Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparative Analysis of Popular Digital Image Watermarking Techniques

Manish Deoli, Rohan Verma
Department of Information Technology, HNBGU, Srinagar Garhwal,
Uttarakhand, India

Abstract—Digital watermarking is a technique which is developed to ensure the authenticity and security of digital images. Watermarking is used for copyright management, content protection, tamper detection and content authentication. A lot of work has been done in the field of digital image processing, audio and video etc. This paper presents comparative analysis of different watermarking techniques and attacks. Prime focus of this analysis is image only.

Keywords—watermark detection,watermarking, visible watermarking, invisible watermarking.

I. INTRODUCTION

The term "digital watermarking" was first coined by Tirkel in 1993, when he presented two watermarking techniques to hide the watermark data in the digital images [1]. Watermarking is a technology that provides data security, authentication and integrity and also provides copyright protection for digital media. Watermarking process mainly consists of two modules, watermark embedding module and watermark extraction and detection module. The main focus of watermarking technology is to embed secret information or signal into digital images, video and audio etc. After embedding the information is detected and extracted and extracted information reveals real identity of media or owner. Watermarking provides following facilities to a user: copying prevention, proof of ownership, Authentication, Broadcast Monitoring, Data hiding. Application area of digital watermarking is very broad, it is used in certification, protection, distribution etc. [4]. So digital watermarking becomes a hot research area for authenticity and security of information [5,6].

II. WATERMARKING TECHNOLOGY

As a rapidly growing technology, digital watermarking incorporates the features and theories of different subjects, such as cryptography, digital signal processing, probability theory, network technology, algorithm design, stochastic theory etc. in digital watermarking a secret information (text, signal, image etc.) is embedded into the target image to ensure the security and authentication. Watermark can be hidden in the digital information either visibly or invisibly. Watermark can be embedded either in spatial or frequency domain. Once a watermark is embedded in the digital media several attacks can be performed on it as it goes through a series of digital image processing events. An attack can be accidental (in case of images, low pass filtering or gamma correction or compression) or intentional (like tempering, cropping, noise etc.). So the watermark has to be robust enough to deal with all these possible attacks. When the owner wants to check whether the data is attacked, it can be checked by simply looking at the watermark which could be extracted from the data. If the extracted watermark is same as embedded watermark then there is no attack performed over the image and if they are not same then it might have been attacked [2].

Requisite for digital watermarking techniques

There are three main requisite for digital watermarking techniques. They are transparency, robustness, capacity.

1) Transparency:

It states that digital watermark should not affect the quality of original image. It is defined by **Cox et al. (2002)** as "perceptual similarity between the original and watermarked versions of the cover work". It is required that watermark should not provide a visible distortion to the image [3].

2) Robustness:

Watermark should have the ability to detect the possible set of attacks after extraction defined by **cox et al. (2002)**. Watermarks could be removed intentionally or unintentionally by trivial image processing operations like contrast or brightness enhancement, gamma correction etc. so therefore watermarks should have strong enough against possible set of digital attacks [3].

3) Capacity:

This property defines what amount of watermark should be embedded to successfully detect after extraction. **Cox et al. (2002)** define capacity or data payload as "the number of bits a watermark embeds within a unit of time or work". Watermark should hold enough information to represent the uniqueness of the image [3].

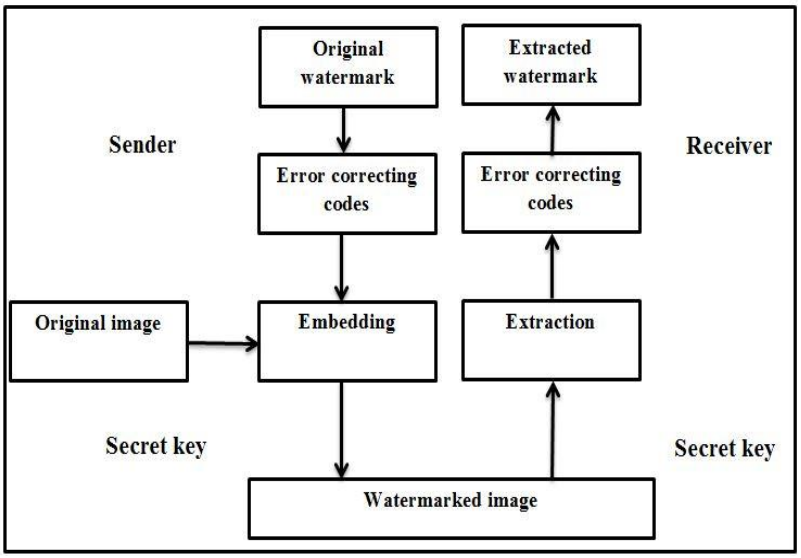

Fig.1 watermarking techniques

III. CLASSIFICATION OF DIGITAL WATERMARKING

Digital images can be represented in spatial domain and transform domain. In spatial domain image is represented by pixels whereas in transform domain it can be represented by frequencies. According to the characteristics the watermarking process can be divided into three categories: robust, fragile and semi fragile. Robust watermarking technique resists all possible set of attacks. Hence provide full security to the image. Fragile watermarking is very sensitive to the changes in the signal and mainly used for integrity protection. Semi fragile watermarking can tolerate some changes in the watermarked image such as lossy compression and quantized noise. In this section digital watermarking techniques classified into various categories [2,3,4,5].

Robust watermarking: Robustness is required for copyright information of digital images, video and audio. The embedded watermark should be robust enough to deal with common image processing techniques, lossy compression and various image processing attacks. In this technique watermark is not affected by any attack and also resist geometrical and non-geometrical attacks without changing embedded watermark [5].

Fragile watermarking: the basic idea behind these techniques is to embed a specific watermark which is generally independent of the image data. Hence, any attempt to change the contents of the image will also put a reasonable amount of changes into the watermark itself. So, in order to ensure authentication it has to search for the distortion in the watermark. The major drawback of this approach is that it is hard to differentiate between malicious and non-malicious attacks [5].

Semi Fragile watermarking: Semi fragile watermarking is different from fragile in case of sensitivity fragile doesn't tolerate any changes in watermark but semi fragile watermarking tolerate some degree of changes in watermarking like addition of quantization noise and lossy compression [5].

Image watermarking: Image watermarking mainly used for digital images in which they hide watermark in images and after that detect and extract that secret information for author's identity [5].

Video watermarking: In video watermarking watermark is added to the video stream in order to provide security. This is the extended version of image watermarking. This method needs real time detection and extraction [5].

Audio watermarking: In audio watermarking unique electronic identifier (UEI) is embedded in audio signal which identify ownership of copyright. Audio watermarking is same as image watermarking where watermark put on image[2].

Text watermarking: Text watermarking adds some secret information to the text file. It is used for text copyright protection. If there is any modification in text file it can be detected by looking the distortion in the watermark [2].

Visible Watermarking: Visible watermarking means adding an image to another image which is visible to user such as some photography agencies or other add copyright symbol ("©") to its photography which is visible. Visible watermarking is used for enhancing copy right protection. Visible watermarking used to indicate identity or ownership [5]**.**

Invisible watermarking: Invisible watermarking technology is used because in visible watermarking watermark can easily modified so it is not secure mechanism compare to invisible watermarking. In invisible watermarking secret information is added to original image which is not visible for users if images are modified so by using software we can easily identify whether watermark is attacked or not [5].

Spatial Domain watermarking: In spatial domain technique we use statistical properties of the digital image to embed watermark. It uses each pixel and its immediate surrounding pixel of host image and also used statistical

properties of host image and watermark image which is to be embedded. Now each pixel in host image is replaced one by one to each pixel of watermark image. So it creates a relationship between the host image and the watermark image in which watermark image become semi transparent and robust and also it minimized the errors while adding and subtracting the watermark image in host image. It is used in LSB and SSM modulation based techniques. [5]

Frequency Domain watermarking: In frequency domain watermarking first the host image is transformed into frequency domain. So different transformed methods are used like DCT, DWT and DFT. Then a watermark signal is embedded to the signal of the original image. Then by checking the distortion in the watermark signal it can be easily analyzed whether the original signal is attacked or not. Compared to spatial domain watermarking, frequency domain watermarking is more compatible and robust for some image standard like JPEG [2].

Blind watermarking: This technique does not require any prior information about the watermark. It extracts watermark bits from the target image itself. So it is very challenging techniques because in doesn't need of original data and watermark data. This technology extracts n-bits from watermark image [2].

Non blind Watermarking: This technique is used for detection purpose. It is also known as private watermarking. It needs original data to detect whether watermark is modified or not. So there are two types of non blind watermarking techniques is available Type-I and Type-II. Type-I first extract watermark from the distorted image and then use original data as a hint to find out whether the watermark is same as in the original image. In Type-II it also needs a copy of watermark to check whether watermark exists or not. Non blind watermarking is more robust [5].

Semi blind watermarking: This technique is also used for detection purpose. It doesn't need original data for detection. Only a copy of watermark is required to check whether it is present or not. Semi blind watermarking is used in copy control, copy right protection in which we only have to find out original recipient from modified data without original data. So it requires only copied watermark by using this technique we find out whether watermark is present or not I distorted image [4].

IV. WATERMARKING APPLICATIONS

Digital watermarking has been successfully deployed over a million of media objects to ensure its authenticity and to provide security from a possible set of digital image processing attacks. In this section we will discuss the application area of digital watermarking [2,4,5].

1) Content Archiving: Generally information content is recognized by their name, but this name can be easily altered, so this technique is very fragile. Watermarking techniques can be used to insert a digital object identifier or some serial number to the digital content like images, video or audio. So therefore, embedding a watermark to the archive data reduces the possibility of tempering.

2) Copyright protection: digital watermarking can be used to protect and identify the copyright ownership of digital content. It protects against the redistribution of the copyrighted content over the untrusted network like Internet or peer-to-peer networks.

3) Tamper detection: Tamper detection is highly required for the applications which use highly sensitive data such as satellite image or medical image. Tempering in Digital content can be easily detected by inserting fragile watermarks. If the watermark is distorted it indicates the tampering so that digital content cannot be trusted. Tamper detection is also desirable in court of law as digital images are used as a proof.

4) Digital fingerprint: This technique is used to represent the ownership of the digital content. In this technique a unique fingerprint, which represent the ownership, is inserted into the digital content. So a single digital content can have different fingerprints because they belong to the different users.

5) Meta-data insertion: Meta-data refers to the data about data. Images can be used in search engines labelled with their contents. Similarly, audio files can hold the lyrics and name of the singer or name the movie with its poster. Medical x-rays can store the patient records. The above mentioned facilities can be availed by using watermark.

6) Broadcast monitoring: It is a technique of cross verifying which determines if the content that was supposed to broadcasted (on TV or Radio) has really been broadcasted or not. The major application of broadcast monitoring is in commercial advertisement in which the company which is advertising be able to monitor if its advertisement is broadcasted according to the schedule or not.

7) Annotation and privacy control: watermarking can be used to append annotation into a digital image. The details related to the patient and its medical condition can be put in a single image which provides privacy to the patient. This in turn also reduces the storage space.

V. CONCLUSION

In this era of illusion it is very hard to ensure the authenticity and security of digital media. So users expect a robust and efficient solution that will ensure copyright protection and guarantee the authenticity of digital media documents. Watermarking techniques discussed above fulfill all the expectations of a user. In this paper we provide a brief overview of current development in watermarking technology, requirement for an algorithm to be efficient and then discussed the various watermarking techniques and their advantages and disadvantages by comparing them.in the end we discussed the applications of digital watermarking in various fields.

REFERENCES

[1] Schyndel RG., Tirkel A., Osborne CF, "A digital watermark", proceedings of IEEE international conference on image processing, ICIP-1994, pp. 86-90.

[2] Chaoli OU, "Text watermarking text document copyright protection", june 2003, pp. 1-12.

[3] Potdar VM, Han S, Cheng E, "A survey of digital watermarking techniques", proceedings of IEEE international conference on industrial informatics, 2005, pp. 709-716.

[4] Rey c, Dugelay JL, "A survey of watermarking algorithms for image authentication", EURASIP journal on applied signal processing, 2002, pp. 613-621.

[5] Singh P, Chadha RS, "A survey of digital watermarking techniques application and attacks", international journal of engineering and innovative technology, March 2013, pp. 165-175.

[6] Cox IJ, Miller ML and Bloom JA, "Digital watermarking", Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.

