International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Review of Digital Image Watermarking Methods

Harikrashna Pratap Singh [a], *Sanjay Khadagade* [b]

[a] *M Tech Scholar, Department of Electronics and Communication, Oriental Institute of Science and Technology, Bhopal, 462022, India.*
[b] *Asst. Professor, Department of Electronics and Communication, Oriental Institute of Science and Technology, Bhopal, 462022, India.*

ABSTRACT

Digital watermarking is used to hide crucial information within other data so that it can only be accessed by the intended recipient (RX) or by the person who owns the relevant data, and is therefore also referred to as security-based technology. This article provides a detailed explanation of the fundamentals of digital watermarking, a classification, a review of various digital watermarking techniques, and a summary of digital watermarking in terms of its various parameters, the methods employed and features associated with each of which are presented in a table. To raise the level of security, watermarking could be combined with cryptography and steganography.

Keywords: Digital Watermarking, image processing, image encryption, etc

1. Introduction

On any paper, there is a watermark that is printed as an image or text. Real-time detection is necessary for compression in video watermarking. The use of sound watermarking in online music. A text shape and area between text and line spaces contain a text watermark. Insertion of a graphic watermark into 2D or 3D graphics is performed [1]. The observer notices watermarking that can be observed. Modifications to the pixel values are not seen in invisible watermarking. Dual watermarking is when there is a delay between the visible and the unseen. Thumbprints and digital watermarking are utilised for broadcast testing [2] [3]. When a watermarked output (O/P) is transmitted to a human and that human makes changes to it, it is referred to as an attack. Inputs (I/Ps) include secret information, watermarks, public or private keys for security, and watermarked outputs. Watermark-cropping, JPG compression, AWGN, quantization, rotation, collusion, demodulation, and averaging are all destroyed by robustness or interference attacks. Affine modification, aspect ratio variation, translation, scaling, rotation, and geometric transformation are examples of extraction failure in presentation attack. A counterfeiting attack modifies genuine data to produce bogus data. Geometric changes of an image, such as row-column blanking, translation, warping, scaling, cropping, and rotating, are known as geometric hacks. Image compression, distortion-Gaussian noise, gamma correction, filtering, brightness, sharpening, histogram equalisation, averaging, collusion, printing, and scanning are examples of non-geometric hacks used in signal processing [3]. A number of authorised RXs work together to create actual data by averaging all watermarked data [2]. By calculating the private key using a laborious brute force method, cryptographic hacks compromise privacy [10]. IBM hack (deadlock, inversion, or counterfeiting hacks) inserts one or more watermarks that are unclear as to which was the watermark of the original vendor [2], and then uses a technique on the hacked data to extract the watermark from it. Protocol hacks close the gaps in the watermarking. I/Ps have a watermark, a private or public key, and an original piece of data (O/P).

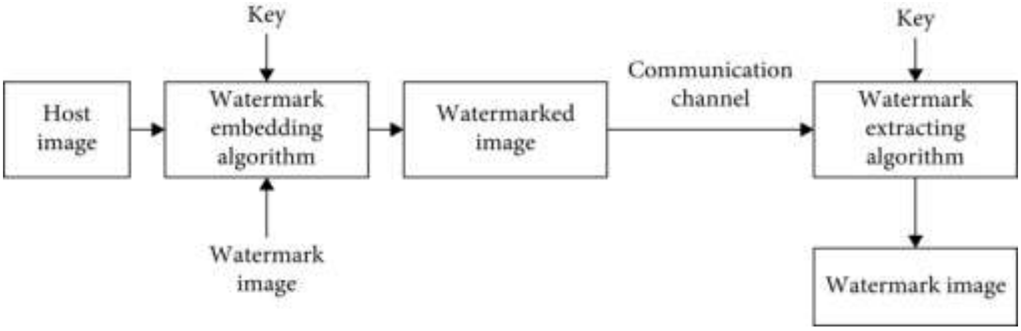


Fig. 1 - System for embedding and extracting watermarks [1]

2. Digital Watermarking Techniques Classification

The note's capacity is 0 bits, making it possible to determine if a watermark is present or not. When a watermark controls an n-bit note, the process is referred to as multiple or non-zero bit watermarking. Calculation and Benchmarking - The evaluation of watermarking techniques provides data for planners cameras have safety criteria adds noise to the genuine image.

1. Semi-fragile watermarking helps somewhat alter a watermarked piece of data [1].

2. Spatial domain watermarking records the data to the value of the pixels. [1]. Specific frequencies are altered from their true images in the frequency domain [1].

3. Real substance is required for visual or secret watermarking [1]. The genuine information is not required for extraction in semi-private or semi-blind watermarking [1].

4. All disseminated image copies in source-based are designated with a distinctive watermark that links to the vendor[1].

In destination-based marketing, the purpose of the watermark is to locate the purchaser in an unauthorised resale state [1].

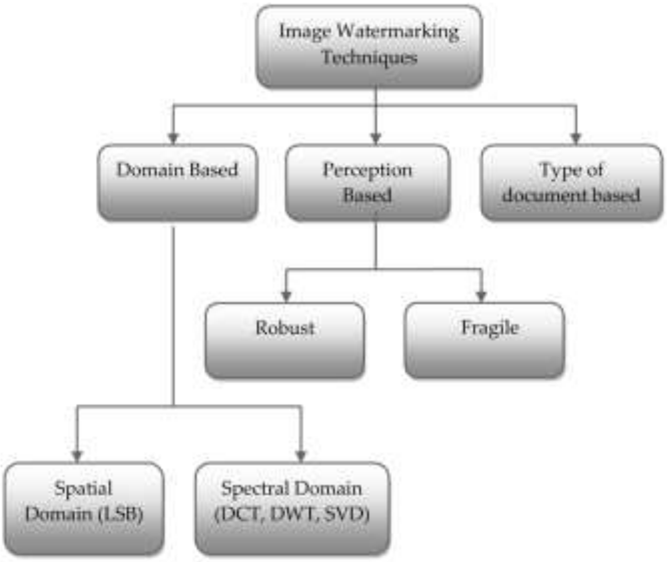


Fig. 2 - Digital Watermarking Techniques Classification

3. Image Watermarking Methods

Many applications where watermarking is required [1]. Since the watermark is translucent, it is unaffected [3]. The zero tree wavelet picture compression and maximum frequency subbands of DWT make it effective [5]. An image has been steganographically altered by LSBs of the secret and stego picture, then stego image has been watermarked in the time and frequency domain. The image has been encoded with a huge private key by converting pixel bits by XOR. In terms of frequencies in the transform domain or spatial domain, images can be represented as pixels. To convert an image to its frequency representation, we employ reversible transforms as the discrete cosine transform (DCT), discrete wavelet transform (DWT), or discrete Fourier transform (DFT) [6]. By altering these values, i.e., the transform domain coefficients [9] or pixel values, watermarks can be added to photographs.

3.1 Watermarking DCT Domain

The high frequency components have a frequency domain watermark. The key actions are:

1) Separate the image into 8x8 blocks that do not overlap.

2) Put each of these blocks through forward DCT.

3) Use some block selection parameters (e.g. HVS)

4) Employ criteria for coefficient selection (e.g. highest)

5) Insert a watermark by changing the chosen coefficients.

6) Apply the inverse DCT transform to every block.

3.2. Watermarking of DWT Domain

The fundamental idea in this case is the same as in DCT, but the method for transforming the image into its transform domain differs, leading to different coefficients as a result. In wavelet transformations, the picture is transformed using wavelet filters such the Daubechies Orthogonal Filter, HaarWavelet Filter, and Daubechies Bi-Orthogonal Filter. These filters divide the image into a variety of frequencies. Four frequency representations of an image, such as LL, HH, LL, HH sub bands, are produced via a single level decomposition.

3.3 DFT Domain

Researchers' preferred method of watermarking the DFT domain is because it offers resistance to geometrical attacks including translation, rotation, cropping, and scaling, among others. DFT-based watermark embedding methods come in two varieties. The first method of embedding a watermark uses direct coding, and the second method uses template-based embedding. Watermarks are embedded in direct embedding by altering the phase information in the DFT. In the DFT domain, a template is a structure that is employed to evaluate the transformation factor. The image is first transformed, after which this template is searched for, the image is synchronised, and finally the detector is used to retrieve the embedded spread spectrum watermark.

However, the future of digital watermarking appears promising. Digital watermarking research is already being conducted by numerous businesses. For instance, Microsoft has created a working prototype of a system that prevents music from being played without permission by permanently attaching a watermark to audio files. Future iterations of the Windows operating system may come standard with such technology. The security technology can typically be hacked. However, digital watermarking will encourage content creators to trust the Internet more if the technology is combined with appropriate legal enforcement, industry norms, and respects for the privacy of people wishing to legally use intellectual property. For many businesses, a huge sum of money is at risk.

The following are the major attributes of a digital watermark:

Robustness: After standard signal processing procedures such image cropping, transformation, compression, etc., the watermark should be able to withstand the effects.

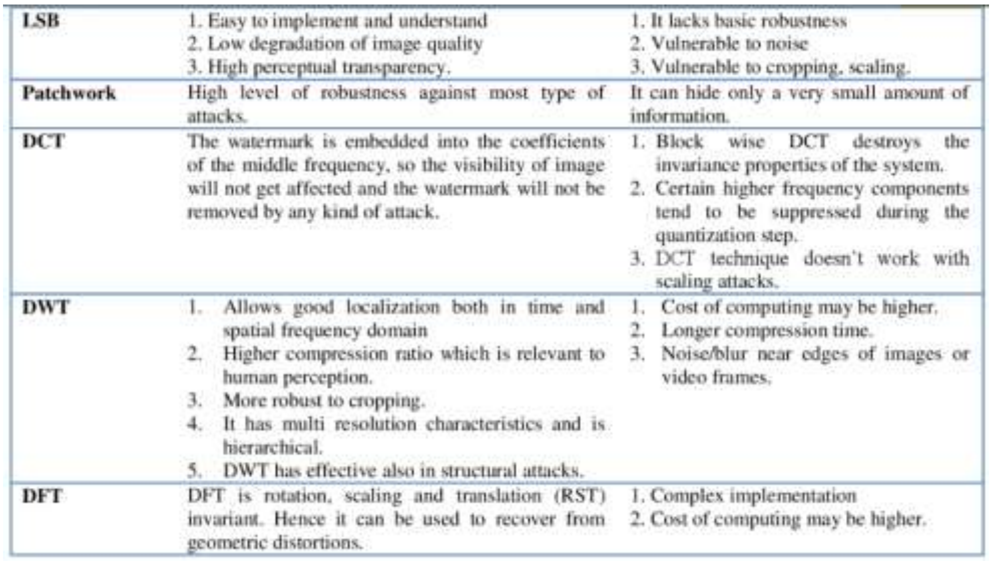
Imperceptibility: To the unaided eye, the watermarked image should appear identical to the original. The encoded watermark cannot be seen by the visitor.

Security: The encoded watermark cannot be detected, retrieved, or altered by an unauthorised person.

4. Conclusion

In essence, it is determined that digital watermarking is used to conceal critical information among other data so that it is only accessible to RX or to the one who owns that data and is not accessible to any attackers. This paper provides a detailed explanation of the fundamentals of digital watermarking, a categorization and review of various digital watermarking techniques, and a summary of digital watermarking in terms of its various advantages and disadvantage, the methods employed and features associated with each of which are presented in a table. The future of digital watermarking is promising because a review offers information on the subject that may be useful in learning more about this area of study.

Table I **Techniques** **Advantages** **Disadvantages**



LSB	1. Easy to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Patchwork	High level of robustness against most type of attacks.	It can hide only a very small amount of information.
DCT	The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step. 3. DCT technique doesn't work with scaling attacks.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception. 3. More robust to cropping. 4. It has multi resolution characteristics and is hierarchical. 5. DWT has effective also in structural attacks.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions.	1. Complex implementation 2. Cost of computing may be higher.

References

[1] Patel Ruchika, Bhatt Parth, a Review Paper on Digital Watermarking and its Techniques, *International journal of computer applications* (2015) 0975-8887 Vol. 110,No.01.

[2] Manpreet Kaur, Jindal Sonika, Behal Sunny, A Study of Digital Image Watermarking,(IJREAS) *International journal of research in engineering and applied sciences* (2012) 2249- 3905,Vol.02.

[3] Jabade.SVaishali, Dr. Gengaje.R Sachin, Literature Review of Wavelet Based Digital Image Watermarking Techniques, *International Journal of Computer Applications* (2011) 0975 – 8887 Vol. 03, No. 01.

[4] Nasereddin H.O. Hebah, Digital Watermarkinga Technology Overview,*(IJRRAS),* (2011)Vol. 06.

[5] Mistry Darshana,Comparison of Digital Water Marking methods,(*IJCSE) International Journal on Computer Science and Engineering* (2010) 2905-2909 Vol. 02, No. 09.

[6] Yousuf Farah Qasim, Din Roshidi, Review on secured data capabilities of cryptography, steganography, and watermarking domain, *Indonesian Journal of Electrical engineering and computer science* (2019) 2502-4752, Vol. 17, No.02.

[7] Mirza AbdurRazzaq Mirza Adnan BaigRiaz Ahmed Shaikh Ashfaque Ahmed Memon, Digital Image Security: Fusion of Encryption, Steganography and Watermarking, *(IJACSA) International journal of advanced computer science and* applications (2017) Vol. 08, No.05.

[8] Jain Deepika (2021), Digital Watermarking Technology – *A Review, Gorteria Journal (2021*) 0017-2294 Vol.34.

[9] Jiao Shuming, Zhoua Changyuan, ShibYishi, ZouaWenbin,LiaXia,Review on optical image hiding and watermarking techniques, *Optics and laser technology*109 (2018)370-380.

[10] Ensaf Hussein Mohamed A.Belal, Digital Watermarking Techniques,Applications and Attacks Applied to Digital Media: A Survey, *(IJERT) International journal of Engineering Research and Technology* (2012) 2278-0181, Vol.01.

[11] F. Ernawan, and M.N. Kabir, “A block-based RDWT-SVD image watermarking method using human visual system characteristics,” *The Visual Computer,* vol. 36, pp. 19-37, 2020.

[12] F Ernawan, and M.N. Kabir, “A blind watermarking technique using redundant wavelet transform for copyright protection,” *14th International Colloquium on Signal Processing & Its Applications (CSPA*), pp. 221-226, 2018.

[13] Hao-Tian Wu, Jean-Luc Dugelay and Yun-Qing Shi, Reversible Image Data Hiding with Contrast Enhancement, *IEEE Signal processing letters* (2015) 81-85, Vol. 22, No.1.

[14] Shivdeep, Ghosh Sudip, Rahaman Hafizur, A New Digital Colour Image Watermarking Algorithm with its FPGA and ASIC Implementation, *IEEE,* (2020)978-1-7281-6564-6/20/.

[15] Das Subhajit, Singh Pragati , Koley Chaitali, Hardware implementation of adaptive feedback based reversible image watermarking for image processing application, *Springer-Verlag GmbH Germany, part of Springer Nature (2018).*

[16] Das Subhajit ,MaityReshmi, Maity N. P, VLSI-Based Pipeline Architecture for Reversible Image Watermarking by Difference Expansion with High-Level Synthesis Approach, *Springer Science+ Business Media(2017).*

[17] Qu Gang, Publicly Detectable Watermarking for Intellectual Property Authentication in VLSI Design, *IEEE transactions on computer aided design Of Integrated circuits and systems (2002)* 1363- 1368,Vol. 21,No.11.