Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Priyanka Kale, IJPRET, 2014; Volume 2 (9): 1117-1124 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

INFORMATION HIDING TECHNIQUE: DIGITAL WATERMARKING

PRIYANKA N. KALE[1], PROF. K. M. PIMPLE[2]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: In this era, the network security is most important issue. The secure transmission of confidential data herewith gets a great deal of attention. In this paper, we try to give a more impact on network security because it is responsible for securing all information passed through networked computers. We can secure data by various techniques such as cryptography, steganography, and watermarking techniques. In this paper we will focus on various digital watermarking techniques. Digital watermarking techniques are classified according to transforms in which watermark is embedded.

Keywords: Watermarking, LSB, DCT, DWT, spread spectrum watermarking.

PAPER-QR CODE

Corresponding Author: MS. PRIYANKA N. KALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Priyanka Kale, IJPRET, 2014; Volume 2 (9): 1117-1124

INTRODUCTION

The rapid growth of Internet is increased in recent years. Thus the digital information which includes images, videos, text etc. is readily available to anyone and the need of protecting this multimedia files is more important. For hiding secret information in images, there exits a large variety of techniques some are more complex but all of them have respective strong and weak points. Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Information hiding techniques include cryptography, steganography, watermarking. Cryptography is the process of converting information to an un-intelligible form so that only the authorized persons are allowed to decrypt the data with public/private keys. As the advances were made in this field, it is simple for unauthorized person to decrypt the data. For better security more sophisticated methods designed over cryptography, steganography and watermarking concepts are then discovered. Steganography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication [1]. The importance of steganography is increased day by day, and a lot of work is done to enhance this field.

Quite difference of steganography and cryptography is that, in cryptography the content of the message is secret on the other hand in steganography focuses on keeping the existence of a message secret.

Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect. Some of the differences between steganography and watermarking are [2].

1. The information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganographic systems just hide any information
2. “Robustness” criteria are also different, since steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal by a pirate
3. Steganographic communications are usually point-to-point (between sender and receiver) while watermarking techniques is usually one-to-many.

2.Classification of watermark:

Some of the important types of watermarking based on different watermarks [3] are given below:

2.1 Visible watermark: Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the centre part of the image. Further, such watermarks are protected against such as statistical analysis. The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface [4].

2.2 Invisible watermark: Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and /or author authentication and for detecting unauthorized copier.

2.3 Public watermark: Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not secure. However, public watermarks are useful for carrying IPR information.

2.4 Fragile watermark: Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. Absence of the watermark indicates that a copy has been made.

2.5 Private watermark: Private watermarks are also known as secure watermarks. To read or retrieve such a watermark, it is necessary to have the secret key.

2.6 Perceptual watermarks: A perceptual watermark exploits the aspects of human sensory system to provide invisible yet robust watermark. Such watermarks are also known as transparent watermarks that provide extremely high quality contents.

3.Techniques of Watermarking:

3.1. Spatial-Domain technologies:

Spatial domain technologies refer to those embedding watermarks by directly changing pixel values of host images. Some common spatial-domain algorithms include Least Significant Bit (LSB) Modification, Patchwork, Texture Block Coding, etc. The most serious drawback of spatial-domain technologies is limited robustness [8]. In case of attacks like lossy compression and low pass filtering, it is difficult for spatial domain watermarks to survive. Also the information can

be embedded in spatial domain is very limited. We introduce the most famous spatial-domain technology, least significant bit (LSB).

3.1.1 LSB:

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks.

For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information.

3.2 Frequency-Domain Technologies:

Frequency domain approach is similar to the spatial domain in the sense that values of the selected frequency can be altered. Compared to spatial-domain watermark, watermark in frequency domain is more robust and compatible to popular image compression standards. Thus frequency-domain watermarking obtains much more attention. To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others.

Most frequency-domain algorithms make use of the spread spectrum communication technique. The spread spectrum watermarking schemes are the use of spread spectrum communication in digital watermarking. Similar to that in communication, spread spectrum watermarking schemes embed watermarks in the whole host image. The watermark is distributed among the whole frequency band. To destroy the watermark, one has to add noise with sufficiently large amplitude, which will heavily degrade the quality of watermarked image and be considered as an unsuccessful attack.

The frequency domain watermarking schemes is compatible with existing image compression standards, in particular, the JPEG standard. The compatibility ensures those schemes a good performance when the watermarked image is subject to lossy compression. In consequence, those schemes become particularly useful in practical applications on the Internet.

The frequency-domain watermark should be embedded into the mid-band of the transformed host image. Watermarks in high frequency band tend to have less influence on the quality of original image, whereas watermarks in low band will achieve a better robustness. And the mid-band scheme is right a tradeoff between the robustness and imperceptibility.

The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Discrete Laguerre Transform (DLT) and the Discrete Hadamard Transform (DHT). The characteristics of the human visual system (HVS) are better captured by the spectral coefficients by the use of frequency domain watermarks.

For example, the HVS is more sensitive to low-frequency coefficients, and less sensitive to high-frequency coefficients. In other words, low-frequency coefficients are relatively significant, which means alterations to those components might cause severe distortion to the original image. On the other hand, high-frequency coefficients are considered insignificant; thus, processing techniques, such as compression, tend to remove high-frequency coefficients aggressively. To obtain a balance between robustness and imperceptibility, most algorithms embed watermarks in the midrange frequencies.

3.2.1 Discrete Cosine Transformation (DCT): In Discrete cosine transform, it represents data in terms of frequency space rather than an amplitude space. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. they are weak against attacks like rotation, scaling, cropping etc. However, they are difficult to implement and are computationally more expensive.

3.2.2 Discrete Wavelet Transform (DWT):

For higher compression levels, DWT is mostly used and thus increase the level of robustness of the information that is hidden, something which is essential in an area like watermarking.

This technique works by taking many wavelets to encode a whole image. They allow images to be compressed so highly by storing the high frequency “detail” in the image separately from the low frequency parts. The low frequency areas can then be compressed which is acceptable as they are most viable for compression. Quantization can then take place to compress things further and the whole process can start again if needed [7].

3.3 Spread Spectrum Watermarking:

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the water-mark extraction is possible without using the original unmarked image [5].

Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium. Spread spectrum techniques are now widely used in military radio communications, due to their very high robustness to detection and extraction. SSIS is a quite mature process, and its aim is to achieve low

detectability, ease of extraction, high data rate and good robustness to removal. It is based on spread spectrum techniques, but it enhances them by adding other encoding steps, acquiring better performance.

The idea of spread spectrum communications, as used in code-division multiple access (CDMA) radio communication systems, was originally developed for secure and unobtrusive radio communication.

4.Attacks on Watermark:

The attack is a method to find and remove watermarking from content. The watermarking information process is called "attacked information". Robustness is an elimination scheme of various attacks. Attacked data can be easily detected by the watermark quality and channel capacity, from bit errors [6]. The largest category of attacks may be further divided into four distinct groups: removable attacks, geographic attacks, cryptographic attacks, and cryptographic protocol attacks [6].

Basic attacks take advantage of limitations in the design of the embedding techniques. Simple spread spectrum techniques, for example, are able to survive amplitude distortion and noise addition but are vulnerable to timing errors.

Robustness attacks remove the presence of a watermark [8]. Although most techniques can survive a variety of transformations, compression, noise addition, etc. they do not cope so easily with combinations of them or with random geometric distortions. If a series of minor distortions are applied the watermark can be lost while the image remains largely unchanged.

Protecting against these attacks can be done by anticipating which transformations pirates are likely to use. Embedding multiple copies of the mark using inverse transformations can increase the resistance to these attacks.

Presentation attacks modify the content of the file in order to prevent the detection of the watermark.

Interpretation attack finds a situation in which the assertion of ownership is prevented [9]. Robustness refers to the ability of the mark to survive transformations and not resistance to an algorithmic attack.

In Implementation Attacks, if the mark detection software is vulnerable it may be possible for attackers to deceive it.

There is a general attack on mark readers which explores an image on the boundary between no mark having been found and one being detected. An acceptable copy of the image can be iteratively generated which does not include the mark [7].

5.Applications of Watermarking:

Watermarking is used in copyright protection; it is used to embed information about the owner of the data in order to prevent other parties from claiming the copyright on the data. A data could contain more than one watermarks, indicating copyright information of different owners.

In Multi-media by using watermarks one could be embedded data with “copy once” or “copy never” watermarks which could be identified by compliant hardware. We can use watermarks to protect software CD from pirating. If the software CD is pirated and used elsewhere, it is used to convey information about the legal recipient.

6.CONCLUSION

Now a days watermark majorly used for copyright the digital image. In this survey we conclude that watermarking function are not only authenticate but also protect for such documents against malicious intentions to change such documents or ever claim the rights of such documents. It can also be used to mark a digital file so that it is intended to be visible (visible watermarking) or visible to its creator(invisible watermarking). The main purpose of watermarking is to prevent the illegal copying or claim of ownership of digital media.

7.REFERENCES

1. A. Kawale, S. Gaidhani, “Digital Image Watermarking” in International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013

2. S. Katzenbeisser, F. A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, 2000, pp. 2.

3. K. Rawat, “Digital Watermarking Schemes for Authorization against Copying or Piracy of Color Images” in Indian Journal of Computer Science and Engineering Vol. 1 No. 4 295-300

4. T. Morkel, J.H.P Eloff, M. Olivier, “An Overview of Image Steganography” Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

5. Digital Watermarking Techniques A. Bhatia, R. Kumari U.I.E.T, Panjab University

6. P. Meerwald, “Digital Image Watermarking in the Wavelet Transform”

7. Steganography and digital watermarking 2004 J. Cummins, Patrick Diskin, S. Lau and R. Parlett, School of Computer Science, The University of Birmingham.

8. G. Voyatzis, N. Nikolaidis and I. Pitas, "Digital Watermarking: An Overview", Department of Informatics, University of Thessaloniki.

9. H. Berghel, and L. Gorman, "Digital Watermarking", http://www.acm.org/~hlb/publications/dig_wtr/dig_watr.html, January 1997