Image Watermarking Techniques for Authenticity: A Review

Rajni Bala[1], Suraj Pal[2]
[1]*M.tech, GCET gurdaspur*
[2]*AP. CSE department, GCET gurdaspur*

Abstract **- Digital watermarking is a highly evolving field, which involves the embedding of a certain kind of information under a digital object (image, video, audio) for the purpose of copyright protection. It is used to verify the authenticity or the identity of its creators. Divergent Image watermarking techniques comprising spatial domain and transform domain have been proposed. In this paper, we survey the diverse techniques, the way they express the watermark and their comparison. This includes a general description of the usage of watermarking and the fundamentals for the different approaches that can be taken when using watermarking.**

Index Terms **- Digital watermarking, Least Significant Bit, Discrete Cosine Transform, Discrete Wavelet Transform.**

1.INTRODUCTION

Digital watermarking is defined as a process of embedding data (watermark), into a multimedia object to help to protect the owner's right to that object. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Digital image watermarking is modification of the original image data by embedding a watermark containing key information such as authentication or copyright codes. Watermark is perceptible or imperceptible identification code which uniquely identifies ownership of an image. It is permanently embedded into the host image. Image watermarking became popular in the 1990s because of the widespread of the Internet. A hidden watermark message is inserted into a host image such that the hidden message will survive intended or unintended attacks. In 1988, Komatsu and Tominaga appear to be the first to use the term "digital watermarking" [1]. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. The information/logo are embedded in image is called a digital image watermark. The information/logo where the watermark is to be embedded is called the *host* image [2, 3]. There are four essential factors those are commonly used to determine quality of watermarking scheme. They are robustness, imperceptibility, capacity, and blindness.

1. Robustness: Watermark should be difficult to remove or destroy. Robust is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, scaling, collision attacks, resizing, cropping etc.
2. Imperceptibility: means quality of host image should not be destroyed by presence of watermark.
3. Capacity: It includes techniques that make it possible to embed majority of information.
4. Blind Watermarking: Extraction of watermark from watermarked image without original image is preferred because sometimes it's impossible to avail original image.

Inseparability and Security are also two main requirement of ideal watermarking [4, 5]. A robust watermark should survive a wide variety of attacks both incidental (Means modifications applied with a purpose other than to destroy the watermark) and malicious (attacks designed specifically to remove or weaken the watermark) [6]. The embedded watermark may be pseudo-random binary sequence, chaotic sequence, spread spectrum sequence or binary/gray scale image and is mainly divided in two categories spatial domain techniques and frequency domain techniques such as DWT and DCT are used for objective embedding watermark and detection using correlation measures.

2 WATERMARKING OVERVIEW

Watermark can be considered as a kind of a signature that reveals the owner of the multimedia object. A watermarking algorithm embeds a visible or invisible watermark in a given multimedia object. The embedding process is guided by use of a secret key which decided the locations within the multimedia object (image) where the watermark would be embedded. Once the watermark is embedded it can experience several attacks because the multimedia object can be digitally processed. The digital image watermarking system essentially consists of a watermark inserter and a watermark detector as shown in figure 1.

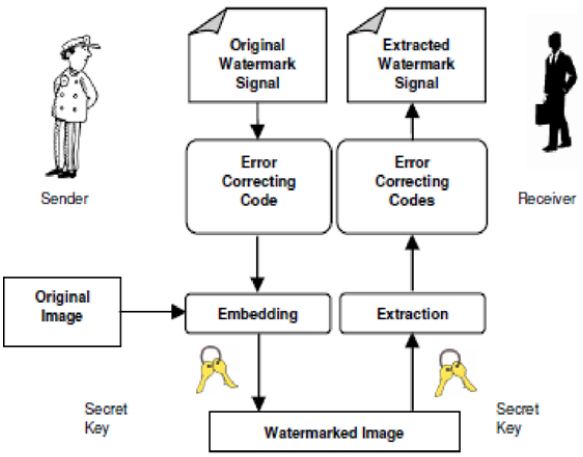

Fig.1 Watermarking Technique

The attacks can be unintentional (in case of images, low pass filtering or gamma correction or compression) or intentional (like cropping). Hence the watermark has to be very robust against all these possible attacks. When the owner wants to check the watermarks in the possibly attacked and distorted multimedia object, s/he relies on the secret key that was used to embed the watermark. Using the secret key, the embedded watermark sequence can be extracted. This extracted watermark may or may not resemble the original watermark because the object might have been attacked. Hence to validate the existence of watermark, either the original object is used to compare and find out the watermark signal (non-blind watermarking) or a correlation measure is used to detect the strength of the watermark signal from the extracted watermark (blind watermarking) [7]. In the correlation based detection the original watermark sequence is compared with the extracted watermark sequence and a statistical correlation test is used to determine the existence of the watermark.

3. TYPES OF WATERMARKING

Various types of watermarking techniques having different applications are given below.

3.1 Inserted Media Category: Watermarking techniques can be categorized on the basis of whether they are used for Text, Image, Audio or Video.

3.2 Robust & Fragile Watermarking: In robust watermarking, the modification to the watermarked content will not affect the watermark whereas fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with.

3.3 Visible & Transparent Watermarking: Visible watermarks are ones, which are embedded in visual content in such a way that they are visible when the content is viewed. Transparent watermarks are imperceptible and they cannot be detected by just viewing the digital content.

3.4 Public & Private Watermarking: In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not authorized to detect the watermark.

3.5 Asymmetric & Symmetric Watermarking: Asymmetric is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking the same keys are used for embedding and detecting watermarks.

4. WATERMARKING ATTACKS

A robust watermark should survive a wide variety of attacks both incidental (modifications applied with a purpose other than to destroy the watermark) and malicious (designed to remove or weaken the watermark) [8, 6]. We categorize the attacks as:

4.1 Simple attacks: Simple or waveform or noise attacks are conceptually simple attacks that attempt to impair the embedded watermark by manipulations of the whole watermarked data (host data plus watermark) without an attempt to identify and isolate the watermark. Examples include filtering, compression (JPEG, MPEG), and addition of noise, addition of an offset, cropping, Digital to analog and analog to digital conversion.

4.2 Detection-disabling attacks: Detection-disabling or synchronization attacks are attacks that attempt to

break the correlation and to make the recovery of the watermark impossible or infeasible for a watermark detector, mostly by geometric distortion like zooming, shift in (for video) direction, rotation, cropping, pixel permutations, sub-sampling, removal or insertion of pixels or pixel clusters, or any other geometric transformation of the data.

4.3 Ambiguity attacks: Ambiguity or deadlock attacks are attacks that attempt to confuse by producing fake original data or fake watermarked data. An example is an inversion attack that attempts to discredit the authority of the watermark by embedding one or several additional watermarks such that it is unclear which the first, authoritative watermark was.

4.4 Removal attacks: Removal attacks are attacks that attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only the watermark. Examples are collusion attacks, denoising, certain filter operations, or compression attacks using synthetic modeling of the image.

5. CLASSIFICATION OF DIGITAL IMAGE WATERMARKING TECHNIQUES

There are various technique used to hidden message/logo in images and are classified as

5.1 Least Significant Bit Modification

The simpler method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object [9]. LSB substitution however has lots of drawbacks. Any addition of noise or lossy compression is likely to defeat the watermark. If we simply set the LSB bits of each pixel to one the watermark obsolete with negligible impact on the cover object. An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key [9].

Security of the watermark would be improved as the watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant.

Pixel Value of Image:	11001010	00110101	00011010	00000000
Watermark:	1	1	1	0 ...
Watermarked Image:	11001011	00110101	00011011	00000000

5.2 Frequency Domain Techniques

Here we can embed watermark in DCT, DFT, FFT domains etc. The main strength offered by transform domain techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions. The benefit is two-fold; Degradation in smoother regions of an image is more noticeable to the HVS, and becomes a prime target for lossy compression schemes. Taking these aspects into consideration, working in a frequency domain of some sort becomes very attractive. The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies ($F_{M)}$ of an 8x8 DCT block as shown below in figure 2.

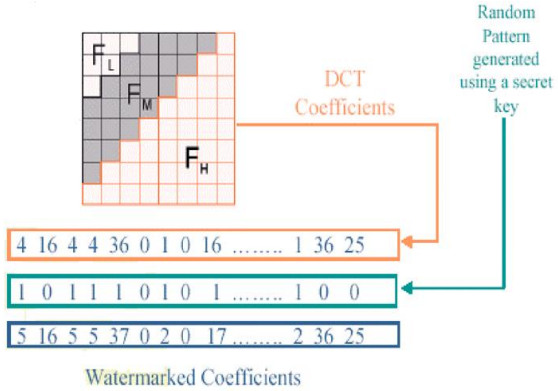

Figure 2 - Definition of DCT Regions

F_L is used to denote the lowest frequency components of the block, while F_H is used to denote the higher frequency components. F_M is chosen as the embedding region as to provide additional resistance to lossy

compression techniques, while avoiding significant modification of the cover image [10].

5.3 Wavelet Watermarking Techniques

Another possible domain for watermark embedding is that of the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in figure 1.3.

EMBED CorelDRAW.Graphic.10

Figure 1.3: 2 Scale 2-Dimensional Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. One of the most straightforward techniques is to use a similar embedding technique to that used in the DCT, the embedding of a CDMA sequence in the detail bands according to the equation 1.5.

$$I_{W\,u,v} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases} \quad (1)$$

where w_i denotes the coefficient of the transformed image, x_i the bit of the watermark to be embedded, and α a scaling factor. To detect the watermark we generate the same pseudo-random sequence used in CDMA generation and determine its correlation with the two transformed detail bands. If the correlation exceeds some threshold T, the watermark is detected. This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for each PN sequence, which is then added to the detail coefficients as per equation 1.5. During detection, if the correlation exceeds T for a particular sequence a "1" is recovered; otherwise a zero. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered. Furthermore, as the embedding uses the values of the transformed value in embedded, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients. The author [11] claims that the technique should prove resistant to JPEG compression, cropping, and other typical attacks.

CONCLUSION

We survey and review number of techniques for the watermarking of digital images, as well as compares their limitations and possibilities. We give the brief description of digital image watermarking and it was still enough to draw several conclusions about digital watermarking. LSB substitution is the simplest technique but not a very good candidate for digital watermarking due to its lack of robustness. LSB embedded watermarks can easily be removed or altered without degrade the image quality. It would appear that LSB will remain in watermarking due to its tremendous information capacity. Most of the distortion-based watermarking techniques mainly aim at protecting the ownership, whereas distortion-free watermarking techniques mostly are fragile and aim at maintaining integrity.

REFERENCE

[1] Frank Hartung, Martin Kutter, "Multimedia Watermarking Techniques", Proceedings of The IEEE, Vol. 87, No. 7, pp. 1085 – 1103, July 1999.

[2] "Digital Watermarking" available at http: //en.wikipedia.org/wiki/Digital_watermarking

[3] Alper Koz, "Digital Watermarking Based on Human Visual System", The Graduate School of Natural and Applied Sciences, The Middle East Technical University, pp 2 – 8, Sep 2002.

[4] J.J.K.O. Ruanaidh, W.J.Dowling, F.M. Boland, "Watermarking Digital Images for Copyright Protection", in IEE ProcVis. Image Signal Process, Vol. 143, No. 4, pp 250 - 254. August 1996.

[5] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" submitted at University Salzburg, pp. 9 – 17, Jan 2000.

[6] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidis, "A SURVEY ON WATERMARKING APPLICATION SCENARIOS AND RELATED ATTACKS", IEEE international Conference on Image Processing, Vol. 3, pp. 991 – 993, Oct. 2001.

[7] Saraju Prasad Mohanty, "Watermarking of Digital Images", Submitted at Indian Institute of Science Bangalore, pp. 1.3 – 1.6, January 1999.

[8] N.F. Johnson, S.C. Katezenbeisser, "A Survey of Steganographic Techniques" in *Information Techniques for Steganography and Digital Watermarking*, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75

[9] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000.

[10] J.R. Hernandez, M.Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure", in IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000.

[11] H. Inoue, A. Miyazaki, T. Katsura "An Image Watermarking Method Based on the Wavelet Transform", Kyushu Multimedia System Research Laboratory.