ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 12; Issue 02; 2024; Page No. 01-08

A Comprehensive Review of Digital Watermarking Methods

Mukesh Choudhary[A], Ms. Shalini Sharma[B]

M Tech. Scholar in RIET, Jaipur

Assistant Professor in RIET, Jaipur

Conflicts of interest: Nil

Corresponding author: Mukesh Choudhary

Abstract

Digital picture authentication is a critical problem for the digital revolution since any image may be tampered with. In recent decades, academics have been particularly concerned with ensuring the validity of digital photographs. To address this challenge, numerous appropriate watermarking methods have been developed based on the targeted uses. However, it is difficult to design a watermarking system that is both strong and secure. This document describes standard watermarking system frameworks and provides certain standard criteria that are utilized when creating watermarking systems for various applications. The latest advancements in digital picture watermarking techniques are also examined to determine the most advanced technologies as well as their limits. Some conventional assaults are described, and future study areas are suggested.

Keywords: LSB; DCT; DFT; DWT; SVD

INTRODUCTION

A watermark is an image or words written on any paper. Video watermarking requires real-time detection and compression. Sound watermarking captures online music. Text watermarking is integrated in the text shape and the region between the text and line spacing. Graphic watermarking is the process of inserting data into 2D or 3D visuals [1].

When someone looks closely enough, they may notice watermarks. No changes to the pixel values are evident with Invisible Watermarking. In dual watermarking, the invisible watermark serves as a visible holdup. Broadcast testing and thumb prints are two examples of digital watermarking's many uses [2] [3].

False data is generated by the manipulation of genuine data in a counterfeiting attempt. Some examples of geometric hacks include scaling, rotation, row-column blanking, warping, translation, and cropping. Nongeometric or signal processing hacks [3].

Thanks to advancements in image processing and the proliferation of the internet, it is now possible to make high-quality digital copies of existing photographs and share them with others quickly and cheaply. Data privacy and security are being jeopardized by the rapid development and advancement of network technologies. Thus, in order to tackle the current and future issues of digital information maintenance, authentication of content, copyright protection, and protection against duplication are crucial.

As an alternate method of protecting multimedia documents from tampering, digital picture watermarking is only digitally watermarking an image. This method also helps with intellectual property ownership and security. Data may be concealed by any digital material, including photos, sounds, and movies. It is easy to illicitly hold,

replicate, and disseminate digital material over a physical transmission media during data storage, processing, and communications. The process of digital picture watermarking is inserting data into a multimedia file and then either detecting or extracting that data. Authentication, content verification, tamper-resistance, and image integration are all achieved via these approaches [4].

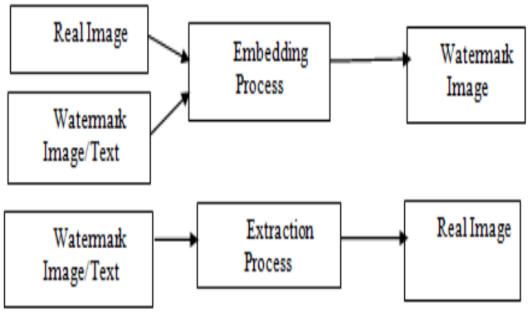

Figure 1: System for Watermarking, Embedding, and Extracting

2. Literature Survey

Steganography shows that hiding information in other medium is quite ancient. The phrase "advanced watermarking" was first used in 1993 by Tirkel et al. [12] to describe two techniques for image data concealment.

Watermarking methods in telemedicine systems have recently seen significant improvements [13]. These methods not only provide another critical need of the healthcare communication system—optimal bandwidth utilization—but they also offer authentication and security. For use in telehealth, the authors of [13] suggested a watermarking system (WS). This approach used lifting wavelet transform (LWT) and discrete cosine transform (DCT) algorithms to include an 80-character medical report and a signature watermark picture. This study used LWT to break the host picture down into its component subbands, and then used DCT to further process the most important subbands. In the end, the subbands that were changed via DCT had the patient report and signature watermark encrypted and embedded within them. To remove the watermark, the procedure was reversed.

The approach suggests a combination of encryption, watermarking, and error-correcting coding for EPRs [14]. Following DWT and turbo encoding, this approach incorporates the watermarking image (WI) and EPR, respectively. In a subsequent step, we use pallier encryption to create an encrypted watermark by applying an inverse DWT to the embedded data. At the same time, an encrypted cover picture is obtained by encrypting the cover image using a pallier cryptosystem. Cover and watermark pictures are encrypted before being re-embedded and delivered across a communication channel. At the destination, the procedure is reversed in order to get the needed information.

In [15], the authors suggest a crypto watermarking approach that might be useful for telemedicine. For telemedicine purposes, EPR data may be concealed in the retinal picture by framing a blind WS, as described in [16]. After the retinal picture is divided into subbands, the EPR watermark is applied to the lower subband (LL) and then it undergoes SVD. The first stage involves extracting the bit plane from the host picture and then incorporating the watermark image into it using a chaotic mapping approach.

For the purpose of detecting altered medical photos using a crypto WS, more study is suggested in [17]. The EPR is included into the radiological pictures for identification and security purposes, but it is not a blind watermarking system. This method applies DCT on a host picture and uses compressive sensing (CS) to encrypt the data used as a

watermark. Using a two-stage watermarking technique, the authors of [18] sought to incorporate patients' two biometrics—fingerprints and faces. At first, the fingerprint was secured by extracting minute details from the original facial picture and encrypting them with a key. To get the second degree of WI, the watermarked picture was then encrypted and integrated into the original fingerprint. Lastly, the encrypted watermark picture and the DCT subbands were combined to embed the watermark.

All of the aforementioned works deal with various transform domains for use in picture watermarking. In order to embed the watermark, they use several transformation techniques, the most popular of which are DWT, DCT, and LWT, and they follow various watermarking methodologies depending on extraction. We used crypto methods to preserve the watermark since previous watermarking strategies were inadequate in protecting the watermark data. In order to circumvent authentication issues, the suggested watermarking method incorporates a QR code watermark. The suggested method uses a chaotic logistic map to transform the text data into a QR picture that is both distorted and unintelligible. Data is encrypted and decrypted using the public and private keys. The suggested approach combines DWT and SVD with adaptive embedding factor values for pictures to circumvent the images' susceptibility to assaults. The suggested method yields four subbands—LL, LH, HL, and HH—following a single level of LWT. LL is chosen because of how efficient it is. Once again, the LL subband is QR-decomposed, and the scrambled QR code watermark is embedded. The goal of combining these two elements is to make them more resilient and difficult to detect. Applying DWT coefficients provides the increases in robustness. A secret key is used to change the DWT coefficients, which embeds the watermark. At the receiving end, the watermark data is recovered by using the inverse technique.

3. Frameworks and Backgrounds for Image

Watermarking Thanks to the proliferation of worldwide computer networks, the web, and multimedia systems, digital material may now be readily disseminated via many forms of communication. In order to prevent unauthorized access, reproduction, alteration, use, and dissemination of digital information throughout communications, data processing, and storage, digital image watermarking can be used as a research area to build a platform for scholars.

Watermarks on paper have been around since at least 1282; therefore, digital watermarking methods have advanced by taking paper configuration, quality, and quantity into account. The usage of watermarks to increase security has been widespread [4]. In 1988, digital watermarking technology was introduced, which offered secrecy, integrity, and availability. Since 1995, many advances in digital picture watermarking have been implemented. A watermark is a symbol of ownership that is placed into a host signal and may subsequently be retrieved using watermarking methods. The invisible or visible watermark data may be a single bit, a sequence of bits, or even many samples from the host signal [5].

Digital picture watermarking relies heavily on information entropy to mimic the human visual perception system. A digital picture watermarking system may use information entropy using a Just Noticeable Difference (JND) model to attain an ideal balance between imperceptibility, resilience, and capacity [6].

The masking effect provides a definition for information entropy, which may be used to find the data insert sites. Better robustness and imperceptibility are achieved in this situation, but perceptual distortion is minimized. An first step in encrypted message transmission is the creation of a cover picture, also known as a host image. A host picture could be nothing more than background noise, background noise with additional information, or a multimedia message in need of transmission.

The data with watermarks travels over a transmission channel, which might be noisy, unreliable, or lossy. As a result, there is a chance that the received data will vary from the original

watermarked data due to potential assaults such as lossy compression, geometric distortion, signal processing procedures, and signal conversion [8]. Noise is introduced into a watermarked picture while it travels across a communication channel. An rise in the average level of uncertainty or ambiguity in a picture is caused by this noise, which maximizes the information entropy [9].

This means that high-resolution, intricately patterned photos with a high information entropy are the only ones that can be watermarked. Consequently, for security purposes, it is necessary to process the encoded picture in a way that ensures robust image reconstruction. One novel approach to optical image encoding uses a random-phase encoding technique on the input and Fourier planes to get the encoded picture [10].

In this method, two deformable mirrors stand in for the two random phase plates on the input and Fourier planes, respectively. So, using the image's amplitude and phase data, the system may shape beams arbitrarily [11]. There are two steps to digital picture watermarking: embedding the watermark and extracting it. This ensures a safe communication architecture. Before finding the picture's integrating capacity information, the cover image is pre-processed in the watermark embedding portion. Then, the image's entropy is assessed. The encoder then uses a secret key to include a watermark picture into the host image, which has a high entropy value, using an optical image encoding approach.

The system then creates the watermarked picture after obtaining the laser beam's amplitude and phase shaping information. Figure 2 shows the component for inserting the watermark. The last phase, watermark extraction, involves preprocessing the watermarked picture. The system then takes the laser beam patterns and uses them to derive information about the amplitude and phase shaping. Afterwards, these beam patterns' entropy is calculated. When extracting the watermark, a high entropy value is used for improved resilience and imperceptibility.

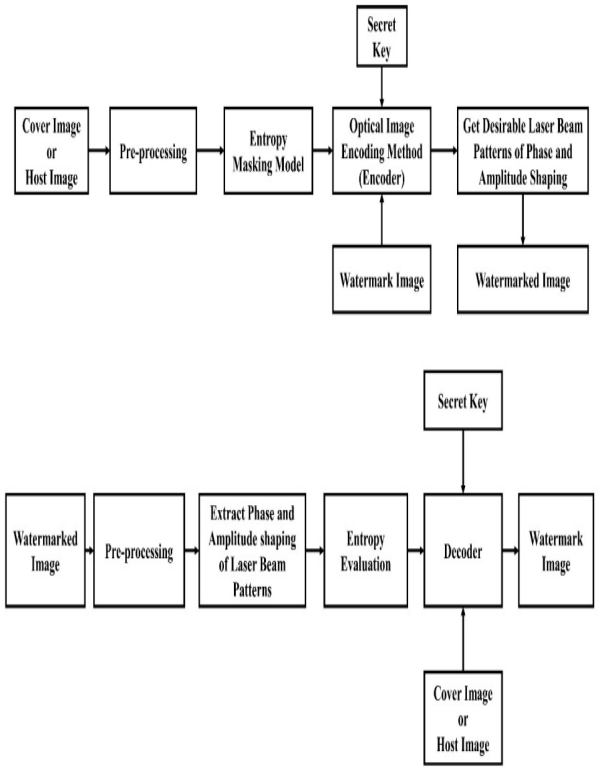

Figure 2. (a) Watermark embedding and (b) watermark extraction.

4. Picture Watermarking System Design Criteria

In order to prevent the unauthorised alteration of multimedia files and to guarantee their validity, digital picture watermarking methods insert a watermark into the data [12]. Therefore, the following sections will outline the necessities or features of a watermarking system. Figure 3 shows the steps needed for watermarking methods. These specifications assess the efficacy of watermarking systems according to their intended uses.

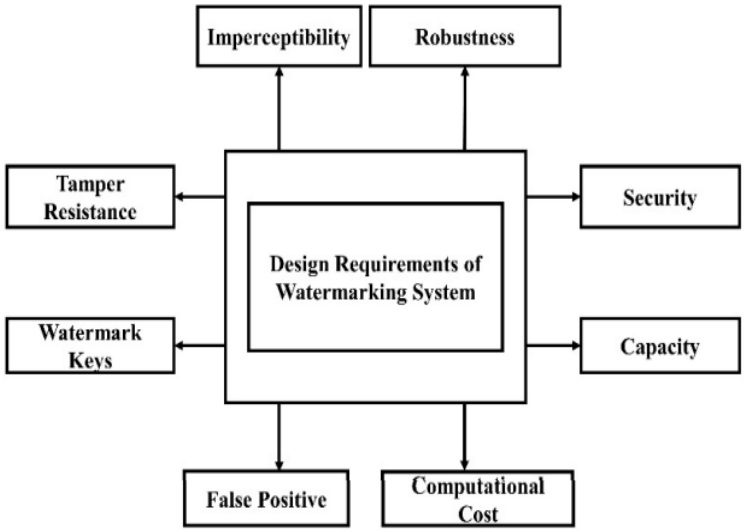

Figure 3: Specifications for a system that watermarks images

Applying Watermarks to Digital Images

Because of its possible use in media applications including copyright protection, annotation, privacy control, data authentication, device management, media forensics, and medical reporting (e.g., X-rays), digital picture watermarking is a highly concentrated field of study. Several related uses of digital picture watermarking are shown in Figure 4.

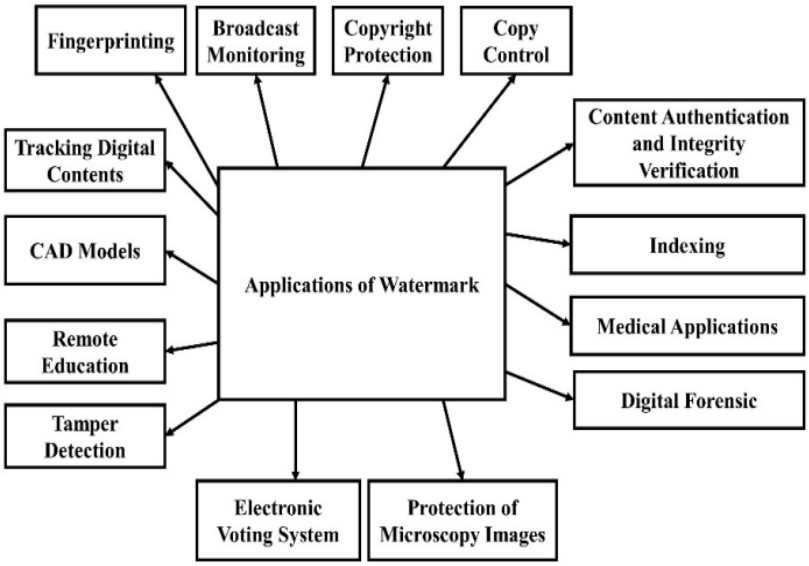

Figure 4: Other uses for digital picture watermarking.

Table 1: Design criteria and their associated applications.

Requirements	Applications
Imperceptibility	Copyright protection and fingerprinting.
Robustness	Copyright protection, content authentication, and integrity verification
Security	Copyright protection, data authentication, fingerprinting and tracking to digital contents, indexing, medical applications, and telemedicine data exchange.
Capacity	Tamper detection and integrity of medical images.
Computational cost	Protection of microscopy images.

5. A Comprehensive Review of Watermarking Methods for Digital Images

Researchers have taken an interest in digital picture watermarking because of its accessibility and the redundant information it delivers. These methods prevent unauthorized individuals from accessing or tampering with digital material. Several uses need these methods, including verification, operator recognition, material security, and trademark protection. Figure illustrates how digital picture watermarking approaches may be categorized according to the working domain, document types, algorithm characteristics, human perception, and application type.

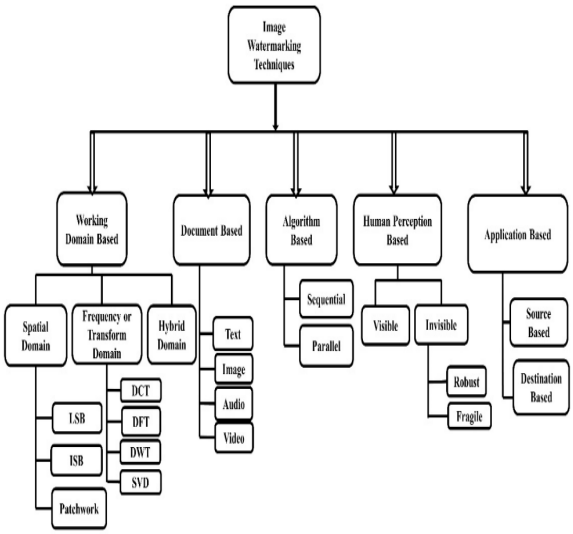

Figure 5: Approaches to picture watermarking categorization

Digital image watermarking methods vary according to operating domain (spatial, frequency, or hybrid), document type (text, image, audio, or video), algorithm type (sequential or parallel), human perceptibility (visible or invisible), and application type (source or destination-based). By reviewing key findings from recent studies, this section compares and contrasts different digital picture watermarking techniques according to their respective working domains. Research on cutting-edge watermarking techniques in the future will find this section useful.

Conclusion

Final Thoughts and Plans for the Future thanks to the interactive and digital transmission of multimedia data, information may now be effortlessly replicated. Digital picture watermarking has emerged as a major area of study due to this problem. To ensure the digital security of images, authenticate them, verify their integrity, identify tampering, and protect copyrights, digital picture watermarking using diverse approaches has become an essential tool. Here, we took a look at

the most popular cutting-edge watermarking methods.

The results of this research show that DWT, with its multi-resolution capabilities, is a reliable and high-quality method for watermarking images. An effective watermarking system must meet three primary criteria: robustness, imperceptibility, and capacity. On the other hand, meeting all of these demands at once is quite difficult. Consequently, it is essential to strike a reasonable balance between these three demands. Digital picture watermarking solutions still face significant security challenges and researchers are faced with the additional issue of accommodating authentication techniques based on blockchain technology and the Internet of Things. The aforementioned three criteria may be satisfied in future study by integrating methods from diverse fields. Researchers should also concentrate on creating new, sophisticated approaches that increase security and robustness simultaneously.

REFERENCES

1. Tao, H.; Chongmin, L.; Zain, J.M.; Abdalla, A.N. Robust Image Watermarking Theories and Techniques: A Review. J. Appl. Res. Technol. 2014, 12, 122–138.
2. Zhang, Y. Digital Watermarking Technology: A Review. In Proceedings of the ETP International Conference on Future Computer and Communication, Wuhan, China, 6–7 June 2009; pp. 250–252.
3. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. Digital Watermarking and Steganography, 2nd ed.; The Morgan Kaufmann Series in Multimedia Information and Systems: Burlington, Massachusetts, 2008.
4. Mohanarathinam, A.; Kamalraj, S.; Venkatesan, G.P.; Ravi, R.V.; Manikandababu, C.S. Digital Watermarking Techniques for Image Security: A Review. J. Ambient Intell. Humaniz. Comput. 2019, 1–9. doi: https://doi.org/10.1007/s12652-019-01500-1.
5. Cox, I.J.; Miller, M.L. A Review of Watermarking and the Importance of Perceptual Modeling. In Human Vision and Electronic Imaging II; San Jose, CA, United States : 1997; Volume 3016.
6. Yang, Q.; Zhang, Y.; Yang, C.; Li, W. Information Entropy Used in Digital Watermarking. In Proceedings of the 2012 Symposium on Photonics and Optoelectronics, Shanghai, China, 21–23 May 2012; pp. 1–4.
7. Yu, C.; Li, X.; Chen, X.; Li, J. An Adaptive and Secure Holographic Image Watermarking Scheme. Entropy 2019, 21, 460.
8. Kumar, V.A.; Rao, C.H.S.; Dharmaraj, C. Image Digital Watermarking: A Survey. Int. J. Adv. Manag. Technol. Eng. Sci. 2018, 8, 127–143.
9. Jaynes, E.T. Prior probabilities. IEEE Trans. Syst. Sci. Cybern. 1968, 4, 227–241.
10. Refregier, P.; Javidi, B. Optical Image Encryption based on Input Plane and Fourier Plane Random Encoding. Opt. Lett. 1995, 20, 767–769.
11. Wu, C.; Ko, J.; Rzasa, J.R.; Paulson, D.A.; Davis, C.C. Phase and Amplitude Beam Shaping with Two Deformable Mirrors Implementing Input Plane and Fourier Plane Phase Modifications. Appl. Opt. 2018, 57, 2337–2345.
12. Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. A digital watermark. In Proceedings of the IEEE 1st International Conference on Image Processing, Austin, TX, USA, 13–16 November 1994; Volume 2, pp. 86–90.
13. Singh, A.K. Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. Multimed. Tools Appl. 2019, 78, 30523–30533.
14. Anand, A.; Singh, A.K. Joint watermarking-encryption-ECC for patient record security in wavelet domain. IEEE MultiMedia 2020, 27, 66–75.
15. Kaur, G.; Agarwal, R.; Patidar, V. Crypto-watermarking of images for secure transmission overcloud. J. Inf. Optim. Sci. 2020, 41, 205–216.
16. Zermi, N.; Khaldi, A.; Kafi, R.; Kahlessenane, F.; Euschi, S. A DWT-SVD based robust digital

watermarking for medical image security. Forensic Sci. Int. 2021, 320, 110691.
17. Borra, S.; Thanki, R. Crypto-watermarking scheme for tamper detection of medical images. Comput. Methods Biomech. Biomed. Eng. Imaging Vis. 2020, 8, 345–355.
18. Lebcir, M.; Awang, S.; Benziane, A. Robust blind watermarking approach against the compression for fingerprint image using 2D-DCT. Multimed. Tools Appl. 2022, 81, 20561–20583.
19. Zhou, X.; Tang, X. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of the IEEE 2011 6th International Forum on Strategic Technology, Harbin, China, 22–24 August 2011; Volume 2, pp. 1118–1121.
20. Shensa, M.J. The discrete wavelet transform: Wedding the a trous and Mallat algorithms. IEEE Trans. Signal Process. 1992, 40, 2464–2482.
21. Vaidya, S.P. A blind color image watermarking using brisk features and contourlet transform. In Proceedings of the International Conference on Recent Trends in Image Processing and Pattern Recognition, Solapur, India, 21–22 December 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 203–215.
22. Vaidya, S.P.; PVSSR, C.M.; Santosh, K.C. Imperceptible watermark for a game-theoretic watermarking system. Int. J. Mach. Learn. Cybern. 2019, 10, 1323–1339.
23. Nason, G.P.; Silverman, B.W. The discrete wavelet transform in s. J. Comput. Graph. Stat. 1994, 3, 163–191.
24. Van Fleet, P.J. Discrete Wavelet Transformations: An Elementary Approach with Applications; John Wiley & Sons: Hoboken, NJ, USA, 2011.
25. Chang, C.; Girod, B. Direction-adaptive discrete wavelet transform for image compression. IEEE Trans. Image Process 2007, 16, 1289