International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

Technicalities of Digital Watermarking: A Review

Er. Sandeep Kaur[1], Er. Jaspreet Kaur[2], Er. Inderpreet Kaur[2]

[1] *M.Tech. Student, CSE, Rayat Bahra Group of institutes, Punjab, India*
[2] *Assistant Professor, CSE, Rayat Bahra Group of institutes, Punjab, India*

Abstract: ***For providing security to the digital media on internet the very useful technology is digital watermarking. Watermark is an image or pattern in document which is used to identify data authentication, data integrity. The user can check the watermarked information with the watermark key and watermarking extraction process. The various techniques of watermarking reviewed in this paper are Least Significant Bit (LSB), Robust, Discrete Cosine Transform (DCT), Spatial Domain, Frequency Domain, Blind and non-blind, Spread Spectrum. Out of these techniques, DCT, Spatial and Frequency based techniques are more efficient. These provide more refined images with less effort and are more secure and robust as compared with other techniques.***

Key words: *Watermarking, DCT, Spatial, Frequency, Authentication, Security.*

1. INTRODUCTION

Digital images are composed of pixels. Each pixel represents the color of image at a single point. A pixel is a dot of any particular color in the image. Digital image processing is increasing with the technology increase. Digital image processing has many beneficial properties as compare to analogue image processing. Digital information is available on internet like images, audio, video, text and it is very easy to copy that data. To avoid this security issue Digital watermarking technique is used. Digital watermarking was introduced in 1993 [5][6]. Various purposes of watermarking are identity check, copy control, data abstraction, certification and authentication.

Digital watermarking is an application of the digital image processing [2]. It is an information hiding technique. Watermark is an encrypted code like digital signature or certificate that attached to the original document. A watermark should be secret so that only the authorized person can legally access and modify the watermark. Watermarking technique is useful for fortification of images, video and text. When any unauthorized user tries to alter digital data, he/she can catch on the basis of retrieved watermark image. When digital data is share over the internet exchange of multimedia content copyright infringement issues are comes into the image. Digital watermarking techniques are of two types that are private and public watermark [3][13].

1.1 Private watermark

A private watermark might contain data for identifying the licensee to prove authentication. To retrieve information from secret watermark at least one secret key is required, which is generated by the sender. Embedded information includes serial numbers or licensee identifying hash values. A serial no is like a link to externally stored information.

1.2 Public watermark

Public watermark is detected by the authorized receiver of copyrighted information. It contains information about copyright or licensee, such as copyright holder, the sender of the information or a URL link to fetch related information [16][17].

2. WATERMARK FRAMEWORK

Watermarking is a technique that embeds a watermark (secret code) or label into digital information. This process is known as watermark embedding process. In this process, the input to the scheme is the watermark, the cover media and a key. Key is used for security purpose, which prevents watermark from unauthorized access, recovery and manipulation. Every watermarking algorithm consists of three parts:

I. The watermark
II. The encoder
III. The decoder

The output of the watermarking scheme is the watermarked data [16][17]. In watermark detection process watermarked data, key and original watermark are the inputs. The output of the watermarking technique ensures that the information is authentic or not.

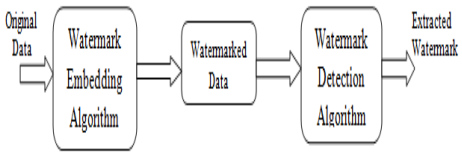

Fig1.Stages in Digital Watermarking

Digital watermarking is like watermarking physical objects expect that Digital watermarking technique is used to secure digital information instead of physical objects [18]. The watermark key to extract the original data has a one to one correspondence with watermark signal. Digital watermarking technique is different from cryptography. A cryptographic system is easily broken when the unauthorized user can read the secret message, but to break a watermarking system there are two stages:

a) The attacker can detect that watermark which is used to embedding the information.
b) The attacker can extract, read, modify or remove the hidden message.

3. TYPES OF WATERMARKING

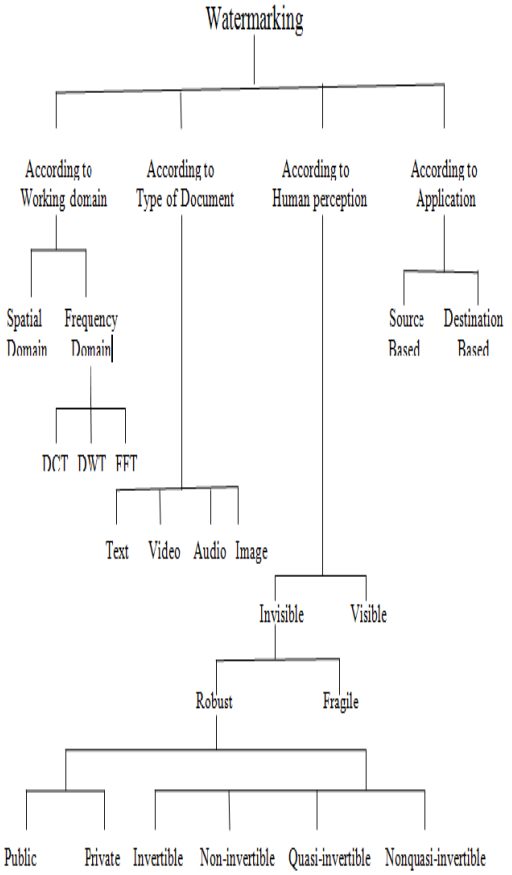

Fig2. Types of Watermarking

According to the document types watermarked watermarking can be divided into four categories:
a) Text Watermarking
b) Image Watermarking
c) Audio Watermarking
d) Video Watermarking

Digital watermarking also divided in other way as follow:
a) Visible Watermark
b) Invisible Watermark
c) Fragile Watermark
d) Robust Watermark

4. TECHNIQUES OF WATERMARKING

Digital watermarking includes theories and results from different research areas, such as signal processing, cryptography, communication and compression [4]. Using different algorithms digital watermarking encrypts the copyright data into the digital data. There are various techniques or algorithms used to hide the information. Digital watermarking techniques are:

4.1 LSB Watermarking Techniques:

LSB watermarking describes a simple and basic method to embed watermark information in digital document. Implementation of *LSB* technique is easy and does not create distortion to the image, so it is not robust against unauthorized access. The embedding of watermark into original image is done by choosing a subset of pixels and substituting the least significant bit of selected pixels with watermark bits [1].
In this technique watermark can be easily retrieved by unauthorized user so this technique cannot be used in practical applications. But this technique has beneficial properties like copy control and authenticity.

4.2 Robust Watermarking Techniques:

To increase the robustness of watermark, it should be embedded in the significant components of the document. In robust watermarking technique the modification to the watermarked content will not affect the watermark content.

4.3 DCT-based watermarking Techniques:

Discrete Cosine Transform is used in many applications like data compression, pattern recognition and image processing. This technique is more secure and robust as compare to spatial domain watermarking techniques [1]. In *DCT* technique following are the main steps:

1. The image is divided into 8x8 pixel blocks [9][10][11].

2. *DCT* transform and quantization.
3. The mid-frequency range *DCT* coefficients are selected.
4. *DCT* coefficients are used for embedding process and modified using linear *DCT* constraints.
5. Apply inverse *DCT* transform on each pixel block.

4.4 Spatial Domain Techniques:

Spatial watermarking techniques are cheap and easy to implement a watermark with less effort as compare with other watermarking techniques. Robustness is the main difference between Spatial and Frequency domain [9][10]. Spatial techniques were initially developed techniques and being developed. Spatial domain technique has the following characteristics:

1. The watermark is applied in pixel domain.
2. During watermarking embedding no transforms are applied to the host signal.
3. Host signal combination is based on simple operation, in pixel domain.

The watermark can be extracted by correlating the pattern with the received signal.

4.5 Frequency Domain Techniques:

Frequency Domain techniques are more robust than Spatial Domain techniques. Robustness and the quality of the watermark can be improved in Frequency domain. It hides the watermark information in noisy regions instead of smoother regions [15].

4.6 Blind and Non-blind Techniques:

Blind watermarking is a technique in which watermark detection can be done without the original data. Watermarked information is extracted from the scanning of source document. In non-blind technique original source is used to extract the watermark by interconnected procedure.

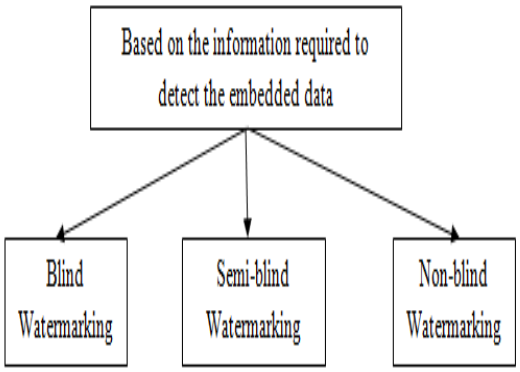

Fig3. Types of Blind Watermarking

In semi-blind watermarking technique watermark require some special information to detect the data in the watermarked signal [12]. But in Non-blind technique watermark require original signal to detect the embedded information in the watermarked signal. It is more robust to any attack on the signal than the Blind watermarks.

4.7 Spread Spectrum Watermarking:

Spread Spectrum watermarking is derived from the communication field and widely used in these days. The main idea of this technique is to spread the data over a large frequency band [8]. It is the whole audible spectrum in the case of audio and it is the whole visible spectrum in case of image. Spread Spectrum is used for navigation and communication [19]

5. APPLICATIONS

Digital watermarking techniques have various applications. Some of them are:

5.1 Copyright Protection:

To identify and protect copyright ownership digital watermarking can be used. Digital content or watermark can be embedded with metadata identifying the copyright owners [7]. This process requires high level of robustness so that the watermark could not be removed without data distortion. Digital watermarking is used to control the redistribution of copyrighted material over the internet.

5.2 Finger Printing:

The concept of fingerprinting is used to identify the real owner of the digital data. Each used has unique identity as fingerprint. Detecting the watermark from any unauthorized user can lead to the identification of that person who leaked the original data.

5.3 Tracking:
To track the digital information over the network digital watermarking can be used. Each copy of the digital data can be uniquely watermarked that specifying the authorized user. These watermarks also used to detect the unauthorized user who replicated the data illegally.

5.4 Broadcast Monitoring:
Watermarking techniques are used to monitor the broadcasting of *TV* channels and radio news. Watermark can be embedded to the commercial advertisement to monitor whether the advertisement is broadcasted. The system receives the broadcast signals and searches for these watermarks to identify where and when the advertisement is broadcast.

5.5 Medical Applications:
To avoiding the ambiguity in searching the medical record watermarking embedded the patient's information as watermark. These watermarks can be visible or invisible. This technique is used by doctors and medical applications to verify that the data or reports are not edited by unauthorized person [14].

5.6 Identity Card/Passport Security:
Digital information like name, address and profile picture can be included in a passport or *ID* card. This information appears on the identity card. The *ID* card can be verified by extracting and comparing the embedded information to the written text. The application can be provide more level of security by including the watermark in it.

5.7 Data Authentication:
Authentication is the process which identifies the content or data. The content received should be exactly same as it was being sent. There should be no editing by unauthorized user in it. For this purpose sender embedded the digital watermark with the digital data. For verification data will be extracted at the receivers end.

5.8 Indexing:
The main information related to the data is embedded as watermark. This watermark information is used by search engines like Google for retrieving the required data without any delay.

5.9 Fraud Detection:
When digital data is used for legal purpose it is important to protect that data from illegal access. At receiver side if any degradation in digital watermark discovers than the document cannot be trusted.

5.10 Copy Control
Illegal copying could not be prevented through proof of ownership as well as watermarks for monitoring, identification and transactional watermarks. The recording and playback devices should a possibility of reacting to embedded signals. Using this if a recording device detects a watermark that indicates recording is prohibited.

6. CONCLUSIONS

It is found that digital watermarking technique is very useful. These techniques provide the domain to enhance images for removing blurriness and to get denoised image. Out of these studied techniques, the *DCT* based spatial and frequency techniques are most commonly used as these methods can provide refined images with less effort and have good signal to noise ratio.

REFERENCES

[1] A. Yadav, and A. Yadav, "Comparison of SVD-Watermarking and LSB-Watermarking Techniques", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue 5, 2014.

[2] C. I. Woo, and S. D. Lee, "Digital Watermarking for Image Tamper Detection using Block-Wise Technique", International Journal of Smart Home, Vol.7, Issue 5, pp.115-124, 2013.

[3] C. Song, S. Sudirman, M. Merabit, and L. Jones, "Analysis of Digital Image Watermark Attacks", IEEE Consumer Communications and Networking Conference (CCNC), 2010.

[4] D. Mistry, " Comparison of Digital Water Marking methods" ,International Journal on Computer Science and Engineering (IJCSE), Vol. 2, 2010.

[5] A. Preeti, S. Kalra, and S. Dhull, "Digital Watermarking", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, 2013.

[6] V. Singh, "Digital Watermarking: A Tutorial", Geethanjali College of Engineering and Technology, Hyderabad India, 2011.

[7] E. Hussein, and M. A. Belal, "Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 7, 2012.

[8] J. Jain, and V. Rai, "Robust Multiple Image Watermarking Based on Spread Transform", Vol. 2, 2012.

[9] M. I. Khan, Md. M. Rahman, and Md. I. H Sarker , "Digital Watermarking for Image Authentication based on Combined DCT, DWT and SVD Transformation" , International Journal of Computer Science Issues, Vol. 10, Issue 3, 2013.

[10] M. Jiansheng, L. Sukang, and T. Xiaomei, "A Digital Watermarking Algorithm based on DCT and DWT", International Symposium on Web Information Systems and Applications Nanchang, China, 2009.

[11] M. Tonge, P. K. Malviya, and A. Gupta, "Implementation of Digital Watermarking Algorithm based on DWT and DCT", International Journal of Advanced Engineering and Global Technology, Vol. 2, Issue 1, 2014.

[12] P. Gupta, "Cryptography based Digital Image Watermarking Algorithm to Increase Security of Watermark Data", International Journal of Scientific & Engineering Research, Vol. 3, Issue 9, 2012.

[13] P. Singh, and R. S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 9, 2013.

[14] R. E. Philip, and M. G. Sumithra, "Development of a New Watermarking Algorithm for Telemedicine Applications", Vol. 3, Issue 1, 2013.

[15] R. V. Totla, and K. S. Bapat, "Comparative Analysis of Watermarking in Digital Images using DCT and DWT", International Journal of Scientific and Research Publications, Vol. 3, Issue 2, 2013.

[16] S. McCloskey, "Hiding Information in Images: An Overview of Watermarking", Cryptography Research Paper ,2000.

[17] V. S. Jabade, and S. R. Gengaje,"Litrature Review of Wavelet Based Digital Watermarking techniques", International Journal of Computer Applications, Vol. 31.

[18] V. Gupta, and Mr. A. Barve "A Review on Image Watermarking and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 1, 2014.

[19] V. Kumar, R. Lautan, M. H. D. Faisal and, K. M. Pandey, "Dwt and Particle Swarm Optimization Based Digital Image Watermarking", International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 9, 2013.