A Review on Digital Image Watermarking

Jobenjit Singh Chahal¹, Shivani Khurana²

¹Research Scholar, ²Assistant Professor, Department of CSE, CT Institute of Engineering, Management & Technology, Shahpur (Jalandhar), India

Abstract—In the recent few years, it has become a daily need to distribute digital images as a part of widespread multimedia technology by means of the World Wide Web. Digital Image Watermarking techniques have been developed to protect digital images from illegal modifications and illegal reproductions. So these techniques have developed widely to maintain the broadcasting media and content authentication, broadcast monitoring, tamper detection, copyright protection, and many other applications. This paper highlights the basic model of Digital Image Watermarking, its applications and its attributes. Moreover, it reviews some of the techniques used in Digital Image Watermarking. In addition, various possible attacks on watermarked images are discussed. To check the Imperceptibility and Robustness, Peak Signal Noise Ratio (PSNR) and Normalized Cross-Correlation (NCC) parameters are being used.

Keywords—Watermarking, Tamper detection, Copyright protection, Imperceptibility, PSNR, NCC.

I. INTRODUCTION

Security of digital data has become a popular topic due to the rapid development of the widespread multimedia technology by means of computer networks. With the increasing use of internet, copyright protection for multimedia data has become an important issue. The traditional information security technology based on cryptography theory has its own limitations. In order to resolve the shortcomings of traditional information security technology, more and more researchers have been focusing on the study of the Digital Image Watermarking technology because it can effectively compensate for the deficiencies of the security and protection application of traditional information security technology. The watermark information can be copyright information, authentication information or controlling information so as to determine the copyright owner of the digital works, certify the authenticity and integrity of multimedia works, control copying according to the embedded control information, achieve the purpose of copyright protection. Digital Image Watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and label of the user information. It has become a very important field in information hiding. This paper analyses the key technologies of Digital Image Watermarking and explore its applications.

Figure 1 Digital Image Watermarking

Figure 1 represents the working domains of Digital Image Watermarking. The frequency or wavelet transformation domain is more robust and compatible to popular image compression standards than spatial domain. The frequency domain includes Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

II. BASIC MODEL OF DIGITAL IMAGE WATERMARKING

Digital Image Watermarking, can be described as a pattern of bits inserted into a digital image that helps to identify the file’s copyright information (the author, the rights, etc.) [1]. The basic model of Digital Image Watermarking consists of two parts: the first part is the Watermark Embedding Process shown in Figure 2 and the second part is the Watermark Extraction Process shown in Figure 3.

Figure 2 Watermark Embedding Process
Figure 3 Watermark Extraction Process

Watermark Embedding Process shown in Figure 2, the watermark is embedded into original image. The output is the Watermarked image. This process is carried out at sender’s side. In Figure 3 at receiver side. The Watermark Extraction Process detects the watermark from the Watermarked image.

III. ATTRIBUTES OF DIGITAL IMAGE WATERMARKING

The requirements for Digital Image Watermarking can be treated as characteristics, properties or attributes of Digital Image Watermarking. Different applications demand different properties of watermarking. Requirements of Digital Image Watermarking vary and result in various design issues depending on applications and purpose. These attributes need to be taken into consideration while designing watermarking system. There are five basic requirements as follows [2].

A. Robustness

The robustness is the ability of detecting the watermark after some signal processing modification such as spatial filtering, scanning, printing, lossy compression, translation, scaling, and rotation [3]. Watermarks should not be removed intentionally or unintentionally by simple image processing operations. Hence watermarks should be robust against variety of such attacks. Robust watermarks are designed to resist normal processing. On the other hand, fragile watermarks are designed to convey any attempt to change digital content.

B. Fidelity

Fidelity (also known as Imperceptibility and Invisibility) is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image [3]. In other words fidelity can be considered as a measure of perceptual transparency or imperceptibility of watermark. This perspective of watermarking exploits limitation of human vision. Watermarking should not introduce visible distortions as it reduces commercial value of the watermarked image.

C. Data Payload

Data payload (also known as capacity) refers to the number of bits embedded into the original image. The data payload of an image could be different according to the application that watermark is designed for [3]. It is the maximum amount of information that can be hidden without degrading image quality. It can be evaluated by the amount of hidden data. This property describes how much data should be embedded as a watermark so that it can be successfully detected during extraction process.

D. Security

Secret key has to be used for embedding and detection process in case security is a major concern. Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark.

E. Computational Complexity

The cost is the reason behind studying the complexity, so it should be at a reasonable cost [4]. Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. To ensure security and validity of watermark, more computational complexity is needed. Conversely, real-time applications necessitate both speed and efficiency.

IV. APPLICATIONS OF DIGITAL IMAGE WATERMARKING

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

A. Copyright protection

The copyright information can be embedded as a watermark into the new image. Once there is a dispute on the ownership, the watermark can be extracted to provide the evidence of who is the owner of this image [5].

B. Broadcast Monitoring

This type of monitoring is used to especially in the advertisements to make sure that the content broadcasted as the contract between the advertisement company and the customer [6].

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 modified or not, this process can be used for authentication [6]. 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 customers. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can prevent this [5]. This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient.

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
Digital Image Watermarking can be used in medical images for several purposes. It used to protect the patient’s information from unauthorized people. Protection and authentication of such images are now becoming increasingly very significant in telemedicine field where images are easily distributed over the internet.

V. 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 (also known as signal image processing attacks) are common image processing attacks which includes compression of image, averaging, filtering, brightness, sharpening, printing, scanning, addition of noise, gamma correction etc.

VI. CONCLUSION
The Digital Image Watermarking is progressing very fast and various researchers from various fields are focusing to develop robust watermarking schemes. This paper reviewed the research work done on Digital Image Watermarking. It presented the basic model for embedding and extraction of watermark. Next, it mentioned the attribute of the watermarking system. Then it listed some of the applications of Digital Image Watermarking. Finally, the possible attacks on Digital Image Watermarking are discussed.

REFERENCES