Review Article

Digital Watermarking Techniques

Kaynat Anjum[1], Prof. Jayesh Jain[2]

[1,2]Baderia Global Institute of Engineering and Management, INDIA

ABSTRACT

"Watermarking" refers to the process of inserting digital data into a carrier signal. Carrier signals can be checked for forgery or corruption with the help of digital watermarks, and the identities of the signal's owners can be revealed. You might think of a watermark as a tag or proof of ownership. A watermark serves to safeguard the original image by superimposing a secondary image over it. It's becoming increasingly clear that digital watermarking is crucial in the new internet-based society. Protection of intellectual property, detection of tampering, tracking of broadcasts, authentication, integrity, and verification are only few of the uses for digital watermarking. Digital watermarking in image processing makes use of numerous techniques. This paper provides an overview of the many watermarking systems now in use, as well as a discussion of their advantages and disadvantages.

KEYWORDS

Digital watermarking, Spatial Domain Techniques, Frequency Domain Techniques, Least significant Bit, SSM Modulation, Discrete Cosine Transform, Discrete Wavelet Transformation, Discrete Fourier Transform

1. INTRODUCTION

In order to prevent alterations or misuse of digital photographs, watermarking technology has been developed [2]. The primary purpose of watermarking is to add an extra layer of protection to various media files (audio, video, image, etc.). The phrase "watermarking" [2] refers to the practice of adding a hidden or overt message to a host signal in the form of a number, text, or graphic. It is imperative that the security of data communications over the internet be improved as e-commerce applications are developed for the World Wide Web today [1]. Data encryption and other methods of masking information were utilized to make online communication more secure. For secure, unaltered data/image transfer, many techniques exist, including cryptography, watermarking, and steganography [1]. A watermark is an additional image superimposed on the primary image for security purposes. Data encryption and decryption via cryptography ensures that only the intended recipient may read the encrypted message.

Only through the processes of encryption and decryption can cryptography guarantee safety. Watermarking, on the other hand, protects content even after encryption has been decrypted [1]. Copyright information can be embedded in digital media files using a process called watermarking [1]. Therefore, the data is safe with watermarking. The user can decode a watermarked image by employing the same method that was used to embed the watermark in the image. The computer science discipline is rapidly expanding, and digital image processing is one of the fastest-growing subfields. Multiple advantages of digital image processing over analogue methods have been identified [4]. Pixels, which are the discrete units of digital representation, are used to accurately depict 2-dimensional representations in digital images. Therefore, processing a picture on a digital computer is known as digital image processing [4]. This is an example of how digital image processing can be put to use: digital watermarking. The term "information concealment" describes this phenomenon. For purposes such as authentication, owner identification, and content protection, digital watermarking incorporates hidden and supplementary information into the original image.

and other forms of copyright protection, Digital Fingerprinting [4], Transaction Tracking [4], and so on [4]. The usage of digital watermarks helps to keep digital files safe from prying eyes. Digital watermarking is undetectable and resilient against several attacks. The effectiveness of watermarking algorithms relies on the embedded watermark's resilience to a variety of attacks [4]. In addition to its use in many well-established applications, digital watermarking is a promising new area of study. Several methods of image processing make extensive use of digital watermarking. All these programmes have the same overarching goal: to keep our digital data safe [4].

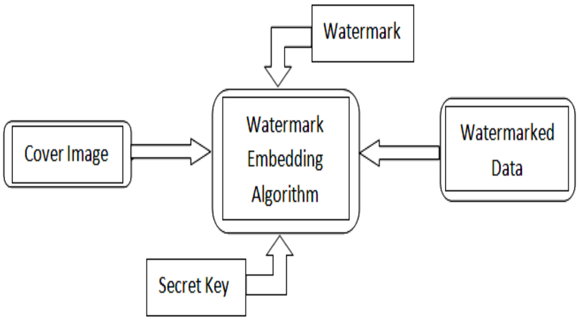

Fig 1: Watermark Embedding [4]

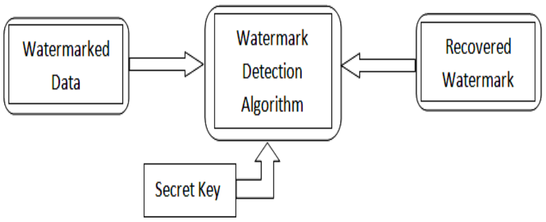

Fig 2: Watermark Detection [4]

Digital watermarking process includes two algorithms: First is embedding algorithm and second is the detecting algorithm. Figure 1 represents watermark embedding process-in which watermark is embedded into the cover image using the embedding algorithm. And Figure 2 represents watermark detection process in which embedded watermark is retained by detection algorithm [4].

2. WORKING OF DIGITAL IMAGE PROCESSING

The result of digital watermarking is an image with secret information embedded within it. The three stages of a digital image watermark in operation are depicted in Figure 3 [4].

Phase A: Incorporation

Here, we use an embedding algorithm and a secret key to insert the watermark into the source image and generate the watermarked image that will be sent over the network [4].

Phase B: Distortion

Here, attacks are carried out on the watermarked images as they travel through the network, either to change or destroy the watermarked data [4].

Phase C: Detection

In this step, the watermark is identified using the detection algorithm and secret key; noise is also recognised at this point [4].

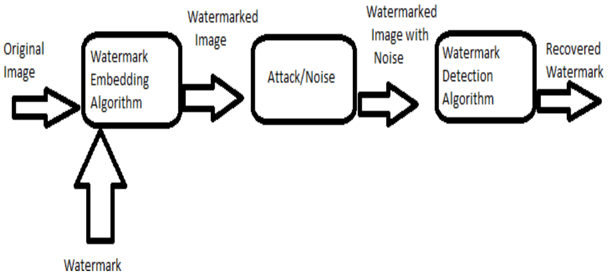
Original Image
Watermark Embedding Algorithm
Watermarked Image
Attack/Noise
Watermarked Image with Noise
Watermark Detection Algorithm
Recovered Watermark
Watermark

Fig 3: working of digital image watermarking

3. DIGITAL WATERMARKING CHARACTERISTICS

Three main characteristics of digital watermarking are [2]:

A. *Fidelity:* The image quality should not get altered after it is watermarked; even watermarking should not make the distortions visible as it will reduce economic value of image.

B. *Robustness:* Watermarks are removed knowingly or unknowingly by image processing operations. It should be robust across several attacks.

C. *Capacity:* This characteristic defines amount of data that has to be embedded as a watermark for successfully detection during extraction.

D. *Security:* Watermark should be secret so that it cannot be identified by the unwanted users.

4. APPLICATIONS OF WATERMARKING

Watermarking is mostly used for [2]:

A. The transfer of content that is protected by copyright can be hindered by the unreliable nature of the internet, however watermarking can help prevent this [2].

B. Content Archiving: Watermarking adds a serial number or other descriptive information to a digital object so that it can be stored in an archive. It's also used to help organize and categories digital materials [2]. Broadcast monitoring (or cross-verification) checks to see if information scheduled for broadcast actually went out [2].

D. Tamper Detection: Watermarking helps identify any modifications made to digital files. Tampering detection is achieved by embedding weak watermarks into digital content; if the watermark is later found to have been damaged, this is taken as evidence of tampering [2].

E. Digital Fingerprinting: This method can be used to identify the owner of digital content by comparing their fingerprints to a database of known owners [2].

F. Data Authentication and Integrity Verification Using Fragile Watermarks Watermarking also preserves data authentication and integrity verification.

5. DIGITAL WATERMARKS TYPES

Watermarking techniques are classified into the following:

A. On the basis of document that has to be watermarked, watermarking techniques are divided into the four types:

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

B. In other way, digital watermarks techniques are divided as follows:

- Visible watermark: It is basically a secondary image that is imposed on original image for protection of that image. In this changes that are made to original image are visible. For example, Figure 4 (a) and (b) shows the original and visible watermarked image [10].

- Invisible-Robust watermark: In this type of watermarking technique the changes that are made to original image in the form of a watermark are unnoticeable and the changes made are easily recovered later with the help of suitable decoding algorithm.

- Invisible-Fragile watermark: Invisible fragile watermarks are added in digital content and if the added watermark is found to be degraded or altered, it indicates tampering with content or modification of image.

Fig 4(a): original image [10]

Fig 4(b): Watermarked image [10]

6. WATERMARKING TECHNIQUES

Digital watermarking consists of several different techniques for protection of digital content [4]. The digital image watermarking falls in two main broad categories:

- Spatial domain techniques
- Frequency domain techniques

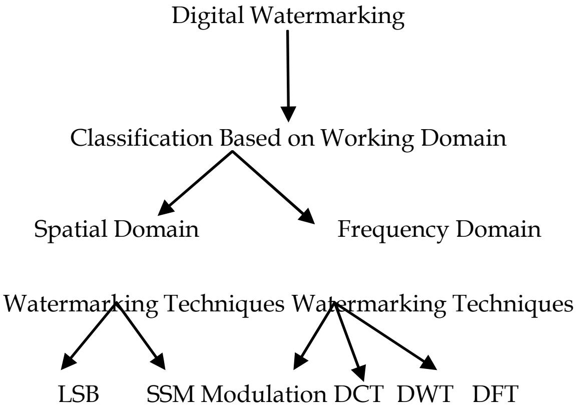

Fig 5: Classification of Watermarking Domain

Spatial domain techniques work on pixels and pixel value are modified for embedding the watermark. The commonly used spatial domain technique is LSB. Whereas frequency domain coefficient is modified by Frequency domain techniques for embedding watermark. DCT, DWT and DFT are commonly used frequency domain technique. In case of robustness and imperceptibility, frequency domain techniques are more reliable than spatial domain technique.

A. Spatial Domain Techniques

This technique presents the image in form of pixels. In this technique, watermark is embedded in the cover image by changing values, intensity and the color of the selected pixels [5]. The key benefits of spatial domain watermarking are its simplicity, low computational complexity and it consumes less time [4]. The estimation speed of spatial domain techniques is very fast in comparison with frequency domain techniques and simply can be applied to any image but it is less robust to attacks than frequency domain techniques [4]. The commonly used method of spatial domain is LSB [4, 7].

- **Least Significant Bit (LSB)**

This is the simplest spatial domain method, as LSB carries less appropriate information and their modification does not cause visible changes [5]. It is simple to embed a watermark in LSB of randomly selected pixels of the original image [4]. An image is given, where each pixel of image is represented by an 8-bit stream, the watermarks are added in the LSB, of selected pixels of the image. This method is easy from implementation point of view and does not produce severe distortion to the image but, it is not very robust across attacks [7]. Example of LSB watermarking [4]:

Image:

10010101 00111010 11001100 01010100….

Watermark:

0 1 0 1…..

Watermarked Image:

1001010**0** 0011101**1** 1100110**0** 0101010**1**…..

The steps of LSB technique for watermark embedding in cover image are [4]:

1) First Converting RGB image into grey scale image.

2) Making double exactness for image.

3) Shifting MSB to LSB of watermark image.

4) Making LSB of cover image zero.

5) Adding shifted version (step 3) of watermarked imageto modified (step 4) host image.

The main benefits of LSB method is that it can be simply applied on images. And it does not deteriorate the quality of image after embedding the watermark. The main drawback of LSB method is it is not very robust against signal processing operations and attacks [4].

- **SSM Modulation Based Techniques:**

In Spread-spectrum Modulation techniques the energy generated at different discrete frequencies is purposively dispersed or appropriated in time, for secure communications establishment, increasing resistance to natural interference and jamming, and for preventing detection. SSM watermarking algorithm embeds information in context of image watermarking and when it is applied to the context of image watermarking, it embeds message by combining the cover image with a small pseudo noise signal modulated by the added watermark [5].

B. Frequency Domain Techniques

The frequency domain techniques are more successful than spatial domain techniques. In frequency domain techniques, the image is illustrated in the form of frequency [4].Frequency domain techniques are more applied than spatial domain techniques. The aim of this technique is to embed the watermarks in the spectral coefficients of the image. Discrete Cosine Transform (DCT), Discrete wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are the commonly used frequency domain technique [4]

- **Discrete Cosine Transform (DCT)**

DCT is used for signal processing. It basically helps in transforming signal from spatial domain to the frequency domain. DCT is used in many fields like compression of data, recognition of pattern and in almost every field of image processing. DCT watermarking is more robust in comparison with spatial domain watermarking [4]. Discrete Cosine Transform is similar to Discrete Fourier Transform; therefore, it represents data in terms of frequency space rather than an amplitude space [7]. It converts signal into elementary frequency components [5]. This type of algorithms is more robust on image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are not robust across geometric attacks like rotation, scaling, cropping etc [5]. Global DCT watermarking and Block based DCT watermarking are sub-categories of DCT watermarking [5]. The main steps of DCT [4, 5]:

1) Image is segmented into non-overlapping blocks of 8x8.
2) Forward DCT is applied to these blocks.
3) Block selection criteria like HVS are applied.
4) Coefficient selection criteria like
5) Selected Co-efficient is modified for embedding watermark.
6) Inverse DCT transform is applied on each block.

DCT divides image into different frequency band for adding the watermark. The DCT due to selection of perceptually significant frequency domain coefficients is more robust across different signal processing attacks [4].

- Discrete Wavelet Transformation (DWT)

Today DWT is widely used in variety of signal processing applications, like in audio and video compression, removing noise in audio, and the simulation of wireless antenna distribution. The energy of Wavelets is centered in time and are appropriate for analysis of transient, time-varying signals. DWT is well suited for many applications as most of the signals in nature changes with time. The biggest challenge in watermarking is to achieve a good tradeoff between robustness and perceptivity. But if strength of enclosed watermark is increased robustness will be achieved but visible damage will also get increased simultaneously [7]. DWT is preferred more as it gives both spatial localization and frequency spread of the watermark within the original image [7]. The main concept of DCT is to decompose the image into sub-image having different spatial domain and independent frequencies [7]. DWT of image gives multi resolution representation of image that provides simple framework for describing image information. Signal is analyzed at different resolutions by DWT. DWT breaks image into high low frequency quadrants and low frequency quadrant is further divided into two more high and low frequencies and this is continued until the signal is completely decomposed [4]. DWT are scalable in nature. DWT are mostly used in image watermarking because of its good spatial localization and multi resolution techniques [4].The main disadvantages of DWT are: it is more complex than DCT, computation cost is higher and computation time is longer.

- Discrete Fourier Transform (DFT):

DFT is robust across geometric attacks such as cropping, scaling, rotation, translation etc. DFT divides an image in sine and cosine form. DFT techniques are categorized into two types: first is direct embedding and another one is the template-based embedding. In direct embedding DFT magnitude and phase coefficients are modified for embedding the watermark, whereas template-based embedding proposes the idea of templates. Basically, template is a structure that is embedded in DFT domain for calculating transformation factor and as the image goes under transformation the template is looked for resynchronizing the image, and then for extracting the embedded watermark detector is used. Central component that consists of low frequency is the main component of DFT [4].

The main benefit of DFT over DCT and DWT is that DCTis found to be Rotation Scaling Translation (RST) invariant. Hence it can easily overcome from geometric distortion, whereas DCT and DWT are not RST invariant. Therefore, they are not able to easily overcome from geometric distortions [4]. And the main drawback is the output of DFT that is always a complex value and more frequency rate is required and even computational efficiency of DFT is very bad. So due to these reasons DFT is not used [4].

7. COMPARISON BETWEEN SPATIAL AND FREQUENCY WATERMARKING DOMAIN

Table I: Comparison between Watermarking Domains [8]

S.no	Factors	Spatial Domain	Frequency Domain
1.	Cost	Very Low	Very High
2.	Robustness	Fragile	Low Robust
3.	Perceptually	Highly Controllable	Low Controllable
4.	Computational complexity	Low	High
5.	Time Consumption	Less	More

8. CONCLUSION

Today Digital image Watermarking has become important research topic for researchers. This survey paper detailed spatial domain (LSB, SSM) and Frequency domain (DCT, DWT, DFT) techniques of digital image watermarking. Different techniques used for watermarking have their own advantages and disadvantages. Digital image watermarking is still a challenging research area and lot of research work needs to be done in the field of watermarking. Future work could include the developmentof more robust and secure watermarking technique than the existing ones.

9. REFERENCES

[1] Namita Chandrika, Jaspal Bagga. -Performance Comparison of Digital Image‖, International Journal of Computer Applications Technology and Research, Volume 2– Issue 2, 126 - 130, 2013.

[2] Vinita Gupta, Mr. Atul Barve, ― 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.

[3] Saraju P. Mohanty*, K.R. Ramakrishnan, Mohan S Kankanhalli," A DCT Domain Visible Watermarking Technique for Images".

[4] Preeti Parashar, Rajeev Kumar Singh, ―A Survey: Digital Image Watermarking Techniques, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124.

[5] Y. Shantikumar Singh, B. Pushpa Devi, Kh. Manglem Singh, ―A Review of Different Techniques on Digital Image Watermarking Scheme, International Journal of Engineering Research (ISSN : 2319-6890)Volume No.2, Issue No.3, pp : 193-199 01 July 2013.

[6] Navnidhi Chaturvedi, ―Various Digital Image Watermarking Techniques and Wavelet Transforms‖, International Journal of Emerging Technology and Advanced Engineering (ISSN 2250- 2459, Volume 2, Issue 5, May 2012).

[7] Manpreet Kaur, Sonika Jindal, Sunny Behal, ― A Study of Digital Image Watermarking, Volume 2, Issue 2 (February 2012).

[8] Shivanjali Kashyap, ― Digital Watermarking Techniques and Various Attacks Study for Copyright Protection‖, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

[9] Frank Hartung, and Martin Kutter, ―Multimedia Watermarking Techniques.

[10] Tsung-Yuan Liu, and Wen-Hsiang Tsai, IEEE, "Generic Lossless Visible Watermarking― A New Approach‖, IEEE Transactions on Image Processing, Vol. 19, No. 5, May 2010.