VARIOUS MEDIA TYPES AND ITS APPLICATION USING DIGITAL WATERMARKING

SATHAWANE M.S. AND BORA P.P.

Department of Computer Science and Engineering, J.D.I.E.T., Yavatmal, MS, India. *Corresponding Author: Email- megha_ssathawane@yahoo.co.in and pulse.ytl56@gmail.com

Received: March 06, 2012; Accepted: May 08, 2012

Abstract- Digital Watermarking came in great demand when sharing information on internet became a usual practice sharing files online, you never know if someone uses them without your consent. To prevent unauthorized commerce use of your file, you can published them to the web in worst quantity or don't published anything worthwhile at all. It isn't a good way to solve the problem of unauthorized use, is it? So, you should look for more effective ways of copyright protection, such as Digital Watermarking.

Digital Watermarking technology is general purpose technology with wide variety of possible application. The technology offers a means of conveying information inside a Digital media file (For Ex. Inside a photo, movie, song). It frequently use to signal basic identifying information about the specific media file in which it contained, much like a file header does. Digital Watermarking doesn't inherently pose risk to privacy. **Keywords-** Digital Watermarking, Digital media file

Citation: Sathawane M.S. and Bora P.P. (2012) Various Media Types and its Application Using Digital Watermarking. World Research Journal of Pattern Recognition, ISSN: 2278-8557 & E-ISSN: 2278-8565, Volume 1, Issue 1, pp.-09-11.

Copyright: Copyright©2012 Sathawane M.S. and Bora P.P. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Introduction

Although different authors use different meanings for the word 'watermark', it is mostly agreed that the watermark is one, which is imperceptibly added to the cover-signal in order to convey the hidden data.

The process of embedding information into another object/signal can be termed as watermarking. Digital watermarking is the process of embedding information into digital signal. The signal maybe audio, picture or video, for example. If the signal is copied, then the information is also carried in the copy.

A digital watermark is, in essence, a hidden message, within a digitized image, video or audio recording. The watermark is integrated into the content itself, so it requires no additional storage space. It can contain any information that a party writing the watermark cares to embed into a given work. Practically speaking though, space is at a premium, so the embedded message is usually quite small, often a short number. However that identifier can be mapped to any other kind of information – the composer's name, the studio musician who recorded his composition, or the name and e-mail address of the consumer. A traditional water-

mark on paper, which is generally visible to the eye, digital watermarks can be made invisible or inaudible. They can however, be read by a computer with the proper decoding software.

Watermarking for Various Media Types Techniques Digital Audio Watermarking

Digital watermarking is a technology which allows a secret message to be hidden in a computer file, without the detection of the user. The watermark is not apparent to the user, and does not affect in any way, the use of the original file. Watermarking information is predominantly used to identify the creator of a digital file, i.e. a picture, a song, or text.

Digital audio watermarking involves the concealing of data within a discrete audio file. Applications for this technology are numerous. Intellectual property protection is currently the main driving force behind research in this area. To combat online music piracy, a digital watermark could be added to all recording prior to release, signifying not only the author of the work, but the user who has purchased a legitimate copy. Newer operating systems equipped with digital rights management software (DRM) will

Bioinfo Publications 9

extract the watermark from audio files prior to playing them on the system. The DRM software will ensure that the user has paid for the song by comparing the watermark to the existing purchased licenses on the system.

Other non-rights related uses for watermarking technology include embedding auxiliary information which is related to a particular song, like lyrics, album information, or a small web page, etc. Watermarking could be used in voice conferencing systems to indicate to others which party is currently speaking. A video application of this technology would consist of embedding subtitles or closed captioning information as a watermark.

Watermarking is not restricted to just images. Audio watermarking uses the time and frequency masking properties of the human ear to conceal the watermark, and make it inaudible. One of the techniques is echo-hiding which involves hiding information within recorded sound by introducing very short echoes. relying on the fact that the human auditory system cannot perceive echoes shorter than a few milliseconds. Information is embedded into audio data by introducing two types of echoes, characterized by their duration and relative amplitude. This allows us to encode ones and zeros within the audio data.

While digital watermarking holds much promise, current techniques are inadequate for general use. Watermarks are destroyed too easily to be used as evidence of copyright infringement in a court of law.

Despite the vulnerability of current techniques, watermarking remains important as long as it hinders the task of copyright infringement, and current tools offer this to a limited degree. Digital watermarking is an as yet unproven technology which, though in its infancy, is set to grow, making a large impact on the way in which digital media is distribute.

Digital Video Watermarking

A very simple definition of video watermarking would be, "the process of watermarking the sequence of video frames". There are several avenues in case of video to watermark. One can watermark the raw frame data, or the compressed data, where watermark the latter is more challenging.

Videos can be considered as a stream of individual images. Hence, all image watermarking techniques are equally applicable to video when the individual frames are treated as images. Such techniques do not make use of the availability of the temporal domain apart from the domain which image provide. This can lead to the design and use of sophisticated techniques, exploiting the presence of temporal domain. At the same time, the video provide new avenues for designing better attacks as well.

The easiest (simplest) way to watermark an image/video is to change directly the values of the pixels, in the spatial domain. A more advanced way to do it, is to insert the watermark in the frequency domain, using one of the well-known transforms.

Image Watermarking

The digital age has simplified the process of content delivery and has increased the ease at which the buyer can re-distribute the content, thus denying the income to the seller. Images published on the internet is an example of such content. This section will questions related to image watermarking.

Visible watermarks on image can be easily achieved through im-

age editing software. Ex. Imagemagick or any other, which have the watermark functionality. Invisible watermarks on images can be achieved through some properitary softwares. There are several papers in the literary world which help one to implement their own invisible watermark. The following are some of the places to start with to learn/implement watermarking for images.

A watermark is a process by which an image becomes part of a piece of paper, usually this is done by having the paper dry non uniformly because a mesh in the shape of the desire watermark was put in contact with the still wet paper stock. Watermark is thus a safety feature as it is part of the paper, not a part of what get printed on top of it and is thus used for banknotes. The same general concept can be expanded with digital information.

Text Watermarking

Digital watermarking texts and sensitive documents is a lot more difficult than watermarking images and videos. There are a lot of redundancies in images, music files and videos. Since every pixel carries with it information, watermarking these types of media is a lot easier than doing the same on sensitive documents or text where every letter or word is important.

University research professors in Purdue have suggested a way of effectively imprinting a digital watermark in texts by using the structure or the syntax of the language itself to embed the watermark. By using a special algorithm, digital watermarks can be obtained within a text or a document by making small grammatical changes in the document while keeping the meaning the same. Moreover, this technique has been found to be effective even when some words have been deleted or changed from the document.

With the growing threat of piracy in the Internet and copyright infringement cases, digital watermarks are sure to serve an important role in the future of intellectual. This problem, which in fact was one of the first that was studied within the information destruct the possible intention of the author. Executable watermarks.

Once the hidden channel has been created it is possible to include even executable contents, provided that the corresponding applet is running on the end user side. Labeling. The hidden message could also contain labels that allow for example to annotate images or audio. Of course, the annotation may also been included in a separate file, but with watermarking it results more difficult to destroy or loose this label, since it becomes closely tied to the object that annotates. This is especially useful in medical applications since it prevents dangerous errors.

Text watermarking is the process of inserting watermark into the text for preserving the creator's identity. An earlier form of watermarking the texts was accomplished by inserting spaces in specific parts of the text. The disadvantage associated with this form of watermarking was that it was quite easy to remove the watermark. Later on, watermarks were placed in the text that depends on linguistic properties like synonyms, sequence of words etc. minor modifications are made to characters, and such characters are used for watermarking. Text watermarking schemes are applicable to any type of texts from usual word documents to PDF files. At detection stage, the watermark is removed by processing which involves the correction for noise, and distortion introduced, if any (during the insertion process) as well. This scheme protects texts like poetry well as, the changes brought about in the text will dam-

age the worth of it. This is also resistant to attacks like photocopying because these do not alter the watermark.

Applications

Some of the additional applications of digital watermarking are broadcast monitoring, usage of contractual watermarks for special purposes, secret communication and copy control.

Broadcast Monitoring

Watermarks are used in broadcast monitoring by inserting watermarks in the message that is to be transmitted. This is done before signal (audio or video) is broadcasted.

Contractual Watermarks

These types of watermarks are also called fingerprints. One of the applications of these is in the distribution of daily film copies. Many people and organizations might be involved in the distribution of a film. In this process, there could be possibilities of leakage of certain copies. Placing a watermark in every copy, which contains the information of the recipient, can prevent this. This doesn't affect the actual version of the copy, and it is possible to identify the person or source responsible for leakage, if any.

Secret Communication

This was one of the earliest applications of watermarking technique. It is a process of transmitted secret messages in concealed form. Specially designed programs are there to accomplish these tasks.

Copy Control

Many watermarks do not actually prevent the copying of content into which they are embedded, but serve as identification marks of the genuine owner of it. But using certain mechanisms that detect the watermarks and inhibit the copying of the information, it is possible to preserve the integrity of the information.

Properties

Some of the properties of the watermarking techniques are strength, fidelity, cost involved, and the tamper resistance.

Strength

Strength is an important parameter because it decides the capacity of the watermarked signal to withstand the wide range of attacks. Especially, the image and video signals need to tolerate the attacks including the geometric ones. Besides, it should be able to endure ordinary attacks like A to D conversion and lossy conformations. More often than not, a watermarked signal is expected to endure common processing transformations only during the time interval between the insertion and decoding of the signal. The toughness of the signal is not limited to any one constraint, but it can be extended to many others. It means, a signal, which is capable of withstanding an attack, may not be able to tolerate another. Consequently, the signal is made to withstand attacks, which may differ from one application to another. Where there is only a necessity to know whether any distortion of signal has occurred and nothing else, the strength is not at all a constraint. Instead, the watermark may be a fragile one. The situation may be quite different in some other cases. One such case is where the attacks

are quite capricious. Herein, the signal is watermarked in such a fashion it can withstand every possible distortion.

Tamper Resistance

If there is a possibility of aggressive or antagonistic attacks, then the watermarked signal must be tamper resistant. Tamper resistance is immaterial if there are slim chances of aggressive attacks. The watermarked signal must be tamper resistant to attacks like passive, active, and falsification attacks. In passive form of attacks, the attacker just likes to determine whether a watermark is present in the signal or not. In contrast to this, an active attack is one in which the attacker tries to remove the watermark from the watermarked signal. There is yet another form of active attack, called collusion attack wherein, the attacker tries to reconstruct the replica with no watermark from different sets of copies with different watermarks. In falsification attacks, the attacker inserts another watermark into the genuine one, thereby, changing the identification of the copy.

Reliability

A watermarked signal may be considered to be highly reliable, if the distortion caused by the inclusion of watermark is quite unnoticeable by the human eye.

Cost involved:

Depending upon the application, the number of watermark embedders and watermark detectors vary. Their working speeds vary as well according to the type of application. The cost involved thus varies greatly depending up on all these constraints.

Conclusion

Digital watermarking is an outstanding technology that can serve a wide range of applications in various media types. Thus we studied about digital watermarking and it's other types like Images, Video, Audio and Text watermarking. Visible watermarks on images can be easily achieved through image editing software. A very simple definition of video watermarking would be, "The process of watermarking the sequence of video frames". Digital watermarking is technology which allows a secret message to be hidden in computer file, without the detection of the user.

References

- [1] Langelaar G., Setyawan I. and Lagendijk R. (2000) *IEEE Signal Processing Magazine*,17, 20-46.
- [2] Rey C. and Dugelay J.L. A survey of watermarking algorithms for image authentication.
- [3] Hern'andez J.R., P'erez-Gonz'alez F., Rodr'guez J.M. and Nieto G. (1988) *IEEE J. Select. Areas Commun.*, 16, 510-524.
- [4] Macq B. and Quisquater J. (1995) Proceeding of the IEEE, 83, 944-956.
- [5] EURASIP, Journal on Applied Signal.

Bioinfo Publications 11