A Review Paper on Digital Watermarking and its Techniques

Ruchika Patel
Information Technology, The Gujarat Technology University SVIT,
Vasad, Gujarat 388306, India

Parth Bhatt
Ass. Professor, Department of IT, Gujarat Technology University SVIT,
Vasad, Gujarat 388306, India

ABSTRACT
In today's Era, message transmissions over the internet have protection problems of the digital data. Hence, protection of secret messages during transmission becomes a difficult subject. Digital watermarking is provide protection of digital information or identifying information against illegitimate exploitations and allocations. watermarking is a technology to guarantee and make possible data certification, security and copyright defense of the information. The intend of watermarking is to consist of hidden data in multimedia information to ensure security examination. It would be then probable to progress the surrounded message, even if the information was distorted by one or more non-dangerous attacks. In this paper, we present the various types of watermarking techniques and application region where water making technique required. Also a survey on the some new work is done in image watermarking field.

Keywords
digital image watermarking.

1. INTRODUCTION
Protection of digital data has become a popular matter due to the quick development of the pervasive multimedia technology. Copyright protection of digital data has become a significant issue over increasing use of internet. Digital watermarking is that technology that provides security, data validation and copyright protection of the digital data. Digital watermarking is the process of embedding secret digital data, signal into the digital media such as image, video, audio and text. Later the embedded information is detected and extracted out to reveal the real identity of the digital media. Watermarking is used for Proof of Ownership, Copying Prevention, data validation, Data Hiding and Broadcast Monitoring. Digital Image Watermarking technology has many applications for protection of digital data, certification, distribution of the digital media and label of the user information. Watermarking of data has become a very important area in information hiding. This paper analyses the key technologies of Digital Image Watermarking and explore its applications and methods for the security purposes.

2. BASIC OF WATERMARKING
The basic model of Digital Image Watermarking consists of two parts:

1. Watermark embedding

2. Watermark extraction

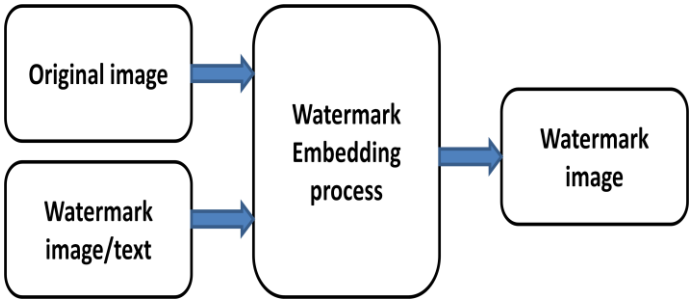

Figure 1: Watermarking Embedding process

The first process is Watermark Embedding that is shown in Figure 1 and the second process is the Watermark Extraction that is shown in Figure 2.

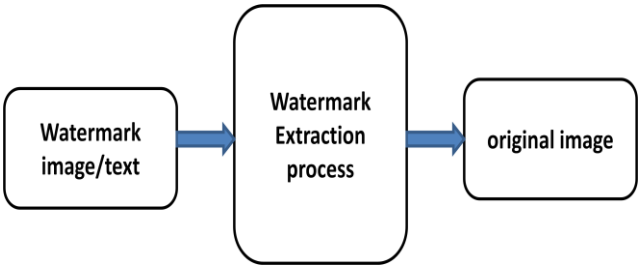

Figure 2: Watermarking Extraction Process

Watermark Embedding is the process of embedding watermark into the original image. The output is the Watermarked image. This process is carried out at sender's side. Watermark Extraction is the Process of detecting watermark from the Watermarked image.

3. PROPERTIES OF WATERMARKING
The basic requirements of the digital watermarking can be treated as attributes, properties. Different applications require singular properties of watermarking. The different attributes of the watermarking take different place in application design. The basic attributes/properties of watermarking are as follow.

A. Robustness
Robustness refers to that the watermark embedded in data has the capability of detecting watermark after a variety of processing operations and attacks. The watermark should not removed by simple processing techniques. Hence watermark should be strong against some attack. Robust watermarks are designed to resist normal processing.

B. Fidelity
Fidelity or Imperceptibility is the most important requirement in watermarking system. Watermark cannot be detect by human eyes or ear, only be detected through special processing of watermark detector. It can be detected by an authorized person only. Such watermarks are used for content or author validation and for detecting unauthorized

copies of the data. In other words fidelity can be considered as a measure of perceptual simplicity.

C. Data Payload

Data payload refers to the number of bits embedded into the original image. It is the highest quantity of information that can be hidden without mortifying image quality. It can be calculated by the amount of hidden information in the original data. This property depicts how much data should be embedded as a watermark so that it can be effectively detected during extraction process.

D. Security

A watermark system is said to be secure, if the unauthorized person cannot remove the watermark without having full awareness of embedding algorithm, detector and composition of watermark. The security is most important factor of watermarking system. Only the authorized person can detect watermark. Thus, the copyrights protection can achieve in watermarking system.

E. Computational Complexity

Computation complexity is defined as the amount of time taken by the watermarking algorithm for embedding and extraction process. More computational difficulty is needed for the strong security and validity of the watermark. On the other hand, real-time applications require both speed and efficiency.

F. Inevitability

Inevitability defined as the possibility to produce the original data during the watermark extraction. The optimization of the parameters is mutually competitive and cannot be plainly done simultaneously. A rational negotiation is always a requirement. Alternatively, if robustness to strong warp is an issue, the message that can be frequently hidden must not be too long.

4. APPLICATION OF WATERMARKING

There are various applications of Digital Image Watermarking. These are listed as follows

A. Copyright protection

The one of the most important application of watermarking is copyright protection from the unauthorized user. Ownership of digital media can be established in the case of a copyright dispute by using the embedded data as a proof.

B. Broadcast Monitoring

This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

C. Tamper Detection

Fragile watermarks are used for tamper detection. If the watermark is degraded or destroyed, it indicates presence of tampering and hence digital content cannot be trusted.

D. Authentication and Integrity Verification

The watermark is embedded to detect if the image has customized or not, this process can be used for verification. Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness to modification in an image.

E. Fingerprinting

The main purpose of fingerprinting is to protect clients. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by embedding single robust watermark for each receiver.

F. Content Description

This watermark can contain some detailed information of the host image such as labeling and captioning. The capacity of watermark for this kind of application should be relatively large and there is no strict requirement of robustness.

G. Medical Applications

In medical field the watermarking is important for the purpose of to protect the hospital's information from unauthorized people such as patient's report etc. Security and verification of such data are now becoming very significant in medical field where the digital data are easily distributed over the internet.

5. CLASSIFICATION OF WATERMARKING

In this section the digital watermarks, features, their techniques and application are classified and segmented into various categories.

1) According to human perception

[1] Visible watermarking

In this type of watermarking techniques the watermark is visible to the casual viewer. Watermark is an image or a message that is visible on primary image the watermark appears is a secondary translucent overlaid into the primary image.

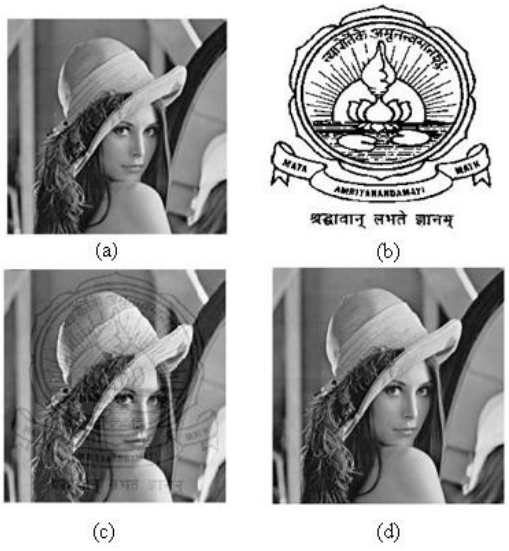

Figure (a) the original Lena image (b) the logo to be watermarked (c) visible watermarked image and (d)invisible watermarked image[7]

[2] Invisible watermarking

Invisible watermark is hidden in the original content. It can be detected by an authorized person only. Watermark is embedding in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

I. Robust:

Robustness watermarking is mainly used to sign copyright information of the digital works, the embedded watermark can defend against the common edit processing, image processing and lossy compression, and the watermark is not cracked after some attack and can still be detected to provide guarantee.

II. Fragile

Fragile watermarking is mainly used for reliability protection, which must be very responsive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

III. Semi fragile

Semi fragile watermarking is capable of tolerating some degree of the change to a watermarked image.

2) According to attached media/host signal

I. Image watermarking

In image watermarking techniques the image is used to hide the digital data. It is used to protect the photos over internet.

II. Video watermarking

In video watermarking the watermark are added to the video stream to control video application. Video watermarking is the extension of image watermarking techniques. This method requires real time extraction and robustness for compression.

***III.* Audio watermarking**

This application area is one of the most popular and hot issue due to internet composition of tunes, MP3.

IV. Text watermarking

This adds watermark to the text file to check the changes made to text files. The watermark is added in the font shape and the space between font and line spaces.

V. Graphic watermarking

It adds the watermark to 2D or 3D computer generated graphics to specify the copyright.

3) According to domain

I. Spatial domain

This domain watermarking adds the watermark by modifying the pixel of selected subsets of images. It directly loads the data into the image pixels value. Some of its methods are Least Significant Bit, SSM Modulation Based Technique.

II. Frequency domain

It is also called transform domain techniques of watermarking. In this domain the certain frequencies are altered from their original image. There are several transform domain methods, such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT).

4) According to detection process

I. Visual watermarking

It is known as private watermarking. In visual watermarking the original content are requires. It is most robust method of watermarking.

II. Semi blind watermarking

It is also known as semi private watermarking. In this watermarking scheme the original data are not required for detection of watermark. The principle of this system to locate whether that the watermark can be detected.

III. Blind watermarking

Blind watermarking is also known as public watermarking. In this watermarking the original data and the embedded watermark are not needed. This is the most demanding type of watermarking.

5) According to application

I. Source based

Source-based watermark are attractive for ownership recognition or validation where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed.

II. Destination based

The destination -based watermark could be used to trace the buyer in the case of illegal reselling.

6. ATTACKS ON DIGITAL IMAGE WATERMARKING

Digital Image Watermarking attacks can be classified to geometric and non-geometric attacks. An attack succeeds if it weakens the watermark less than acceptable limits.

A. Geometric attacks

Geometric attacks is a set of parameters that can be applied on the image. In other words geometric attacks are basic geometric transformations in an image. These attacks may include rotation, cropping, scaling, warping, translation etc. these attacks attempt to destroy synchronization of detection.

B. Non Geometric Attacks

Non Geometric attacks are common image processing attacks which includes compression of image, averaging, filtering, brightness, sharpening, printing, scanning, addition of noise, gamma correction etc.

7. CONCLUSION

In this survey paper we provided a recent research in the watermarking field. In this paper we have offered various characteristics for digital watermarking like basic of watermarking, techniques, applications, attacks that affects watermarking system. Copying photos from the Internet is just a matter of right clicking on a photo and saving it on the computer hence the security and authenticity of the image or data are cracks. The watermark is required to prevent the original images and other documents over the internet.

8. REFERENCES

[1] Xia, X.G., C. Boncelet, and G. Arce, 1998. Wavelet transform based watermark for digital images. In the International Online Journal of Optics.

[2] Santa Agreste, Guido Andaloro, Daniela Prestipino, Luigia Puccio, 2007. An image adaptive, wavelet-based watermarking of digital images. In Elsevier Journal of Computational and Applied Mathematics.

[3] M. L. M. Ingemar J. Cox, Jeffrey A. Bloom, Jessica Fridrich, and. Ton Kalker, 2008. Digital Watermarking and Steganography: Morgan. In Kaufmann Publishers.

[4] Jeng-Shyang Pan, Hsiang-Cheh Huang, Lakhmi C. Jain, and Wai-Chi Fang, 2004.Intelligent Multimedia Data Hiding. In Springer.

[5] Jain Liu, and Xiangjain, 2005. A review study on Digital Watermarking. In International Conference on Information and Communication Technologies.

[6] Y. Yusof, and O.O. Khalifa, 2007. Digital watermarking for digital images using wavelet transform. In Telecommunications and Malaysia International conference on Communications.

[7] Shraddha S. Katariya,2012.Digital Watermarking: Review in International Journal of Engineering and Innovative Technology

[8] http://jayitsecurity.blogspot.in/2012/06/what-are-blind-semi-blind-and-non-blind.html

[9] http://www.scribd.com/doc/6816148/WATERMARKING

[10] Vinita Gupta and Mr. Atul Barve " A Review on Image Watermarking and Its Techniques" in International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, January 2014.

[11] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[12] Ruchi Kashyap, Mr. Karan Mahajan "Embedding Useful Information in Digital Watermarking: A Review" in Int. Journal of Engineering Research and Applications, Vol. 4, Issue 6(Version 5), June 2014.

[13] Jobenjit Singh Chahal, Shivani Khurana " A Review on Digital Image Watermarking" in International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 12, December 2013.

[14] Manpreet Kaur,Sonika Jindal and Sunny Behal," A STUDY OF DIGITAL IMAGE WATERMARKING" in IJREAS Volume 2, Issue 2 ,February 2012.

[15] Vaishali S. Jabade, Dr. Sachin R. Gengaje," Literature Review of Wavelet Based Digital Image Watermarking Techniques" in International Journal of Computer Applications, Volume 3, October 2011

[16] CHAPTER 2: LITERATURE REVIEW, Source: Internet

[17] http://ippr-practical.blogspot.in

[18] www.scisstudyguides.addr.com