A

Seminar report

on

“Digital Watermarking”

Submitted in partial fulfillment of the requirement for the award of degree
of Bachelor of Technology in Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Preface

I have made this report file on the topic **Digital Watermarking,** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Contents

Abstract

The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form.

Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants.

It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms.

One such effort that has been attracting increasing interest is based on *digital watermarking* techniques.

Introduction

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video.

The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible.

A digital watermark is a message which is embedded into digital content (video, images or text) that can be detected or extracted later.

Moreover, in image the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. Watermarking is the insertion of imperceptible and inseparable information into the host data for data security & integrity.

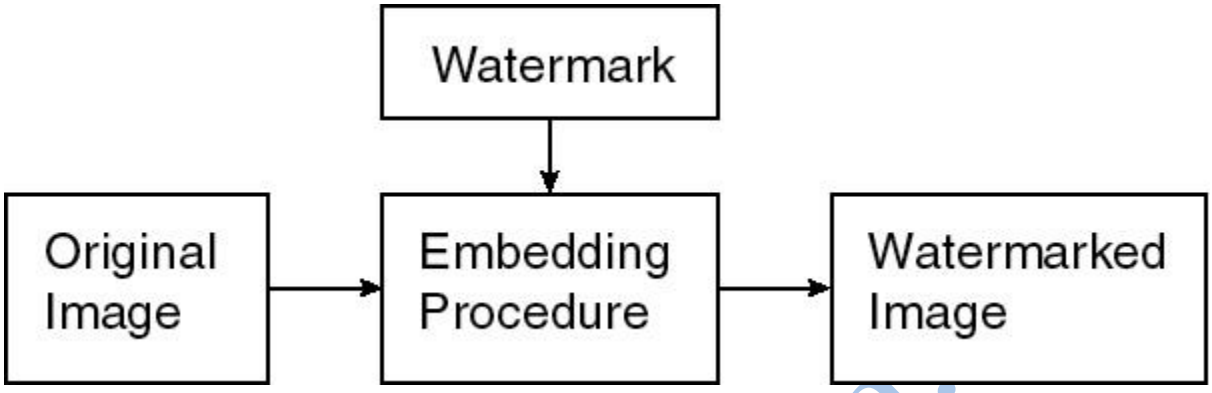
They are characterizing patterns, of varying visibility, added to the presentation media as a guarantee of authenticity, quality, ownership, and source.

However, in digital watermarking, the message is supposed **not** to visible (or at least not interfering with the user experience of the content), but (only) electronic devices can retrieve the embedded message to identify the code.

Another form of digital watermarking is known as steganography, in which a message is hidden in the content without typical citizens or the public authorities noticing its presence.

Only a limited number of recipients can retrieve and decode the hidden message. Unlike a traditional watermark 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.

Figure shows the general watermarking embedding procedure. In an original image with the help of embedding procedure watermark is embedded and then we get a watermarked image.



The most common example of watermark is an Indian currency.

History

More than 700 years ago, watermarks were used in Italy to indicate the paper brand and the mill that produced it. By the 18th century watermarks began to be used as Anticounterfeiting measures on money and other documents.

The term watermark was introduced near the end of the 18th century. It was probably given because the marks resemble the effects of water on paper.

The first example of a technology similar to digital watermarking is a patent filed in 1954 by Emil Hem Brooke for identifying music works .In 1988, Komatsu and Tominaga appear to be the first to use the term “digital watermarking”.

Types of watermark

Digital watermarks are of four types:

- Visible
- Invisible
- Public, and
- Fragile

A **visible watermark** typically consists of a conspicuously visible message or a company logo indicating the ownership of the image. Any removal or tampering with the logo would break the copyright agreement. Another way is to write the copyright notice and other information into an extra couple of lines within the image file. The extra lines can be removed from the image, without detriment to the image quality and content, but this again would break the copyright agreement of the image.

A visible watermark was added to the image to create this image.

The watermark is a repeating image of a bird in flight. Visible watermarks often look as if they were "embossed" onto the original image, as illustrated here.

An **invisible watermarked** image appears very similar to the original. The existence of an invisible watermark can only be determined using an appropriate watermark extraction or detection algorithm. It can be detected by an authorized agency only. Such watermarks are used for content and/or author authentication and for detecting unauthorized copier.

To insert the invisible watermark, we first supplied a special password, or a "key," for security. The key may be used to recover the message contained in the invisible watermark, *and* to determine whether the image was altered since the invisible watermark was inserted.

Public watermark such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure.

Fragile watermarks are also known as tamperproof watermarks. Such watermarks are destroyed by data manipulation. Fragile watermark is a mark which is (highly) sensitive to a modification .A fragile watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification. It serves at proving the authenticity of a document.

Different attributes associated with watermarking

The characteristics of a watermarking algorithm is normally tied to the application is designed for. The most important properties of any digital watermarking techniques are robustness, security, imperceptibility, complexity, and verification. The following merely explain the words used in the context of watermarking.

Imperceptibility:-In watermarking, we traditionally seek high fidelity, i.e. the watermarked work must look or sounds like the original. Whether or not this is a good goal is a different discussion. Imperceptibility means the watermark is not seen by the human visual system.

Robustness:- By "robust" we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, just to enumerate some. Robustness is defined as if the watermark can be detected after media (normal) operations such as filtering, lossy compression, color correction, or geometric modifications. In some cases the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.
It is more a property and not a requirement of watermarking. The watermark should be able to survive any reasonable processing inflicted on the carrier (carrier here refers to the content being watermarked).

Security:-The watermarked image should not reveal any clues of the presence of the watermark, with respect to un-authorized detection, or (statistical) indefectibility or unsuspicious (not the same as imperceptibility). Security means the embedded watermark cannot be removed beyond reliable detection by targeted attacks.

Complexity is described as the effort and time required for watermark embedding and retrieval**.**

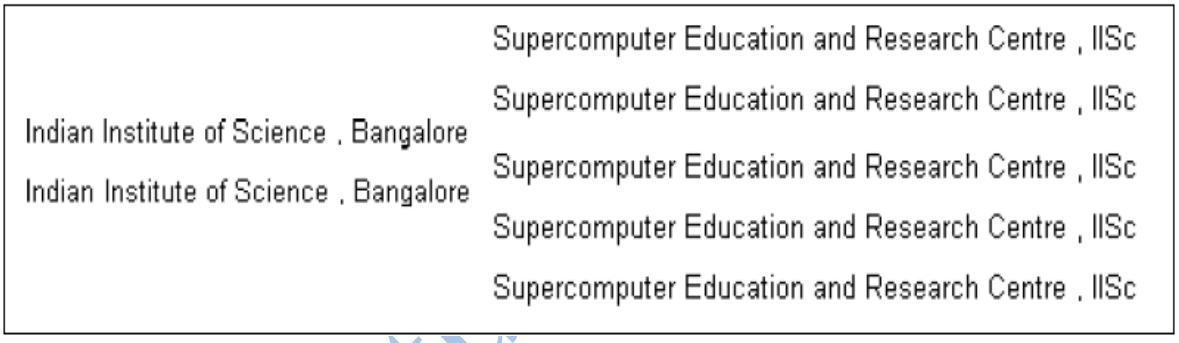
Verification is a procedure where by there is a private key or public key function

Watermarking Techniques

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.

***Watermarking for text*:** Two methods have been proposed for watermarking text, namely –

Word space coding: In this method, the spacing between words is varied by horizontally shifting the locations of the words within text lines, thus watermarking the document uniquely. This however is applicable only to documents in which variable spacing between adjacent words is possible. Also because interword spacing is often varied to format the document, the original document is necessary to verify the watermark. An example of word space coding is given below.

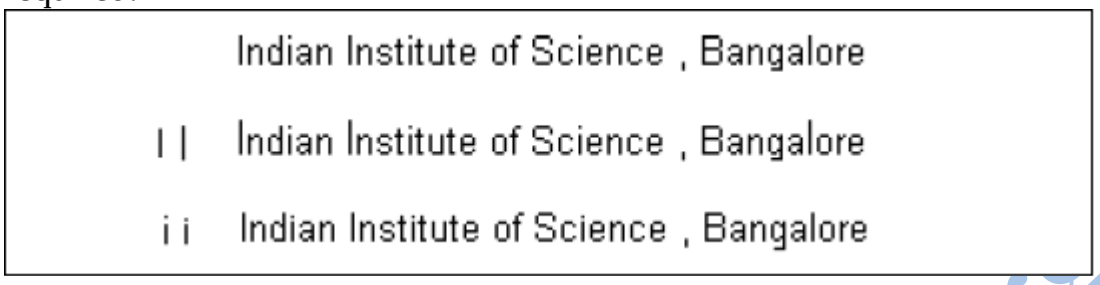


This figure illustrates word shift encoding. Note the additional space of one pixel between ‘n’ of ‘Indian’ and ‘I’ of ‘Institute’. Such minor variations are not perceptible to the human eye. They are recognized only on close comparison**.**

***Line shift coding*:** The same concept of word space coding is used, only it is applied in the vertical domain. Text lines are shifted vertically to watermark the image uniquely. If the original image has uniform line spacing, then verification of the watermark can be accomplished without the original. An example of line shift coding is shown in above figure. This illustrates the technique of line shift encoding (see lines 2 and 3). Notice that line shift encoding is more evident than word shift encoding because of the length of the lines.

Feature coding: This method alters the specifications of particular characters by either lengthening or shortening them. It provides numerous

possibilities of watermarking. However, for decoding, the original image is necessary, or rather, the original characteristics of the characters are required.



In the second line the length of the letter 'I' has been imperceptibly increased; it is evident only on close comparison. In the third line the distance between the dot and the line in the character 'i' has been reduced. Such features are not noticeable until and unless specifically looked for.

ii) ***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 and 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.

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. Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. 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.

Frequency Domain watermarking: Frequency domain watermarking technique is also called transform domain. 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. The watermark is applied to the whole image so as not to be removed during a cropping operation. However, it is more difficult to decode a watermark applied in the frequency domain. Verification can be difficult since this watermark is applied indiscriminately across the whole image.

Detection of Watermarks

It needs to be emphasized that a watermark can be defeated in two ways – one, by removing the watermark from the original data and two, by proving it to be unreliable i.e. identifying a watermark when there is none. If the latter can be achieved then the watermark cannot be proved in a legal battle. Hence detection of watermarks needs to be even more reliable than their embedding. Detection algorithms are dependent on or are derived from embedding algorithms. Hence, a rigorous and detailed classification is ruled out.

Detection algorithms can be divided into two broad categories –those which need the original unwatermarked data, and those which do not. The former generally makes a byte-by-byte Comparison and arrives at a decision after allowing for a reasonable amount of error. Say, for example, the image has been watermarked by increasing the intensity of certain pixels in the Original unwatermarked image by a known factor K, the average intensity of these pixels in the original image and the test image are compared. If they differ by more than 0.7K, the image is watermarked while if they differ by less than 0.3K, the image is not watermarked. The in-between range of 0.3K to 0.7K is a gray area and needs a more detailed analysis of the conditions undergone by the image. It should be said that the figures of 0.3K and 0.7K are an offhand estimate. They need to be arrived at after mathematical estimations.

Applications of watermarking

The first applications that came to mind were related to copyright protection of digital media. In the past duplicating art work was quite complicated and required a high level of expertise for the counterfeit to look like the original.

However, in the digital world this is not true. Now it is possible for almost anyone to duplicate or manipulate digital data and not lose data quality. Similar to the process when artists creatively signed their paintings with a brush to claim copyrights, artists of today can watermark their work by hiding their name within the image.

Hence, the embedded watermark permits identification of the owner of the work.There are a number of possible applications for digital watermarking technologies and this number is increasing rapidly.

Security: In the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports.

Example on the left of a protected identity card. The identity number "123456789" is written in clear text on the card and hidden as a digital watermark in the identity photo. Therefore switching or manipulating the identity photo will be detected.

Digital watermarking permits linking information on documents. That means that key information is written twice on the document. For instance, the name of a passport owner is normally printed in clear text. But it would also

be hidden as an invisible watermark in the passport photo. If anyone tries to tamper with the passport by replacing the photo it would be possible to detect the change by scanning the passport and verifying the name hidden in the photo.

Tampering with images: Another application is the authentication of image content. The goal of this application is to detect any alterations and modifications in an image.

The three pictures below illustrate this application. The picture on the left shows an original photo of a car that has been protected with a watermarking technology. In the center, the same picture is shown but with a small modification: the numbers on the license plate have been changed. The picture on the right shows the photo after running the digital watermark detection program on the tampered photo. The tampered areas are indicated in white. We can clearly see that the detected area corresponds to the modifications applied to the original photo.

(a) (b) (c)

Using digital watermarks for integrity verification: the protected image is the image (a) above; a modified image is obtained by swapping the numbers 9 and 4 of the number plate (b); digital watermarking technology allows detecting and highlights the modified areas, as shown on (c).

Copy prevention or control. Watermarks can also be used for copy prevention and control. For example, in a closed system where the multimedia content needs special hardware for copying and/or viewing, a

digital watermark can be inserted indicating the number of copies that are permitted. Every time a copy is made the watermark can be modified by the hardware and after a point the hardware would not create further copies of the data. An example of such a system is the Digital Versatile Disc (DVD).

Advantages

- Digital Watermarking allows embedding of arbitrary information (the watermark) into digital media (such as video or images) by applying imperceptible, systematic alterations to the media data.
- Higher level of security**:** Security and confidentiality of the embedded information is provided by a secret key. Without this key the watermark cannot be accessed or modified. Watermarks can be designed in such a way that the embedded information is still retrievable even after the carrier medium changed.
- The advantage of digital watermarking is that the product of the embedding process is still a digital medium. Customers can do everything with a marked medium that they can do with an unmarked one. Watermarked media can be played or copied without any restrictions
- Digital Watermarking is non-restrictive – only misuse is detectable and traceable.

Disadvantages

Digital watermarking is a recent research field; therefore its intrinsic limits are not well understood yet.

On the other hand, more insight into the technical possibility of satisfying the requirements imposed by practical applications is needed, if the practical possibility of using watermarking for copyright protection is to be evaluated. In the following, some of the most common limits shared by digital watermarking schemes are described.

- Visible watermark can be easily removed.

- A watermarking algorithm which is really robust does not exist yet. In the image case, robustness is still an open issue. More specifically, resistance to geometric manipulations such as cropping is recognized as a very difficult goal to achieve in a computationally efficient way.

- Owners can erase the mark: virtually all the watermarking schemes proposed so far are reversible according to the definition previously given.

  In other words, by knowing the exact content of the watermark, and the algorithms used to embed and retrieve it, it is always possible to make it unreadable without any significant degradation of the data.

Conclusion

The study of the watermark technology has become active since mid-1990s, and some technologies are already adopted in practical applications as a product or as proprietary services for enterprises.

Although this is a relatively new technology area, it quickly becomes a practical and effective solution in some application areas, and has great potential for some other areas as well.

The key to the successful implementation is to understand the advantages and the limitations of the watermark technology, and to use the watermark technology as a complimentary element to the existing security elements.

References

www.ieeexplore.ieee.org
www.watermarkingworld.com
www.wikipedia.com

Editorial Steganography and digital watermarking
Information Security, IEE Proceedings
Volume 153, Issue 3, Date: Sept. 2006