RESEARCH ARTICLE OPEN ACCESS

Embedding Useful Information in Digital Watermarking: A Review

*Ruchi Kashyap, **Mr. Karan Mahajan
*Department of Information Technology, Chandigarh group of College, Landran, Mohali
**Department of Information Technology, Chandigarh group of College, Landran, Mohali

Abstract
Nowadays watermarking is being used to protect multimedia in digital technology. Embedding the data is known as watermark. On the internet where various images available are being used as watermarks. Digital watermarking is a process in which different types of information is being combined into a digital signal. Watermarking techniques ensures two main factors integrity and robustness of data. A number of watermarking techniques such as DFT, DCT etc. are discussed in this paper.
Keywords: watermark, DCT, DFT, DWT

I. INTRODUCTION

With the widen use of internet, digital media are widely used. Digital media are easily and illegally destroyed, copied and change. So there is a need of transmitting the data securely and confidentially and for this we need an effective data hiding scheme. This is where watermarking system comes in existence. Digital Watermarking is the technique which allows an owner to add hidden copyright notices, image, and signature, audio, video or other messages to digital media. If the media is copied by unauthorized user, then the information embedded in digital media is also carried in the copy. Image watermarking means to embed visible or invisible information in to image that identify the genuine owner.

Watermarking is a widely used technique to embed information in an image. However, the main purpose is to provide authentication and establishing the true ownership of an image [1]. Digital watermarking is a new technology used for copyright protection of digital media.

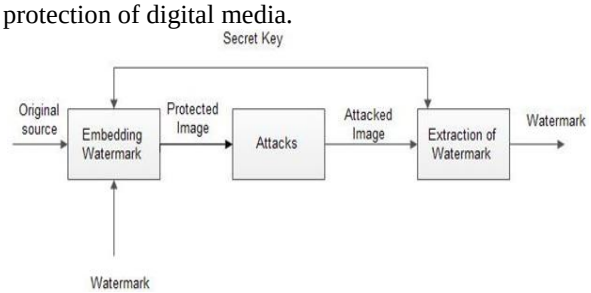

Fig 1.Block diagram of watermarking system

This paper is organized as follows. Section II describes properties of digital watermarking. Section III focuses on Application of watermarking. Section IV explains the types of digital watermarking. Section V presents various limitations of watermarking. Section VI represents conclusion.

II. PROPERTIES OF DIGITAL WATERMARKING

The main Properties of digital watermarking are [6][10]

- **Robustness**:

Watermarks could be removed intentionally or unintentionally by simple image process in operations like contrast or improvement in brightness. Hence robust watermarks should be robust against variety of such attacks. For robustness we can also add watermark at more than one position in the image, if one or two are removed then the other is there.

- **Invisibility**

An embedded watermark is not noticeable. Content consist of invisible watermark that is hidden in it. Authorized party can only detect this hidden watermark. Therefore Such watermarks are used for author authentication and for detecting unauthorized copier.

- **Computational Complexity**

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.

- **Data Payload**

Data payload is also known as capacity of watermarking. 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.

- **Transparency or Fidelity**

The digital watermark should not affect the quality of the original image after it is watermarked. Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

- **Security**

A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized agencies. Security is the main requirement and the and the watermark is usually achieved by the use of more alphabet keys.

III. DIGITAL WATERMARKING APPLICATIONS

There are many application of digital watermarking as following:

i. Copyright Protection.

Digital watermark embedded within the host signal can be retrieved later to assert the owner's copyright over the marked media. [2]. Ownership of digital media can be verified in the case of a copyright dispute by using the embedded data as a proof. The requirements on the watermark for this purpose are that the watermark be robust and be tolerant to malicious and unintentional attacks on the watermarked image. [1]

ii. Authentication

Fragile watermarks could be used to detect and highlight unauthorized modification to the protected data. These are weak watermarks and are designed to be destroyed in case of alteration of the marked data in an unauthorized manner [2]

iii. Fingerprinting

The owner of a digital content can choose to embed distinct watermarks within the content supplied to different customers. This method helps in identifying the customers that break license agreements by supplying the content illegally to unauthorized parties. Prevention of unauthorized copying is accomplished by embedding information about how often an image can be legally copied [3].

IV. TYPES OF DIGITAL WATERMARK

A. According to the human perception,

The digital watermarks can be dividing into three different types as follows. [4]

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

1. Visible

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. It should be visible to a casual viewer on a careful inspection.

2. Invisible-robust

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.

3. Invisible-fragile

Watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

4. Dual watermark

Is a combination of an invisible and a visible watermark. In this type an invisible watermark is used as a backup for the visible watermark as clear from the following diagram

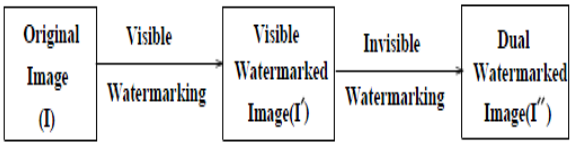

Figure 2: Schematic representation of dual watermarking

1. Image Watermarking [5]

Many techniques have been developed for the watermarking of still image data. For grey-level or for color-image various embedding watermark techniques are created to insert the watermark directly into the original image data. Requirements for image watermarking include imperceptibility, robustness to common signal processing operations, and capacity. Common signal processing operations which the watermark should survive include compression (example JPEG), filtering, rescaling, cropping, A/D and D/A conversion, geometric distortions, and additive noise. Capacity refers to the amount of information (or payload) that can be hidden in the host image and detected reliably under normal operating conditions. Some examples of watermark information include a binary sequence representing a serial number(credit card), a symbol, an image, or a trademark.

- **DCT Domain Watermarking**

DCT based watermarking techniques are more robust as compared to spatial domain watermarking techniques this algorithm is robust against simple image processing operations. However, they are difficult to implement and are computationally more costly. And also they are weak against geometric attacks like scaling, rotation and cropping etc. [6].A common transform framework for images is the block-based DCT which is a fundamental building block of current image coding standards such as JPEG. The DCT is performed on 8×8 blocks of data. [5]. Apply forward DCT to each of these blocks and apply some block selection criteria (e.g. HVS) Apply coefficient selection criteria (e.g. highest) Embed watermark by modifying the selected coefficients are then modified and watermark embedded. On each block inverse DCT transform is applied [7].

- **DWT Domain Watermarking**

DWT based watermarking schemes use the same guidelines as DCT based schemes, i.e., concept is the equal despite, image transformation process into its transform domain varies and hence the resulting coefficients are different.[6] Wavelet transforms use wavelet filters like Haar Wavelet Filter, Daubechies Orthogonal Filters and Daubechies Bi-Orthogonal Filters to transform the image. Each of these filters decomposes the image into several frequencies. Decomposition of single level gives four frequency representations of an image like LL, LH, HL, HH sub bands.[7].DFT and DCT are full frame transform, and hence any change in the coefficients transform affects the entire image except if block based approach is implemented using DCT. However DWT has dimensional locality property, which means if signal or watermark is embedded it will affect the image narrowly. Hence a wavelet transform contributes both frequency and spatial information for an image.

- **DFT Domain Watermarking**

DFT domain has been studied by researches because it provides robustness against geometric attacks like scaling, cropping, rotation, translation etc. [6] there are two different kinds of DFT based embedding watermark techniques. Firstly watermark is directly embedded and another one is template based embedding. In direct embedding watermark is embedded by modifying the phase information within the DFT. A template is a structure which is embedded in the DFT domain to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, and then use the detector to extract the embedded spread spectrum Watermark [7].

2. Video Watermarking

I.J.Coxetal.algorithm also works for video if watermarking is done frame wise. [8]. Video watermarking applications can be grouped as security related like, fingerprinting, ownership identification, authentication, or value added applications like estate system enrichment, database linking, video affixing, digital video broadcast monitoring[2].Existing video watermarking techniques are divided into different categories

- **Spatial Domain Watermarking**

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image/video directly. Low computational complexities and simplicity are the main strengths of pixel domain methods.[9] Basically it embeds a watermark pattern W in the spatial domain by changing intensity values to guarantee robustness against color conversions. If the spatial correlation value Co exceeds a certain threshold τ, the watermark is detected otherwise no watermark. This allows the embedding of one-bit pay load. [7]

3. Audio Watermarking

Many of the requirements for audio watermarking are similar to image watermarking, such as imperceptibility (noiseless), robustness to signal variation such as compression, filtering, and A/D and D/A conversion.[5] The amount of data that can be embedded into audio is considerably low than amount that can be hidden in images, as audio signal has a dimension less than two-dimensional image files. Embedding additional information into audio sequence is a more tedious than images, due to dynamic supremacy of HAS than HVS. [7] propose three techniques for audio watermarking—a spread spectrum technique, replica method, and phase coding.

- **Phase coding**

The main idea is to divide the original audio stream into blocks and embed the whole watermark data sequence into the phase spectrum of the first block.

- **Spread-Spectrum Method**

This scheme spreads pseudo-random sequence across the audio signal. The noise of wideband can be spread into either time-domain signal or transform domain signal. Frequently used transforms include DCT, DFT, and DWT.

- **Replica Method**

Original signal can be used as an audio watermark. Echo hiding is a good example. Replica modulation also embeds part of the original signal in frequency domain as a watermark.

Echo Hiding

Echo hiding embed data into an original audio signal by introducing an echo in the time domain

4. Text/document Watermarking [5][7]

Most of this work is based on hiding the watermark information into the layout and formatting of the document directly. Various techniques are focused on watermarking the binary-valued text regions of a document. Detection of watermark consists of post processing steps to try to remove noise. These techniques are quite effective against some common attacks such as multigenerational photocopying

- **Spread Spectrum Watermarking**

Watermark bits are mixed with PRN (Pseudorandom Noise) generated signal and then this signal is inserted in the host signal. This PRN signal functions as a secret key. This specific PRN signal can later on be detected by correlation receiver or match filter.

- **Line-Shift Coding**

Here each even line is slightly shifted up or down according to the bit value in the payload. If the bit is one, the corresponding line is shifted up; otherwise, the line is shifted down. The odd lines are considered as control lines and used at decoding.

- **Word-Shift Coding**

Here each line is first divided into groups of words. Each group has a sufficient number of characters. Then, every even group is shifted towards left or the right according to the bit value in the payload.

- **Feature Coding**

In this method, certain text features (e.g., vertical end lines) are altered in a specific way to encode the zeros and ones of the payloads. Watermark detection is achieved by comparing the original document with the watermarked document

V. LIMITATIONS OF DIGITAL IMAGE WATERMARKING

Here w**e** discuss the various technical issues related to watermarking, such as properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful.

1. Properties of visual signal

Since image and videos are visual signals, it is essential to understand the nature of visual signals in order to find ways to hide additional information in them. These waveforms reveal a lot of information about the visual signals properties. Following are some properties of visual signals are:-

- **Nonstationarity**

Nonstationarity property is common to all signals. Image and video signals contain a property of segments of flat or slowly changing intensity, as well as edges and balance regions. Preservation of the edges need to be maintained emotive quality, the balance regions need to be judiciously used to store additional information.

- **Periodicity**

There exists line to line and frame to frame periodicity in image and image signals. They are not exactly regular but there exists redundancy between lines and frames. These repetitions are overworked in any compression scheme, and need to be considered during the watermarking process.

2. Properties of the Human Visual System (HVS)

The success of any watermarking scheme lies in making the best use of the human visual system (HVS). In this section, we discuss the various properties of the human visual system which are exploited in designing watermarking algorithms.

- **Texture Sensitivity**

The visibility of distortion depends on the texture background. When the background has a strong texture texture then based visibility is low. In a highly image block that is textured, energy aims to be more evenly distributed among the `different coefficients of DCT. The image having a flat-featured portion of the image the energy is concentrated in the low frequency spectrum components. This shows that regions having strong texture more watermark signal can be added.

- **Brightness Sensitivity**

The human eye is sensitive in observing a low intensity signal in the presence of backgrounds of different intensity. As the surrounding region intensity is reduced and the sensitivity in the light areas is increased. Eye has high sensitivity at low intensity levels and greatly reduced sensitivity at high intensity levels.

VI. CONCLUSION

The purpose of this paper is to present a review of digital image watermarking approaches. The process of watermarking is studied in a detailed fashion in this paper. A detailed study of all the watermarking techniques and their implementation is also being done in this paper. Also we study about watermarking properties, application and its limitations. It is concluded that digital watermarking

technique is very impressive and effective for authentication and protection from various attacks.

REFERNCES

[1] Sunil Mohan AdapaJayanthiSivaswamy, "*Useful Information Embedding in Images Using Watermarks*", International Institute of International Institute of Information Technology, Hyderabad Information Technology, Hyderabad.

[2] AbduljabbarShaamala, "*Study of the effected genetic watermarking Robustness under dct and dwt domains"*, International journal on new computer architectures and their applications (ijncaa) 2(2): 353-360the society of digital information and wireless communications, 2012 (ISSN: 2220-9085).

[3] Keshav S Rawatet. al. / Indian Journal of Computer Science and Engineering Digital watermarking scheme for authorization against copying or piracy of color image volume.1 No. 4 295-300.

[4] Saraju P. Mohanty, "*Digital Watermarking: A Tutorial Review",* Dept of Comp Sc&Eng.Unversity of South Florida.

[5] Christine I. Podilchuk and Edward J. Delp "*Digital Watermarking: algorithm and application",*Ieee Signal Processing Magazine, July 2001.

[6] Vinita Gupta, "*A Review on Image Watermarking and Its Techniques*", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, January 2014 ISSN: 2277 128X.

[7] L. Robert, "*A Study on Digital Watermarking Techniques*", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[8] I.J Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "*Secure spread spectrum watermarking for multimedia*" in IEEE Transactions on Image Processing, vol. 6, no. 12, Dec.1997, pp:1673 -1687.

[9] Gopika V Mane," *Review Paper on Video Watermarking Techniques* ", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153

[10] Gaurav N Mehta," *Digital Image Watermarking: A Review*", International Journal of Scientific Engineering and Technology (ISSN: 2277-1581) www.ijset.com, Volume No.1, Issue No pg: 169-174 01 April 2012.