Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 4, April -2015

Digital Watermarking Techniques: A Survey

Khushbu Sahu[1] and Utkarsh Sharma[2]

[1]Department of Electronics & Telecommunication, Shri Shankaracharya Technical Campus
[2]Department of Electronics & Telecommunication, Shri Shankaracharya Technical Campus

Abstract — *In today's situation because the technology is advancing, therefore exponentially threats of cyber crimes are also increasing. So, to protect our contents from these threats we'd like Digital watermarking. Here, we are going to study concerning the Digital Watermarking. We are going to watermark a color image into a host image. For color digital image a multipurpose blind watermarking algorithm based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) is projected in maintenance with the need of multipurpose blind watermarking algorithm. The most important objective is to be told regarding different kinds of watermarking techniques, which may be utilized in day-after-day lives. In today's scenario because the technology is advancing with time, therefore exponentially threats of cyber crimes are also increasing alarmingly. So, to protect our contents from these threats we'd like Digital watermarking. Digital watermarking applications are copyright protection, authentication and security.*

Keywords- *Discrete cosine transform, Digital watermarking, Discrete wavelet transform, Multi-purpose blind watermarking algorithm.*

I. INTRODUCTION

Digital watermarking is a technique which allows to insert the secreted copyright notices or other confirmation messages to digital image, audio and video signals and documents. A digital watermarking is defined as a logically marker which secretly fixed during a noise-tolerant signal like audio, image or visual information and is typically used to recognize rights of the copyright of the signal.

"Watermarking" is the process of hiding digital data in the original data; the secreted data does not need to link to the original data. Digital watermarks might be used to substantiate the authenticity of the original data and it is significantly used for tracing copyright infringements and for banknote authentication. Properties of a digital watermark depend on the use case in which it is applied [1]. After modification, a digital watermark has to be robust to the carrier signal for copyright information of the multimedia files [2].

A visible or noticeable "seal" to be found above an image to spot the copyright is an example of a digital watermark. Though the watermark might have some extra information including the characteristics of the consumer of a particular duplicate of the material. A multipurpose blind watermarking algorithm for color digital image based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) is projected in keeping with the lack of multipurpose blind watermarking algorithm.

II. CLASSIFICATION OF WATERMARK ALGORITHMS

Classification of watermarking algorithms specializing in the domain during which watermark information is embedded.

2.1 Taxonomy of Watermarking

The different classifications of digital watermark algorithms are:-

First, watermark techniques will be divided into four groups consistent with the kind of data to be watermarked:

- Text Watermarking.
- Image Watermarking.
- Video Watermarking.
- Audio Watermarking.

Second, supported human perception, watermark algorithms are divided into 2 categories:

- Visible watermarking.
- Invisible watermarking.

Visibility is related to perception of the human eye thus if the watermark is embedded within the info in the manner that may be seen without extraction, we've a tendency to call the watermark visible. Samples of visible watermarks are logos that are utilized in the video and pictures [3]. On the opposite hand, an invisible watermarking can't be seen by the eye of person. Thus it is embedded it is data without affecting the content and might be extracted by the

owner or the one that has right for that.

2.2 Watermarking Algorithm Based on Detection

Watermark algorithms classifications based on information for detection are:

- Blind or Public Watermarking: - In public watermarking, there\'s no need for original signal throughout the detection process to detect the watermark. Only the key is needed. For instance, in image blind watermarking we tend to don't want the original image.
- Non-Blind or private Watermarking: - original signal is needed for detection of the watermark image in the non blind or private watermarking [4].
- Semi-Blind watermarking: - there is a requirement of the admittance to the 'published' watermarked signal, in several watermarking techniques after adding the watermark i.e. the original signal. This technique is termed as semi-blind watermarking technique.

Watermark algorithms classification supported processing-domain are: -

- Spatial Domain: - A watermark technique based on the spatial domain, spread watermark data to be embedded within the pixel value. These approaches use minor changes within the pixel value intensity [3]. The best example is to embed within the least significant bits (LSB) of image pixels in the watermarking image. In alternative words, important parts of low frequency components of images ought to be changed so as to insert the watermark data in a very reliable and robust way. As another example, an image is split into a similar size of blocks and a definite watermark data is added with the sub-blocks.
- Transform domain: - During this methodology, transform coefficients are changed for embedding the watermark. Transform domain is also known as frequency domain as a result of values of frequency is altered from their original. The prime necessary techniques in transform domain are discrete cosine transform (DCT) and discrete wavelet transform (DWT).

2.3 Watermarking Algorithm Based on Robustness

Additionally, classification is based on the robustness feature. Different techniques of this category are as follows:

- Robust Watermark: - We call a watermark algorithm robust if it will survive when common signal processing operations like filtering and lossy compression [5].
- Fragile Watermark: - A fragile watermark ought to be able to be detected when any modification in signal and additionally possible to identify the signal before modification and is used for the verification or authenticity of original content.
- Semi-Fragile Watermark: - Semi-fragile watermark is sensitive to a point of the change to a watermarked image. Moreover, from application purpose of view, watermark techniques are classified as source based or destination based. In source based, all copies of a selected data have a unique watermark, which identifies the owner of that data, whereas in the destination based; every distributed copy is embedded using a unique watermark data, which identifies a selected destination.

2.4 Types of watermarking Techniques

2.4.1 Spatial Domain Techniques

- Least-Significant Bit (LSB)
- SSM-Modulation-Based Technique

2.4.2 Frequency Domain Techniques

- Discrete Cosine Transformation (DCT)
- Discrete Wavelet Transformation (DWT)

2.4.1 Spatial Domain Techniques

Spatial Techniques of watermarking are as follows:

- Least-Significant Bit (LSB): - The earliest work of digital image watermarking schemes embeds watermarks within the LSB of the pixels. Given an image with pixels, and every pixel being represented by an 8-bit

sequence, the watermarks are embedded within the last (i.e., least significant bit), of chosen pixels of the image [6]. This technique is straightforward to implement and doesn't generate serious distortion to the image; but, it's not terribly strong against attacks. For example, an attacker may merely disarrange all LSBs, which effectively destroy the hidden info.

- SSM-Modulation-Based Technique: - Spread-spectrum techniques are strategies within which energy generated at one or a lot of discrete frequencies is deliberately spread or distributed in time or frequency domains. Once applied to the context of image watermarking, SSM based mostly watermarking algorithms embed info by linearly combining the host image with a little pseudo noise signal that\'s modulated by the embedded watermark.

2.4.2 Frequency Domain Techniques

- Frequency-domain techniques are most widely used as Compared to spatial-domain techniques. The aim is to introduce the watermarks within the spectral coefficients of the image. Discrete wavelet transform (DWT), discrete cosine transform (DCT), discrete Fourier transform (DFT),discrete Hadamard transform (DHT), discrete Laguerre transform (DLT) are the commonly used frequency domain transforms [7]. The uniqueness of the human visual system (HVS) are higher captured by the spectral coefficients is the reason for watermarking within the frequency domain. For example, the HVS is low sensitive to high-frequency coefficients and is more sensitive to low-frequency coefficients [6]. In alternative words, low-frequency coefficients are perceptually important, which suggests alterations to those components may cause severe distortion to the original image [8]. On the opposite hand, high-frequency coefficients are considered insignificant; so, process techniques, like compression, tend to get rid of high-frequency coefficients aggressively. To get a balance between imperceptibility and robustness, most algorithms embed watermarks within the midrange frequencies [6].

- Discrete cosine transformation (DCT):- DCT like a Fourier Transform, instead of an amplitude space it represents data in terms of frequency space. DCT primarily based watermarking techniques are robust compared to spatial domain techniques. This can be helpful because that corresponds a lot of to the way humans understand light, in order that the part that don\'t seem to be perceived will be known and thrown away. Such algorithms are robust against simple image process operations like low pass filtering, contrast and brightness adjustment, blurring etc. However, they\'re tough to implement and are computationally costlier. At the same time they\'re weak against geometric attacks like cropping, rotation, scaling etc. DCT domain watermarking will be classified into global DCT watermarking and Block primarily based DCT watermarking. Embedding within the perceptually good portion of the image has its own benefits as a result of most compression schemes remove the perceptually insignificant portion of the image.

Discrete wavelet transformation (DWT):- A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. The Discrete wavelet Transform (DWT) is presently utilized in a good form of signal process applications, like in video and audio compression, removal of noise in audio, and also the simulation of wireless antenna distribution. Wavelets have their energy focused in time and are well suited for the analysis of time-varying signals. Most of the real life signals encountered are time varying in nature, the wavelet transform suits several applications alright.

III. DIGITAL WATERMARKING LIFE CYCLE PHASES

The information to be embedded in a signal is named a digital watermark, though in some contexts the phrase digital watermark means the distinction between the watermarked signal and the signal. The signal wherever the watermark is to be embedded is named the host signal.

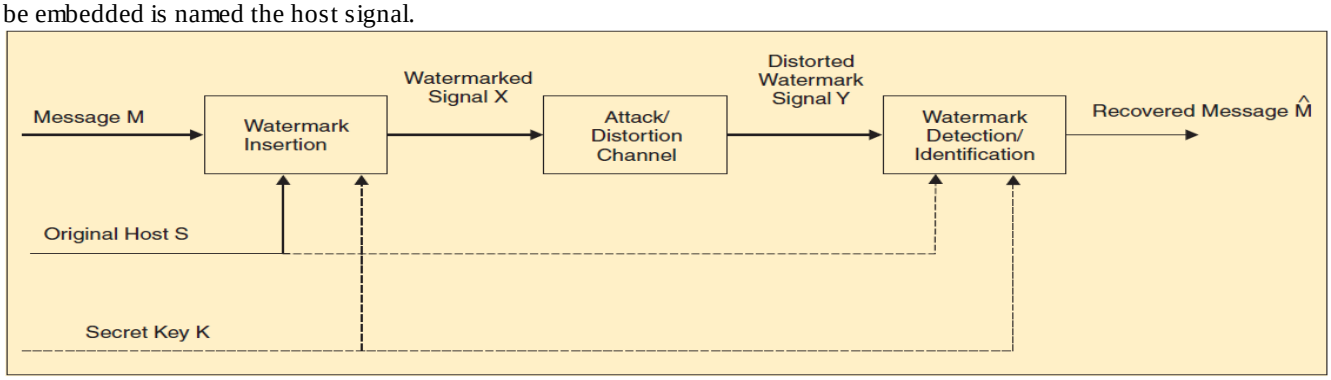

Figure 1. Block diagram of a watermarking system.

3.1 Watermarking system:-

A watermarking system is usually divided into three distinct steps :

- Embedding
- Attack
- Detection/Extraction

3.1.1 Embedding: -

In embedding, an algorithm accepts the host and therefore the data to be embedded, and produces a signal which is watermarked. Inputs to the system are the watermark, the cover data and non-mandatory public or secret key. The outputs are watermarked data. The secret is used to enforce security.

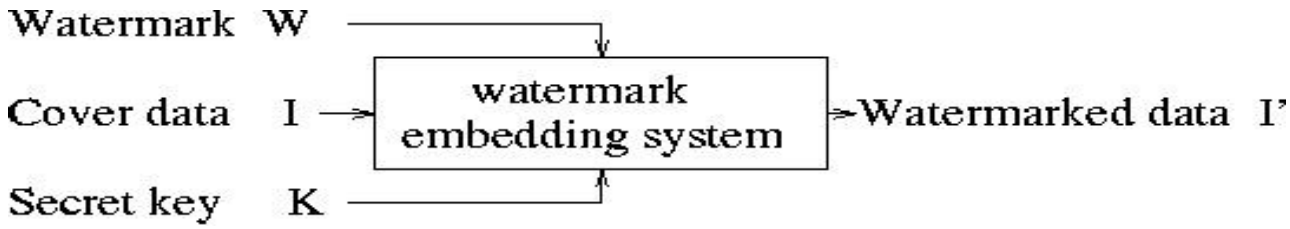

Figure 2. Embedding

3.1.2 Attacks: -

The watermarked digital signal is transmitted to a different person. If this person makes a modification, this can be referred to as attack. Whereas the modification might not be malicious, the term attack emerges from copyright protection application, wherever pirates plan to remove the digital watermark through modification. There are several modifications, as an example, lossy compression of the data, cropping a picture or video, by choice adding noise.

3.1.3 Extraction: -

Extraction algorithm is applied to the attacked signal to extract the watermark from it. If the signal was unmodified throughout transmission, then the watermark in the image still is present and it should be extracted.

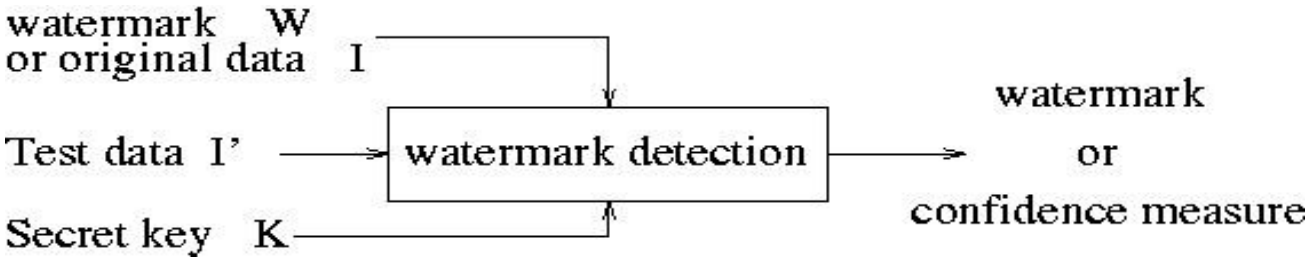

Figure 3. Extraction

Inputs to the scheme are the watermarked data, the secret or public key and, counting on depending on, the original information and/or data watermark. The output is that the recovered watermarked W or some reasonably confidence measure indicating however seemingly it\'s for the given watermark at the input to be present within the data below under.

IV. CONCLUSION

In this review paper we surveyed DWT-based watermarking methods are quick and robust and so, will be protected against varied manipulations. Simulation results prove that the functions of copyright protection and content authentication will be enforced. However the ability of the watermarks in resisting the JPEG compression and therefore the attacks isn't too strong.

This study described here measured the robustness of the available transform domain watermarking algorithms against major attacks [9]. These attacks are aimed to destroy the watermark data within the image. There are different attacks like brutal force attacks that attempt to notice and extract watermark data from the image. Our study will be extended to incorporate those attacks and measure to include the algorithms against them. The robustness of a watermarking technique depends on wherever the watermark is embedded. As totally completely different images have different frequency contents, the robustness also will be dependent on the kind of the image.

REFERENCES

[1] Charu Kavadia, Vishal Shrivastava, "A literature review on water marking techniques", International Journal of Scientific Engineering and Technology, vol. 1 No. 4, pp. 08-11, 2012.

[2] Prof. Dr. K. N. Barbole, Prof. S.D. Satav, "Security for watermark image, International Journal of Management & Information Technology", vol. 3. No. 1, pp. 77-82, 2013.

[3] Reena, Mrs. Vandana, "Modified approach of digital image watermarking using combined DCT and DWT", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3 No.7, pp. 429-435, 2013.

[4] Roma Rewani, Mahendra Kumar, Aditya Kumar Singh Pundir, "Digital image watermarking: A Survey", International Journal of Engineering Research and Applications, vol. 3 No.4, pp. 1750-1753, 2013.

[5] Mitra Abbasfard, "Digital Image Watermarking Robustness: A Comparative Study", Delft University of Technology, The Netherlands, 2009.

[6] Shilpa Kharpate, Himanshu Yadav, Anurag Jain, "A Review of Watermarking Scheme for Confidential Image", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4 No.12, pp. 176-180, 2014.

[7] Priyanka N. Kale, Prof. K. M. Pimple, "Information hiding technique: digital watermarking", International journal of pure and applied research in engineering and technology, vol. 2 No.9, pp.1117-1124, 2014.

[8] Keshav S Rawat, Member, IEEE, Dheerendra S Tomar, Member, IEEE, "Digital watermarking schemes for authorization against copying or piracy of color images", Indian Journal of Computer Science and Engineering, vol. 1 No.4, pp. 295-300.

[9] Omer Siddik, "Radon transform based robust non-blind watermarking", Cankaya University, Graduate School Of Natural And Applied Sciences Mathematics And Computer Science, 2013.

