Global Journal of Computer Science and Technology
Graphics & Vision
Volume 12 Issue 13 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Digital Watermarking

By Nidhi Rani
Dronacharya College of Engineering

Abstract - Today's world is digital world. Nowadays, in every field there is enormous use of digital contents. Information handled on INTERNET and MULTIMEDIA NETWORK SYSTEM is in digital form. The copying of digital content without quality loss is not so difficult .Due to this , there are more chances of copying of such digital information. So , there is great need of prohibiting such illegal copyright of digital media. Digital watermarking (DWM) is the powerful solution to this problem. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc. Digital watermarks are of different types as robust, fragile, visible and invisible. Application is depending upon these watermarks classifications. There are some requirements of digital watermarks as integrity, robustness and complexity.

GJCST-F Classification : I.4.0

Strictly as per the compliance and regulations of:

Digital Watermarking

Nidhi Rani

Abstract - Today's world is digital world. Nowadays, in every field there is enormous use of digital contents. Information handled on INTERNET and MULTIMEDIA NETWORK SYSTEM is in digital form. The copying of digital content without quality loss is not so difficult .Due to this , there are more chances of copying of such digital information. So , there is great need of prohibiting such illegal copyright of digital media. Digital watermarking (DWM) is the powerful solution to this problem. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc. Digital watermarks are of different types as robust, fragile, visible and invisible. Application is depending upon these watermarks classifications. There are some requirements of digital watermarks as integrity, robustness and complexity.

I. Introduction

The process of embedding information into another object/signal is termed as digital watermarking. In visible watermarking, the information is visible in the picture or video. 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 is also a visible watermark. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden). The watermark may be intended for widespread use and is thus made easy to retrieve or it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It is also possible to use hidden embedded information as a means of covert communication between individual. The purpose of embedding the information depends upon application and need of user of digital media. Digital watermarking provides the solution for difficult problem of providing guarantee to organizer and consumer of digital content about their legal rights .Copyright protection for multimedia information is nothing but a golden key for multimedia industry. Digital watermarking is a technology that opens a new door for authors, producers, publishers and service providers for protection of their rights and interest in multimedia documents. In general sense, Digital Watermarking means "Author Signature".

Digital watermarking is the process of encoding hidden Copyright information in an image by making small modifications in it's pixel content. In this case watermarking doesn't restrict the accessing image information. The important function of watermarking is to remain present in data for proof of ownership. The use of digital watermarking is not restricted upto copyright.

II. Digital Watermarking

Digital Watermarking is hidden information inside signal. For watermarking several techniques has been developed. These can be categorized as:

- Spatial Domain Watermarking
- Frequency Domain Watermarking.

Spatial Domain

- Spatial domain watermarking uses blockxblock watermarking.
- e.g they embed the watermarks on a randomly selected 8x8 blocks of pixels of the image.

Frequency Domain

To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible image transformations include discrete Fourier Transform.

III. Properties and Classification

a) *Properties*

For better activeness, watermark should be perceptually invisible within host media, statistically invisible to unauthorized removal, readily extracted by owner of image, robust to accidental and intended signal distortion like filtering compression, resampling, retouching, crapping etc. For a digital watermark to be effective for ownership, it must be robust, recoverable from a document, should provide the original information embedded reliably and also removed by authorized users.

All these important properties of digital watermarks are described as:

i. *Robustness*

The watermark should be robust such that it must be difficult to remove. The watermark should be robust to different attacks. The robustness describes

Author : Computer Science Dronacharya College of Engineering.
E-mail : goyal_nidhi1123@yahoo.com

whether watermark can be reliably detected after performing some media operations.

ii. *Perceptual transparency*

This property describes that whether watermark is visible or invisible to human sensor organ. Perceptible watermarks are visible to human while imperceptible are not. Imperceptible watermarks are such that content remains same after applying digital watermarking technique.

iii. *Security*

Security property describes that how easy to remove a watermark. This is generally referred to as "attack" on watermarking. Attack refers to detection or modification of watermark.

iv. *Complexity*

This is important property which is to be considering in Real time applications like video. Complexity property is concerned with amount of effort needed to extract or retrieve the watermark from content.

v. *Capacity*

Capacity property of digital watermarks refers to amount of information that can be embedded within the content. The important point is that more data is used in watermark, watermark will become less robust. In addition to these properties, watermarks are having some extra properties as unambiguity, tamper resistance, inseparable from the works and able to undergo some transformation as works.

b) Classification

Digital watermarks are classified according to their applications. The watermarks are classified as perceptible watermarks and imperceptible watermarks, robust and fragile, public and private. This classification of watermarks is broadly described in following sections.

i. *Perceptible watermarks and imperceptible watermarks*

Perceptible watermarks are visible to human eye while imperceptible watermarks are invisible. The perceptible watermarks are useful for primary application i.e. for statement ownership or authorship. So for this reason it should be visible. .On the other hand imperceptible watermarks are useful for complex applications such as document identification in which content being watermarked must appear in unchanged form. Examples of visible (perceptible) watermarks are logos on TV, IBM's watermark and that of invisible (imperceptible) watermarks are ATT, NEC/MIT, UU etc.

Perceptible watermarks i.e. visible one are extension of the concept of logos. They are applicable to images only. These watermarks are embedded into image. They are applicable in maps, graphics and software user interface .Imperceptible watermarks i.e. invisible one remains hidden in the content. They can be detected only by authorized agency. These watermarks are useful for content or author authentication and for detecting unauthorized copier.

ii. *Robust watermarks and fragile watermarks*

Robust or fragile is nothing but degree to which watermarks can withstand any modifications of any types caused due to the transmission or lossy compression. Perceptible watermarks are more robust in nature than imperceptible one. But meaning of this is not that imperceptible watermarks are fragile one. Robust watermarks are those watermarks which are difficult to remove from the object in which they are embedded. Fragile watermarks are those watermarks which can be easily destroyed by any attempt to tamper with them. Fragile watermarks are destroyed by data manipulation.

iii. *Private watermarks and public watermarks*

Private watermarks requires at least original data to recover watermark information Public watermarks requires neither original data nor embedded watermarks to recover watermark information. Private watermarks are also known as secure watermarks. To read or retrieve private watermark, it is necessary to have secret key. Public watermark can be read or retrieve by anyone using specialized algorithm. In this sense public watermarks are not secure. Public watermarks are useful for carrying IPR information. They are good alternatives to labels.

IV. Relative Concepts and Attacks

a) Relevant Terms

Digital watermarking, steganography, information hiding, cryptography are closely related concepts. In each technique, a digital signal or pattern is inserted into, onto, before or after digital document. There are some difference between working principle of these techniques and their meanings. Information hiding is also called as 'Data hiding'. The hiding is concerned with making information imperceptible or keeping it's existence secrete. Information hiding means encompassing wide range of problems beyond that of embedding messages in content. Information hiding deals with communication security. It consists of encryption and traffic security. Encryption protects the content during distribution over an open network such as internet. The traffic security is related to concealing its sender, its receiver. Thus, here an attempt is made to have secreted communication between each two parties where existence is unknown to attacker.

i. *Steganography*

It is nothing but sub-discipline of information hiding. Here secrete information is hidden in harmless message, which is also known as cover message. Steganography is used to avoid drawing suspictions to transmission of hidden message so as to

remain undetected. The idea behind this is that to hide message in envelope or wrapper. In steganography, existence of hidden message in content is not known audience.

ii. *Cryptography*

This technique is related with data protection. It is commonly used for protecting digital information. Once, data is decrypted, it can't remain protected for long time i.e. there may be more chances of illegal copying of this data .So, there is great need of cryptography technique. Watermarking is special case of cryptography. Cryptography involves some suitable and complicated techniques so that no unauthorized user is allowed to access the data to protect. Authorization of user is checked by certain keys or signature.

iii. *Watermarking*

Watermarking is technology derived from steganography. It is also sub-discipline of information hiding. Watermarking is process of embedding secrete and robust identifier inside audio, video content. The purpose of watermarking is to establish the copyright of content creator. In this sense watermarks are also known as the hidden copyright messages. Watermarking secures the content, thus any attempt to modify the content can be easily detected. The watermarking can trace the path followed by content in distribution chain. This helps in tracing malicious users.

b) Attacks

Due to some reasons, there is need of adding, altering or removing false watermarks. Attacks on watermarks may be accidental or intentional. Accidental attacks may cause due to the standard image processing or due to the compression procedures. Intentional attacks includes cryptanalysis, steganalysis, image processing techniques or other attempts to overwrite or remove existing watermarks. Following are the methods of attacks vary according to robustness and Perceptibility.

i. *Mosaic attack*

Mosaic attack is the method in which pictures are displayed so as to confuse watermark-searching program, known as "Web Crawler". Mosaic is created by subdividing the original image into randomly sized small images and displaying the resulting image on webpage.

ii. *Geometric attack*

Geometric attack is related to geometric properties of data. It is concerned with images, documents and audio files. This attack is further classified as-

a. Subtractive attack

It involves the attacker in the area of located watermark if imperceptible and then removing the mark by cropping or digital editing.

b. Distortive attack

In this attack, attacker attempts to make some uniform distortive changes in the images such that mark becomes unrecognizable. These two watermark attacks are usually performed on robust watermark.

iii. *Stirmark attack*

Stirmark is generic tool developed for simple robustness techniques of image marking algorithms and steganographic techniques. In it's simplest version, stirmark simulates resampling process in which it introduces same kind of errors into an image to print it on high quality printer and scanning it again with high quality scanner. It includes minor geometric distortion. This testing tool is an effective program to remove fairly robust watermarks in images and become a form of attack on its own.

iv. *Forgery attack*

Forgery attack is also known as 'Additive attack' in some cases. Forgery attack includes the attacker who can add his or her own watermark overlaying the original image and marking the content as their own.

v. *Inversion attack*

Inversion watermark render the watermark information ambiguous. The idea behind the inversion attack that attacker who receives watermarked data can claim that data contains his watermark also by declaring part of data as his watermark. The attacker can easily generate the original data by subtracting the claimed watermark.

vi. *Cryptanalysis*

It is mostly associated with cryptography. It is a method in which attacker attempts to find the decryption key for an encrypted pieces of information so that it can be made useful again. Attacker can remove licensing watermark that decrypts the data, attacker would use cryptanalysis to find decryption key so that data can use in decrypted form free from its watermark.

V. Conclusion

The large need of networked multimedia system has created the need of "COPYRIGHT PROTECTION". It is very important to protect intellectual properties of digital media. Internet playing an important role of digital data transfer. Digital watermarking is the great solution of the problem of how to protect copyright. Digital watermarking is the solution for the protection of legal rights of digital content owner and customer.

- Modifications of all DCT coefficients distort the image drastically.
- Modification of low – frequency coefficients distorts the image, Gives the hacker a clue about where the watermark is embedded.

References Références Referencias

1. [Adelson87a] Edward H. Adelson, Eero P. Simoncelli, and Rajesh Hingorani. Orthogonal pyramid transforms for image coding
2. Analysis based coding of image transform and subband coefficients. In *Applications of Digital Image Processing XVII, Proceedings of the SPIE,*, volume 2564, pages 11 - 21, 1995.
3. Fast watermarking of DCT-based compressed images. In Hamid R. Arabnia, editor, *Proceedings of the International Conference on Image Science, Systems, and Technology, CISST '97*, Las Vegas, USA, 1997.
4. High quality document image compression with djvu. *Journal of Electronic Imaging*, July 1998.
5. [Bruyndonckx95a] O. Bruyndonckx, Jean-Jacques Quisquater, and Benoit M. Macq.
6. Spatial method for copyright labeling of digital images. In *IEEE Workshop on Nonlinear Signal and Image Processing '95, Thessaloniki, Greece*, pages 456 - 459, 1995.
7. [Buccigrossi97a] Robert W. Buccigrossi and Eero P. Simoncelli.
8. [Corvi97a] Marco Corvi and Gianluca Nicchiotti.
9. Wavelet-based image watermarking for copyright protection. In *Scandinavian Conference on Image Analysis SCIA '97*, Lappeenranta, Finland, June 1997.
10. Image coding using optimized significance tree quantization. In *Proceedings of Data Compression Conference*, pages 387 - 396, 1997.
11. [Dugad98a] Rakesh Dugad, Krishna Ratakonda, and Narendra Ahuja.
12. A new wavelet-based scheme for watermarking images. In *Proceedings of the IEEE International Conference on Image Processing, ICIP '98*, Chicago, IL, USA, October 1998.
13. Methods for data hiding. Technical report, Center for Intelligent Systems, SUNY Binghamton, USA, 1997.
14. Combining low-frequency and spread spectrum watermarking. In *Proceedings of the SPIE Symposium on Optical Science, Engineering and Instrumentation*, San Diego, USA, July 1998.
15. A digital watermark based on the wavelet transform and its robustness on image