Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 9, June-2019, ISSN 2230-7540

Digital Watermarking Techniques and Its Applications

K. Raghavendra Prasad*

Research Scholar, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh

Abstract – Digital media as an alternative to printed media is a constant need for the public. When digital media arose, information required protection when going across the Internet or other platforms. Watermarking strategies have been established to deal with this need. This gives both watermarking strategies that are specifically tailored towards the imaging and execution of watermarking models in the world today.

Key Words: - Watermarking, Techniques, Applications

----------X----------

INTRODUCTION

New technical advances are observed in today's century. A photograph shot by a cell camera shows the new media quite well. The use of digital media is widespread in the present century. Text, voice, video etc. are another immersive technology example. We realize that the Internet is the best place to transmit data to everyone in the world. With the evolution of this technology, the possibility of piracy and copyright for holders is quite evident. Watermarking is a form of data security against these problems, combining the name of the consumer (watermarking) into digital media to distinguish sender and receiver data safety. This approach is accessible in all formats of interactive communication, including text, audio, video and papers.

The following sections are organized:

- Watermarking image description with watermarking history
- Detailed watermarking photo types
- Methods of recognition and watermarking
- Watermarking material risks

GENERAL INTRODUCTION OF IMAGE WATERMARKING

Image Watermarking is the method of embedding the copyright identification of the host file. Although watermarking is first used, it can be used in 1282 in Bologna, Italy. It is first used in paper mills as a mark. In reality, before the 20th century, it is common. After the watermark is also seen in the postage stamp and currency notes in certain nations.

Digital image watermarking is essentially derived from Steganography, a process in which digital data is disguised with other details for the secure transmitting of digital data. In particular, while data to be covered are obscured during delivery by courier, steganography and watermarking are very similar to each other.

The crucial difference between these two systems is that hidden data is a moderate priority for senders and recipients, but watermarking bot source images and hidden pictures, signatures or details are of higher priority.

Example of watermark on Indian currency

Process of Image Watermarking

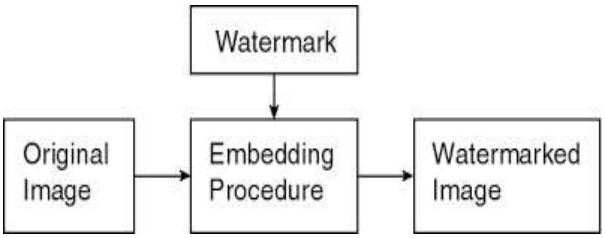
The process of watermarking is divided into two parts:

a) Embedding of watermark into host image.

b) Extraction of watermark from image.

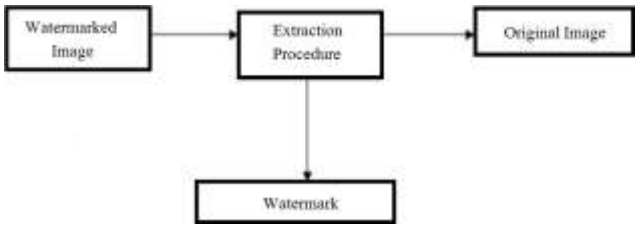
Watermarking Embedding

At the end of the source is the image watermarking process. This system incorporates every algorithm or system of watermarking in the host image.



Watermarking Extraction

This is the technique by reversing the embedding algorithm to extract watermark from the watermarked picture.



CLASSIFICATION & APPLICATIONS

Digital watermarking techniques are categorized into individual types. This name was based on a range of variables. The table below lists the two classifications.

Watermarking strategies are typically used in the image. It is a geographical region and a movement phase. However, strategies of domain transfer are more commonly used than spatial domains.

S.no	Criteria	Classification
1.	Watermark Type	1. Noise: pseudo noise, Gaussian random and chaotic sequences 2. Image: Any logo, Stamp Image etc.
2.	Robustness	1. Fragile: Easily Manipulated. 2. Semi-Fragile: Resist from some type of Attacks 3. Robust: not affected from attack
3.	Domain	1. Spatial: LSB, Spread Spectrum 2. Frequency: DWT, DCT, DFT, SVD
4.	Perceptivity	1. Visible Watermarking: Channel logo 2. Invisible Watermarking: like Steganography
5.	Host Data	1. Image Watermarking 2. Text Watermarking 3. Audio Watermarking 4. Video Watermarking
6.	Data Extraction	1. Blind 2. Semi-Blind 3. Non-Blind

Transfer Domain Techniques:

Compared to the spatial domain watermarking, the transform domain watermarking is stronger. The picture is seen in the type of frequency in the watermark transform domain. In transforming domain watermarking techniques, a predefined transformation first of all transforms the original file. We then insert the watermark into the picture of transformation or into the coefficient of transformation. Finally, we turn the reverse to get the watermarked file.

Commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

I. Discrete Cosine Transform (DCT)

It is used for signal processing in general. In this we transform the picture into the frequency domain. It is used in many fields such as pattern recognition, encoding of records, and image processing. This technique is more robust than watermarking techniques in the space domain. The principal phases in DCT are:

- Take the picture first and break it into 8 * 8 blocks.

- Calculate forward DCT for each block that does not overlap.
- Use selection criteria for HVS blocks.
- Now use the largest selection coefficients.
- Then insert the watermark into the coefficient selected.
- Now take each block's reverse DCT transformation

II. Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) shows the picture in multi resolution. This picture offers a basic context for understanding the creation of the picture. In multiple resolution the DWT analyses the signal. If the DWT is applied to an image, it splits the image into two quadrants, namely high frequency quadrant and small frequency quadrant. This process proceeds until the signal is fully decomposed. As one stage DWT is added to a two-dimensional picture it divides it into four sections, i.e.

LL: It consists of the low-frequency picture data. We may claim that this section is about the graphic.

LH: It consists of vertical picture data.

HL: The horizontal specifics of the initial picture are used.

HH: It consists of high-frequency picture data.

III. Discrete Fourier Transform (DFT)

The DFT gives more robustness against geometric attacks such as scaling, cropping, transformation, rotation, etc. It degrades a picture in the shape of a sinus and a cosine. In this way, embedding can be achieved in two ways: direct incorporation and template-based incorporation.

We change the magnitude and phase coefficients of DFT in the direct embedding technique and then embed a watermark. The template-based embedding methodology incorporates the model's principle. During embedding we insert the blueprint in the DFT domain, which is used for discovering the transformation component. When the picture is converted, this prototype is first scanned and then used to resync. After that, the detector is used to delete the combined watermark range

Everyone can use watermarking strategies for citizens, although these strategies have lately been used by researchers. These variants enable developers to use the best features of each provided methodology.

Applications of watermarking

In all digital media, watermarking technologies are implemented, while authentication and owner recognition are required. The following are some of the more popular programs.

Owner Identification

The use of watermarks that he has created is to identify all media owner. Any paper watermarks are removed easily by a small attacker exercise. The interactive watermark was made. The watermark is the interactive image 's internal portion such that it cannot be easily detected and removed.

Copy Protection

Unlawful copying is also forbidden by watermarking copy protection. This defense involves the integration into the watermarking identification circuit of copying machines.

Broadcast Monitoring

Watermarking is also monitored on radio and TV networks. For commercial media, such as sport and television, this is typically done.

Medical applications

Social media and documents were often remotely reviewed with the information of the patient and attending physicians. Both translucent and opaque watermarks may be used. This watermarking helps doctors and medical organizations to ensure that their records are not wrongly written.

Fingerprinting

Fingerprinting is a process by which a particular identification may be provided in the form of a watermark through retaining certain digital content. The identification of the person who has leaked the original contents may help distinguish the watermark from an unauthorized copy. In cinemas, films are digitally filmed by satellite and have a theatre I'd such that action against a theatre may be taken if theatre identity is found by a pirated copy.

Data Authentication

Authentication is the process by which the collected information or data may be supplied correctly. There should be no intimidation for it. The sender incorporated the digital watermark into the host data and the data were captured and tested at the edge of the recipient. For example, as a search for CRC or parity (cyclic redundancy search).

WATERMARKING ATTACKS

As the watermarked media are published, multiple assaults on this watermarked media arise. These assaults may be as follows:

- **Delete Attack:** The unauthorized attacker attempts in this situation to erase the watermark, i.e. hidden details from the watermark.
- **Intrusion Attack:** The disturbance is introduced into watermarked media in certain forms of assaults. Averaging, quantification, compression, etc. are several instances of this type.
- **Geometric attack:** certain attacks will alter the image's geometry. Crossing, flipping, etc. are instances of this group.
- **Low Pass Filtering Attack:** this kind of attack happens when a low pass philter passes the watermarked data.
- **Aggressive assault:** the most critical strike. Aggressive assault. In this scenario the unauthorized consumer manages to delete the watermark or only renders the watermark so that no activity will identify it.
- **Passive attacks:** Unauthorized users actually try to figure out through this form of assault if the individual data contain a watermark or not.
- **Image Degradation:** In these forms of attacks model sections are removed and durable watermarks are destroyed. Part cropping, row removal and column exclusion, Gaussian noise injection, are instances of these assaults.

CONCLUSION

Digital image watermarking of frequency and device frameworks include DCT, DWT, DFT and applications. The watermark is installed and extracted utilizing the techniques. Watermarking is a significant issue for us now. Different watermarking approaches have their own advantages and disadvantages. Visual watermarking is still a subject and watermarking work needs to be completed. Create a cleaner, more robust watermarking method than established ones.

REFERENCES

[1] Christine I. Podilchuk, Edward J. Delp (2001) —Digital watermarking: Algorithms and applications, IEEE Signal processing Magazine.

[2] Jiang Xuehua (2010) —Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation

[3] C.T. Li and F.M. Yang (2003) —One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291.

[4] V. M. Potdar, S. Han and E. Chang (2005). "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[5] N. Chandrakar and J. Baggaa (2013). "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, Vol. 2, No. 2, pp. 126-130.

[6] F. Daraee and S. Mozaffari (2013). "Watermarking in binary document images using fractal codes", Pattern Recognition Letter.

[7] N. Tiwari, M. k. Ramaiya and Monika Sharma (2013). "Digital watermarking using DWT and DES", IEEE.

[8] S. S. Gonge and J. W. Bakal (2013). "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, Vol. 1, No. 2.

[9] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan (2012) —A Novel Technique for Digital Image Watermarking in Spatial Domain, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[10] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE 'A Review of digital image watermarking in health care'.

[11] Edin Muharemagic and Borko Furht (2001) —A Survey of watermarking techniques and applications.

[12] Namita Chandrakar, Jaspal Bagga (2013) —Performance Comparison of Digital Image‖, International Journal of Computer Applications Technology and Research, Volume 2– Issue 2, 126 – 130.

[13] Vinita Gupta, Mr. Atul Barve (2014) — A Review on Image Watermarking and Its Techniques‖, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1.

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

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

[16] Y. Shantikumar Singh, B. Pushpa Devi, Kh. Manglem Singh (2013) —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.

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

[18] Manpreet Kaur, Sonika Jindal, Sunny Behal (2012) — A Study of Digital Image Watermarking‖, Volume 2, Issue 2.

Corresponding Author

K. Raghavendra Prasad*

Research Scholar, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh

ekta.eklavyaeducators@gmail.com