ISSN (Online): 2230-7893
www.IJCEM.org

Digital Watermarking for Protection of Intellectual Property

Prachi Khanzode, Siddharth Ladhake[2] and Shreya Tank[3]

[1] Department of Computer Science and IT,Sipna COET
Amravati,Maharashtra,444601,India
prachi_khanzode@yahoo.co.in

[2] Department of Electonics and telecommunications,Sipna COET
Amravati,Maharashtra,India

[3] Department of Computer Science and IT,Sipna COET
Amravati,Maharashtra,444601,India
tank_shreya@yahoo.co.in

Abstract

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove and protect the copyright of media signals. This paper aims to provide a universal review and background about the watermarking definition, purpose, techniques and types of concept and the main contributions in this field. It starts with a general view of digital data, the Internet and the products of these two, namely, the multimedia and the e-commerce. Then, it provides with some initial background and history of digital watermarking. This paper presents an extensive and deep literature review of the field of digital watermarking and watermarking algorithms. It also highlights the future prospective of the digital watermarking

Keywords: *Mediasignals;multimedia ;watermarking algorithms*

1. Introduction

The desire for the availability of information and quick distribution has been a major factor in the development of new technology in the last decade .There is the increased use of multimedia across the Internet. Multimedia distribution has become an important way to deliver services to people around the world. It is commonly applied in Internet marketing campaigns and electronic commerce web sites. Due to the growing usage of multimedia content on the Internet, serious issues have emerged. Counterfeiting, forgery, fraud, and pirating of this content are rising. Virtually anyone with a sound card, scanner, video frame grabbers, or Multimedia authoring systems allow them to incorporate copyrighted material into presentations, web designs, and Internet marketing campaigns.

Consequently, copyright abuse is rampant among multimedia users, who are rarely caught This copyright abuse is the motivating factor in developing new encryption technologies .One such technology is digital watermarking. Digital watermarking techniques have been developed to protect the copyright of media signals. Different watermarking schemes have been suggested for multimedia content such as images, video and audio signal. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

2. DIGITAL INTELLECTUAL PROPERTY

Information is becoming widely available via global networks. These connected networks allow cross-references between databases. The advent of multimedia is allowing different applications to mix sound, images, and video and to interact with large amounts of information. The industry is investing to deliver audio, image and video data in electronic form to customers, and broadcast television companies, major corporations and photo archivers are converting their content from analogue to digital form. This movement from traditional content, such as paper documents, analogue recordings, to digital media is due to several advantages of digital media over the traditional media. Some of these advantages are:

1. The quality of digital signals is higher than that of their corresponding analogue signals. Traditional assets degrade in quality as time passes. Analogue data require expensive systems to obtain high quality copies, whereas digital data can be easily copied without loss of fidelity.
2. Digital data can be easily transmitted over networks, for example the Internet. A large amount of multimedia data is now available to users all over the world. This expansion will continue at an even greater rate with the widening availability of advanced multimedia services like electronic commerce, advertising, interactive TV, digital libraries, and a lot more.
3. Exact copies of digital data can be easily made. This is very useful but it also creates problems for the owner of valuable digital data like precious digital images. Replicas of a given piece of digital data cannot be distinguished and

their origin cannot be confirmed. It is impossible to determine which piece is the original and which is the copy. 4. It is possible to hide some information within digital data in such a way that data modifications are undetectable for the human senses.[1]

3. Copyright Protection of Intellectual Property

An important factor that slows down the growth of multimedia networked services is that authors, publishers and providers of multimedia data are reluctant to allow the distribution of their documents in a networked environment. This is because the ease of reproducing digital data in their exact original form is likely to encourage copyright violation, data misappropriation and abuse. These are the problems of theft and distribution of intellectual property. Therefore, creators and distributors of digital data are actively seeking reliable solutions to the problems associated with copyright protection of multimedia data.

Moreover, the future development of networked multimedia systems, in particular on open networks like the Internet, is conditioned by the development of efficient methods to protect data owners against unauthorized copying and redistribution of the material put on the network. This will guarantee that their rights are protected and their assets properly managed. Copyright protection of multimedia data has been accomplished by means of cryptography algorithms to provide control over data access and to make data unreadable to non-authorized users. However, encryption systems do not completely solve the problem, because once encryption is removed there is no more control on the dissemination of data.

The concept of digital watermarking arose while trying to solve problems related to the copyright of intellectual property in digital media. It is used as a means to identify the owner or distributor of digital data. Watermarking is the process of encoding hidden copyright information since it is possible today to hide information messages within digital audio, video, images and texts, by taking into account the limitations of the human audio and visual systems.

4. DIGITAL WATERMARKING CONCEPT

This section aims to provide the theoretical background about the watermarking field but concentrating mainly on digital images and the principles by which watermarks are implemented. It discusses the requirements that are needed for an effective watermarking system. It shows that the requirements are application-dependent, but some of them are common to most practical applications. It explains also the challenges facing the researchers in this field from the digital watermarking requirement viewpoint.

Visible vs. Invisible Watermarks

Digital watermarking is divided into two main categories: visible and invisible. In visible digital watermarking, the information is visible in the picture or video. It is equivalent to stamping a watermark on paper, and for this reason is sometimes said to be digitally stamped.Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such. The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. . Though a lot of research has been done in the area of invisible watermarks, much less has been done for visible watermarks. Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Visible watermarks are especially useful for conveying an immediate claim of ownership. Their main advantage, in principle at least, is the virtual elimination of the commercial value of a document to would-be thief, without lessening the document's utility for legitimate, authorized purposes. Invisible watermarks, on the other hand, are more of an aid in catching a thief than for discouraging theft in the first place (Mintzer et al., 1997; Swanson et al., 1998).

4.1. DIGITAL WATERMARKING: What, Why, When and How?

It seems that digital watermarking is a good way to protect intellectual property from illegal copying. It provides a means of embedding a message in a piece of digital data without destroying its value. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music. This chapter focuses on digital watermarking for images and in particular invisible watermarking.

What is Digital Watermarking?

A digital watermark is a signal permanently embedded into digital data(audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked. Digital watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or "covered" and graphos

or "to write"). Steganography is the science of communicating information while hiding the existence of the communication. The goal of steganography is to hide an information message inside harmless messages in such a way that it is not possible even to detect that there is a secret message present. Both steganography and watermarking belong to a category of information hiding, but the objectives and conditions for the two techniques are just the opposite. In watermarking, for example, the important information is the "external" data (e.g., images, voices, etc.). The "internal" data (e.g., watermark) are additional data for protecting the external data and to prove ownership. In steganography, however, the external data (referred to as a vessel, container, or dummy data) are not very important. They are just a carrier of the important information. The internal data are the most important. On the other hand, watermarking is not like encryption. Watermarking does not restrict access to the data while encryption has the aim of making messages unintelligible to any unauthorized persons who might intercept them. Once encrypted data is decrypted, the media is no longer protected. A watermark is designed to permanently reside in the host data. If the ownership of a digital work is in question, the information can be extracted to completely characterize the owner.

Why Digital Watermarking?

Digital watermarking is an enabling technology for e-commerce strategies: conditional and user-specific access to services and resources. Digital watermarking offers several advantages. The details of a good digital watermarking algorithm can be made public knowledge. Digital watermarking provides the owner of a piece of digital data the means to mark the data invisibly. The mark could be used to serialize a piece of data as it is sold or used as a method to mark a valuable image. For example, this marking allows an owner to safely post an image for viewing but legally provides an embedded copyright to prohibit others from posting the same image. Watermarks and attacks on watermarks are two sides of the same coin. The goal of both is to preserve the value of the digital data. However, the goal of a watermark is to be robust enough to resist attack but not at the expense of altering the value of the data being protected. On the other hand, the goal of the attack is to remove the watermark without destroying the value of the protected data. The contents of the image can be marked without visible loss of value or dependence on specific formats. For example a bitmap (BMP) image can be compressed to a JPEG image. The result is an image that requires less storage space but cannot be distinguished from the original. Generally, a JPEG compression level of 70% can be applied without humanly visible degradation. This property of digital images allows insertion of additional data in the image without altering the value of the image. The message is hidden in unused "visual space" in the image and stays below the human visible threshold for the image.

When Did the Technique Originate?

The idea of hiding data in another media is very old, as described in the case of steganography. Nevertheless, the term digital watermarking first appeared in 1993, when Tirkel et al. (1993) presented two techniques to hide data in images. These methods were based on modifications to the least significant bit(LSB) of the pixel values.[2]

How Can We Build an Effective Watermarking Algorithm?

The following sections will discuss further answering this question. However, it is desired that watermarks survive image-processing manipulations such as rotation, scaling, image compression and image enhancement, for example.

Taking advantage of the discrete wavelet transform properties and robust features extraction techniques are the new trends that are used in the recent digital image watermarking methods. Robustness against geometrical transformation is essential since image-publishing applications often apply some kind of geometrical transformations to the image, and thus, an intellectual property ownership protection system should not be affected by these changes.

4.2. DIGITAL WATERMARKING LIFE CYCLE PHASES

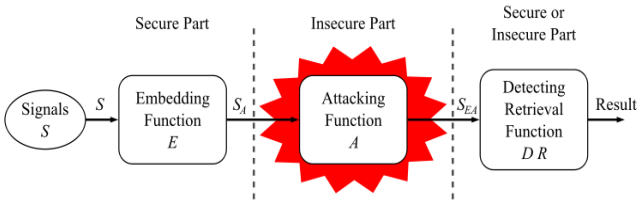

Fig 1. General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions.

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for

example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

4.3 ROBUST WATERMARKING SCHEME REQUIREMENT

In this section, the requirements needed for an effective watermarking system are introduced. The requirements are application-dependent, but some of them are common to most practical applications. One of the challenges for researchers in this field is that these requirements compete with each other. Such general requirements are listed below.

Security

Effectiveness of a watermark algorithm cannot be based on the assumption that possible attackers do not know the embedding process that the watermark Digital Watermarking for Protection of Intellectual Property 15 went through (Swanson et al., 1998). The robustness of some commercial products is based on such an assumption. The point is that by making the technique very robust and making the embedding algorithm public, this actually reduces the computational complexity for the attacker to remove the watermark. Some of the techniques use the original non-marked image in the extraction process. They use a secret key to generate the watermark for security purpose.

Invisibility

Perceptual Invisibility. Researchers have tried to hide the watermark in such a way that the watermark is impossible to notice. However, this requirement conflicts with other requirements such as robustness, which is an important requirement when facing watermarking attacks. For this purpose, the characteristics of the human visual system (HVS) for images and the human auditory system (HAS) for audio signal are exploited in the watermark embedding process.

Statistical Invisibility. An unauthorized person should not detect the watermark by means of statistical methods. For example, the availability of a great number of digital works watermarked with the same code should not allow the extraction of the embedded mark by applying statistically based attacks. A possible solution is to use a content dependent watermark (Voyatzis et al., 1998).[3]

Robustness

Digital images commonly are subject to many types of distortions, such as lossy compression, filtering, resizing, contrast enhancement, cropping, rotation and so on. The mark should be detectable even after such distortions have occurred. Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the image signal (Ruanaidh et al., 1996). For example, a watermark hidden among perceptually insignificant data is likely not to survive lossy compression. Moreover, resistance to geometric manipulations, such as translation, resizing, rotation and cropping is still an open issue. These geometric manipulations are still very common.

Watermarking Extraction: False Negative/Positive Error Probability

Even in the absence of attacks or signal distortions, false negative error probability (the probability of failing to detect the embedded watermark) and of detecting a watermark when, in fact, one does not exist (false positive error probability), must be very small. Usually, statistically based algorithms have no problem in satisfying this requirement.

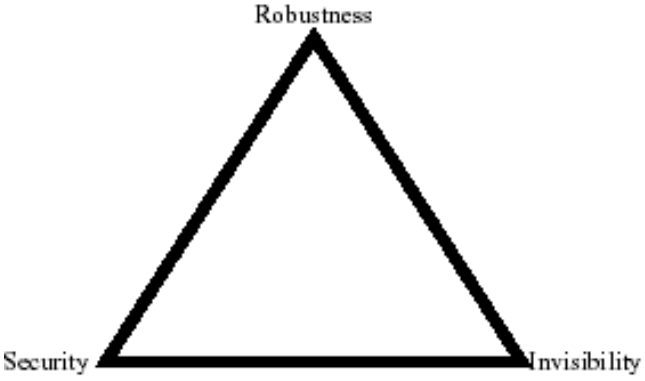

Figure 2. Digital watermarking requirements triangle

Capacity Issue (Bit Rate)

The watermarking algorithm should embed a predefined number of bits to be hidden in the host signal. This number will depend on the application at hand. There is no general rule for this. However, in the image case, the possibility of embedding into the image at least 300-400 bits should be guaranteed. In general, the number of bits that can be hidden in data is limited. Capacity issues were discussed by Servetto et al. (1998).

Comments

One can understand the challenge to researchers in this field since the above requirements compete with each other. The important test of a watermarking method would be that it is accepted and used on a large, commercial scale, and that it stands up in a court of law. None of the digital techniques have yet to meet all of these requirements. In fact the first three requirements (security, robustness and invisibility) can form sort of a triangle (Figure 2), which means that if one is improved, the other two might be affected.

5. DIGIAL WATERMARKING ALGORITHM

Current watermarking techniques described in the literature can be grouped into three main classes. The first

includes the transform domain methods, which embed the data by modulating the transform domain signal coefficients. The second class includes the spatial domain techniques. These embed the watermark by directly modifying the pixel values of the original image. The transform domain techniques have been found to have the greater robustness, when the watermarked signals are tested after having been subjected to common signal distortions. The third class is the feature domain technique. This technique takes into account region, boundary and object characteristics. Such watermarking methods may present additional advantages in terms of detection and recovery from geometric attacks, compared to previous approaches.

In this the algorithms in this survey are organized according to their embedding domain, as indicated in Figure 1. These are grouped into:

1. spatial domain techniques
2. transform domain techniques
3. feature domain techniques

6.DIGITAL WATERMARKING APPLICATION

Watermarking has been proposed in the literature as a means for different applications. The four main digital watermarking applications are:

1. Copyright protection
2. Image authentication
3. Data hiding
4. Covert communication

7. FUTURE HIGHLIGHTS

Nevertheless, the future seems bright for digital watermarking. Many companies have already been active in digital watermarking research. For example, Microsoft has developed a prototype system that limits unauthorized playback of music by embedding a watermark that remains permanently attached to audio files. Such technology could be included as a default playback mechanism in future versions of the Windows operating system. If the music industry begins to include watermarks in its song files, Windows would refuse to play copyrighted music released after a certain date that was obtained illegally. Also, Microsoft Research has also invented a separate watermarking system that relies on graph theory to hide watermarks in software. Normally the security technology is hackable. However, if the technology is combined with proper legal enforcement, industry standards and respects of the privacy of individuals seeking to legitimately use intellectual property, digital watermarking will encourage content creators to trust the Internet more. There is a tremendous amount of money at stake for many firms. The value of illegal copies of multimedia content distributed over the Internet could reach billions of dollars a year. It will be interesting to see how the development and adoption of digital watermarking plays out. With such high stakes involved for entertainment and other multimedia companies, they are likely to keep pushing for (and be willing to pay for) a secure technology that they can use to track and reduce copyright violation and capture some of their foregone revenues. Finally, it is expected that a great deal of effort must still be put into research before digital image watermarking can be widely accepted as legal evidence of ownership.

REFERENCES

[1]Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1997). Robust watermarking of still images for copyright protection. 13th International Conference on Digital Signal Processing Proceedings, DSP 97, (vol. 1, pp. 499-502).

[2]Bas, P., Chassery, J., & Davoine, F. (1998, October). Using the fractal code to watermark images. International Conference on Image Processing Proceedings, ICIP 98, (vol. 1, pp. 469-473).

[3]Baudry, S., Nguyen, P., & Maitre, H. (2000, October). Channel coding in video watermarking: Use of soft decoding to improve the watermark retrieval.

[4]International Conference on Image Processing Proceedings, ICIP 2000, (vol. 3, pp. 25-28).

[5]Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996).