark is preferred. In publicly broadcast video the watermark is the corporate logo whose constant presence acts as a watermark and advertises the channel. In private screenings, the same is possible. Invisible watermarks for video data face the same problems as for audio data and tend to be more complex and demanding. Considering the fact that the volume of data dealt with is enormous and that the data is usually compressed, watermarking video data is a daunting task. We have examined various watermarking techniques for a wide range of data. Watermarking ASCII (American Standard Code for Information Interchange) representations of text is nearly impossible, as modifying even the LSB will alter the meaning or the basic utility of the data. Text needs to be represented either as a bitmap or as a formatted document in order to be able to watermark it.

A. Embedding and Extraction

In this technique the insignificant portion of the fractional part of the pixel intensity value of the cover image is encoded to provide watermark. A watermark in the insignificant part has helped to maintain the fidelity of the cover image. As seen from the results, imperceptibility is well preserved. Large capacity of watermarking is an added advantage of this scheme. Thus, large capacity watermark may be successfully embedded and extracted using this scheme, which can be extremely useful for companies engaged in developing watermarking applications and digital information security products. Embedding and extraction algorithms are used in this technique [3].

B. Secure Spread Spectrum Watermarking

We describe a digital watermarking method for use in audio, image, video and multimedia data. We 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 malicious attack. However, it is well known that modification of these components can lead to perceptual degradation of the signal. To avoid this, we 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 wideband channel that is the data. The watermark is difficult for an attacker to remove, even when several individuals conspire together with independently watermarked copies of the data. It is also robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital conversion, resampling, quantization, dithering, compression, rotation, translation, cropping and scaling. The same digital watermarking algorithm can be applied to all three media under consideration with only minor modifications, making it especially appropriate for multimedia products. Retrieval of the watermark unambiguously identifies the owner, and the watermark can be constructed to make counterfeiting almost impossible. We present experimental results to support these claims [4].

C.DCT-based watermarking

The image is first divided into 8 × 8 pixel blocks. After DCT transform and quantization, the mid-frequency range DCT coefficients are selected based on a Gaussian network classifier. The mid-frequency range DCT coefficients are then used for embedding. Those coefficients are modified using linear DCT constraints. It is claimed that the algorithm is resistant to JPEG compression. [5]

D. Wavelet Based Watermarking

The multi resolution data fusion is used for embedding where the image and the watermark are both transformed into the discrete wavelet domain. The watermark is embedded into each wavelet decomposition level of the host image. During detection, the watermark is an average of the estimates from each resolution level of wavelet decomposition. This algorithm is robust against JPEG compression, additive noise and filtering operations.

E. Robust Watermarking Technique

Contrary to the LSB approach, the key to making a watermark robust is that it should be embedded in the perceptually significant components of the image. A good watermark is one which takes into account the behaviour of human visual system. For the spread spectrum based watermarking algorithm, a scaling factor can be used to control the amount of energy a watermark has. The watermark energy should be strong enough to withstand possible attacks and distortions. Meanwhile large watermark energy will affect the visual quality of the watermarked image. A perceptual model is needed to adjust the value of the scaling factor based on the visual property of the host image to achieve the optimal trade-off between robustness and invisibility.

F. Invisible Watermarking

This technique presents a novel invisible robust watermarking scheme for embedding and extracting a digital watermark in an image. The novelty lies in determining a perceptually important sub image in the host image. Invisible insertion of the watermark is performed in the most significant region of the host image such that tampering of that portion with an intention to remove or destroy will degrade the aesthetic quality and value of the image. One feature of the algorithm is that this sub image is used as a region of interest for the watermarking process and eliminates the chance of watermark removal. Another feature of the algorithm is the creation of a compound watermark using the input user watermark (logo) and attributes of the host image. This facilitates the homogeneous fusion of a watermark with the cover image, preserves the quality of the host image, and allows robust insertion-extraction. Watermark creation consists of two distinct phases. During the first phase, a statistical image is synthesized from a perceptually important sub image of the image. A compound watermark is created by embedding a watermark (logo) into the statistical synthetic image by using a visible watermarking technique. This compound watermark is invisibly embedded into the important block of the host image. The authentication process involves extraction of the perceptive logo as well statistical testing for two-layer evidence. A result of the experimentation using standard benchmarks demonstrates the robustness and efficacy of the proposed watermarking approach. Ownership proof could be established under various hostile attacks [6].

F. CONCLUSION

In this paper, we have surveyed many of the techniques proposed for watermarking. Thus this paper may serve as a ready reference for any new researcher willing to explore the basics and foundation works in the area of digital watermarking since its evolution to the point where it started gaining prominence in the area of digital media control. This paper gives a base to understand the recent advances in digital watermarking. In this paper we have presented description and analysis of recent advances in watermarking in digital media controls. By this paper I have concentrated to do work on audio watermarking technique.

References

[1] N. Nikolaidis, I. Pitas, “Copy right Protection of images using robust digital signatures”, in proceeding, IEEE International Conferences on Acoustics, Speech and signal processing , Vol.4, 1996, pp. 2168-2171.

[2] Cox, J. Kilian, F. Leighton, T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Processing, vol. 6,pp. 1673–1687, 1997.

[3] [Online]Available: http://www.ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=560429[new technique]

[4] C. Podilchuk and W. Zeng. Image-adaptive Watermarking Using Visual Models. In IEEE Journal Selected. Areas of Communications, vol. 16, pp. 525-539, May 1998.

[5] C. Podilchuk and E. Delp. Digital Watermarking Algorithms and Applications. In IEEE Signal Processing Magazine, vol. 18, no. 4,July 2001.

[6] [Online] Available: http://www.deliver y.acm. org/10.1145/1420000/1413865/a12mohanty.pdf?ip=203.129.220.149&CFID=39257849&CFTOKEN=22823083&__acm__=1314075842_8220e809658bae8e b4f2777727740a1a

[7] C.-T. Li and F.M. Yang. One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.