Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.686 – 690

REVIEW ARTICLE

A Review on Digital Watermarking and Its Techniques

Kirti[1], Vikram Nandal[2]

[1]M.Tech student, CSE Dept, R.N College of Engineering & Management

[2]Assistant Professor, CSE Dept, R.N College of Engineering & Management

[1] Kirtinandal3@gmail.com, [2] vikramcselive.com

Abstract: Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the internet has created copyright infringement issues. In this paper we aim to present a survey of different techniques on digital image watermarking. Digital watermarking technique is becoming more important in this developing society of internet. Digital watermarking is used as a key solution to make the data transferring secure from illegal interferences. In this paper we have also discussed various attacks on watermarking and application area where water making technique need to be used.

Keywords: Digital Watermark, Frequency Domain, Spatial Domain

I. INTRODUCTION

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Now-a-days use of internet is increasing day by day. With the rapid advancement in technology, speed of data over networks has crossed the bars. There is urgent need to preserve the copyright of individual's creation, which is done by using digital image watermarking. There has been significant interest in watermarking in recent years mainly because of two reasons, one is digitization of documents and second is rapid and untroubled traffic over internet. Digital data offers many advantages and new potentials to the user. Digitized documents can easily be manipulated thus, losing its originality. In result of that watermarking techniques came in light [1]. To identify the owner of the image and to solve the problem of its ownership, digital image watermarking is required. We can also define a watermark as the digital data embedded in multimedia objects

such that the watermark can be detected or extracted at later times in order to make an assertion about the object. The main purpose of digital watermarking is to embed information imperceptibly and robustly in the host data. Typically the watermark contains information about the origin, ownership, destination, copy control, transaction etc.[2].

II. DIGITAL WATERMARKING TECHNIQUES

Watermarking is not a new phenomenon. In the modern era, providing authenticity is becoming increasingly important as most of the world's information is stored as readily transferable bits. Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer [3]. Content providers want to embed watermarks in their multimedia objects (digital content) for several reasons like the owner of the copyright protection, content authentication, tamper detection etc. There are various watermarking techniques as follows:

1. Based on working domain

Based on working domain, there are two techniques:

1.1. The spatial domain techniques: In this technique, the watermark is inserted in the cover image changing pixels or image characteristics [4]. The algorithm should carefully weigh the number of changed bits in the pixels against the possibility of the watermark becoming visible. It further consists of two categories:

1.1.1. Least-Significant Bit: Least Significant Bits (LSB): This is the simplest approach, because the least significant bit carries less relevant information and their modification does not cause perceptible changes. Among these approaches there are types using only the salient points or types, which use some kind of cryptography on the watermark message before the embedding, process [5].

1.1.2. SSM Modulation Based Techniques: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. This is done for different reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection.

1.2. The frequency-domain techniques: The frequency-domain techniques mainly used for watermarking of the human visual system are better captured by the spectral coefficients. The transforms are broadly categorized in two ways:

1.2.1. Discrete Cosine Transformation (DCT): Discrete Cosine Transform is like as Discrete Fourier Transform. It is a technique for converting a signal into elementary frequency components. The 2-dimentional DCT of given matrix gives the frequency coefficients in the form of another matrix. The left topmost corner of the matrix represents the lowest frequency coefficients while the right bottom most corner represents the highest frequency coefficients. Watermarking with DCT techniques are robust as compared to spatial domain techniques.

1.2.2. Discrete Wavelet Transformation (DWT): Discrete Wavelet Transform is a mathematical tool for hierarchically decomposing an image. It is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelet transform provides both frequency and spatial description of an image. The wavelet transform decompose the image in four channels (LL, HL, LH and HH) with the same bandwidth thus creating a multi-resolution perspective. Due to this advantage the watermark can embed in any of the frequency bands and on inverse transform the watermark will be distributed throughout the low and high frequencies as well as in the spatial domain.

2. Based on human Perception

Based on human perception, there are two techniques:

2.1. Visible watermarks: 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 center part of the image.

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

3. Robust & Fragile Watermarking

Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. As opposed to this, fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with. 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.

4. Public & Private Watermarking

In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not.

5. Asymmetric &Symmetric Watermarking

Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking (or symmetric key watermarking) the same keys are used for embedding and detecting watermarks.

6. Steganographic & Non-steganography watermarking

Steganographic watermarking is the technique where content users are unaware of the presence of a watermark. In non-stenographic watermarking, the users are aware of the presence of a watermark. Steganographic watermarking is used in fingerprinting applications while Non steganographic watermarking technique.

III. ATTACKS IN WATERMARKING

The transmission media can cause some loss in the signal implying in a damaged content. These attacks may be intentional or accidental [6]. Intentional attacks use all available resources to destroy or modify the watermark making it impossible to extract it, the methods usually used are: signal processing techniques, cryptanalysis, steganalysis. On the other hand, accidental attacks are inevitable, because every image processing or transmission noise may introduce distortions. Besides these types, there are other types of attacks called estimation based on attacks. In estimation based attacks, estimates of either the watermark data or the original object can be obtained using stochastic methods.

1. **Removal and Interference Attacks**: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Moreover, interference attacks are those which an additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging and noise storm are some examples of this category of attacks. The collusion attack occurs when a number of authorized recipients of the multimedia object come together to generate an unwatermarked object by averaging all the different watermarked objects.
2. **Geometric Attacks**: Geometric attacks are specific to images and videos. Geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data. This type of attack includes affine transforms such as rotation, translation, and scaling. Warping, line/column removal and cropping are also included in this family of attacks. Another example of geometric attack is the mosaic attack. In this mosaic attack, the watermark image is divided into several parts and rearranged using proper HTML code, constructing watermark image in which the watermark detector will fail to provide desired results. Local pixel jittering is an efficient spatial domain geometric attack.
3. **Cryptographic Attacks**: The above two types of attacks, removal and geometric, do not breach the security of the watermarking algorithm. On the other hand, cryptographic attacks deal with the cracking of the security. For example, finding the secrete watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [7]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.
4. **Protocol Attacks**: The protocol attacks exploit the loopholes in the watermarking concept. One example of such attack is the IBM attack [8]. The IBM attack is also known as the deadlock attack, inversion attack, or

fake-original attack. This attack embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was. Watermarking of an already watermarked image is called rewatermarking. In some inversion attacks, a fake original object is created that produces the same results through the detector as that of the real original object.

IV. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

There are various watermarking applications for images, as listed below [9] [10]:

1) **Fingerprints**: The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained. Associating unique information about each distributed copy of digital content is called fingerprinting, and watermarking is an appropriate solution for that application because it is invisible and inseparable from the content[11].Prevention of unauthorized copying is accomplished by embedding information about how often an image can be legally copied [12].
2) **Tamper Detection**: Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted [15].
3) **Image and content authentication**: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera [13].
4) **Medical applications**: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [14].
5) **Broadcasting Monitoring**: This type of monitoring is used to confirm the content that is supposed to be transmitted and. As an example, commercial advertisements could be monitored through their watermarks to confirm timing and count.
6) **Owner Identification**: The conventional form of intellectual ownership verification is a visual mark. But, nowadays, this is easily overcome by the use of software that modifies images. An example is images with a copyright registration symbol © which have this mark removed by specialized software. In this case invisible watermarks are used in order to overcome the problem.
7) **Signatures**: The content owner is recognized by the watermark. It is possible that this might be exploited by a potential user to get hold of legal rights to copy or publish the content from the contact owner.
8) **Publication Monitoring and Copy Control**: The watermark contains owner data and specifies the corresponding amount of copies allowed. This presupposes hardware and software able to update the watermark at every use. It also allows copy tracking of unauthorized distribution since owner data is recorded in the watermark.

V. CONCLUSION

Digital watermarking of multimedia content has become a very active research area over the last several years. Watermarking is a very important field for copyrights of various electronic documents and media. With images widely available on the Internet, it may sometimes be desirable to use watermarks. Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. In this paper we have discussed several watermarking techniques and attacks which might occur.

REFERENCES

[1] Petitcolas F. A. P., Anderson, R. J. Kuhn, M. G., "Information Hiding– A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 1062-1078, July 1999.
[2] I. J. Cox and M. L. Miller, "Electronic watermarking: the first years". Fourth, IEEE Workshop on Multimedia Signal Processing, 2001, pp. 225-230.
[3] Md. Mahfuzur Rahman and Koichi Harada, "Parity enhanced topology based spot area watermarking method for copyright protection of layered 3D triangular mesh data", IJCHNS International Journal of Computer Science and Network Security, Vol. 6, No. 2A, February 2006.
[4] M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain", University of Bonn Germany, Tech. Rep., 2006.
[5] S. Riaz, M. Y. Javel, and M. A. Anjum, "Invisible watermarking scheme in spatial and frequency domains", International Conference on Emerging Technologies, 2008.
[6] J.Liu and X.He, "A review study on digital watermarking", 1st International Conference on Information and Communication Technologies, pp. 337-341, 2005.
[7] G. Coatrieux, L. Lecornu, Member, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member IEEE, "a review of digital image watermarking health care".
[8] F. Hartung, J.K. Su., and B.Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks", pp. 147-158, 1999.
[9]. F. Hartung and M. Kutter,Stefan Katzenbeisser and FabienA. P. Petitcolas, editors, Information Hiding Techniques for Steganography and Digital watermarking , Artech House, 2000 [6] .
[10]. Juergen Seitz, Digital Watermarking for Digital
Media,Information Science Publishing, 2005.
[11]. Elias Kougianos , Saraju P. Mohanty , Rabi N. Mahapatra "Hardware assisted watermarking for multimedia" Computers and Electrical Engineering 35 (2009) 339- 358.
[12]. Keshav S Rawat et. al. / Indian Journal of Computer Science and Engineering Digital watermarking scheme for authorization against copying or piracy of color image volume. 1 No. 4 295-300.
[13]. Edin Muharemagic and Borko Furht "a survey of watermarking techniques and applications" 2001.
[14]. G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'a review of digital image watermarking in health care'.
[15]. J. Fridrich, "Image watermarking for tamper detection," in Proc. IEEE Int. Conf. Image Processing, Chicago, IL, Oct. 1998, pp. 404-408

