*International Journal of Innovative Research in Technology and Science*
ISSN: 2321-1156 www.ijirts.org Volume 11 Issue 3, May 2023

# Review of Digital Image Watermarking Based on DWT and DCT Methods

Astha Rani, Aditi Purohit, Rajesh Boghey
Department of CSE, TIT, RGPV, Bhopal, India
dwivediasth2310@gmail.com, khushi.aditi@gmail.com, rajeshboghey@gmail.com

*Abstract* - Digital watermarking has recently gained significant attention as a prominent research topic, thanks to the remarkable computer and internet technology advancements. Digital watermarking serves as an effective solution to combat illegal copying, modification, and redistribution of multimedia data such as audio, images, and videos. This paper provides a concise overview of different techniques for image watermarking in both the spatial domain and the transform domain. The authors propose a novel digital watermarking algorithm for grey images based on the discrete wavelet transform (DWT), two-dimensional discrete cosine transform (DCT), and singular value decomposition (SVD). The objective is to achieve robust watermarking of digital images to protect digital media copyright efficiently. A comprehensive survey on digital image watermarking is conducted, focusing on hybridising Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) with SVD. While established watermarking algorithms demonstrate their robustness, there is still room for exploration in areas like principal component analysis and redundant and feature extraction-based hybridisation of transforms as alternatives to SVD to enhance performance further. The proposed and existing DCT-based methods are evaluated by comparing their peak signal-to-noise ratio (PSNR) and robustness against various attacks. The paper also discusses different attack scenarios in detail.

*Keywords: Watermarking, DCT (Discrete Cosine Transform), PSNR (Peak Signal-to-Noise Ratio), Robustness, Spatial Domain, Transforms Domains, Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Watermark Detection.*

## I. INTRODUCTION

Watermarking is a technique used to embed a pattern of bits into digital files such as images, audio, or videos, which identifies the file's copyright information, including authorship and rights. The watermark bits are distributed throughout the file, making them difficult to detect and manipulate. Digital watermarking ensures that the concealed information remains hidden unless special software is used to extract it. Two main types of algorithms are used for watermarking: spatial domain and transformed domain. Spatial domain watermarking involves modifying the pixel values of randomly selected subsets of images. It directly alters the raw data within the image pixels. This can be achieved using different patches or manipulating the least significant bit planes [1].

On the other hand, transformed domain watermarking relies on modifying transform coefficients using commonly used transforms such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). While encryption can protect multimedia content from unauthorised access, the data can be illegally duplicated and distributed once decrypted. Digital watermarking provides an effective solution to prevent such illegal duplication. It enables copyright protection, data authentication, and content identification. However, achieving effective copyright protection requires meeting certain basic requirements, including imperceptibility, robustness, capacity, and security. These requirements often conflict, necessitating a trade-off to strike the right balance between them. Increasing the data rate in watermarking systems can lead to a decrease in the quality of the watermarked image and a reduction in robustness against attacks [2]. The basic model of image watermarking is illustrated in Figure 1, comprising a watermark embedder, a communication channel, and a watermark detector. The watermark embedder takes the image and covers images as inputs to generate a fully watermarked image. This watermarked image is then transmitted through the communication channel, which can be subject to various attacks and noise. Ultimately, the watermark

is extracted using a watermark detector. To ensure the effectiveness of digital watermarking techniques, they must be resilient against noise and security attacks encountered in the communication channel. In spatial domain digital image watermarking methods, the watermark is directly incorporated into the host image by altering the image characteristics or manipulating pixels. Digital watermarking involves the insertion of an invisible data stream, known as a watermark, into a multimedia signal. Many proposed methods require a secret key during the embedding and extraction processes, making it impossible to embed or extract the watermark without utilising it.

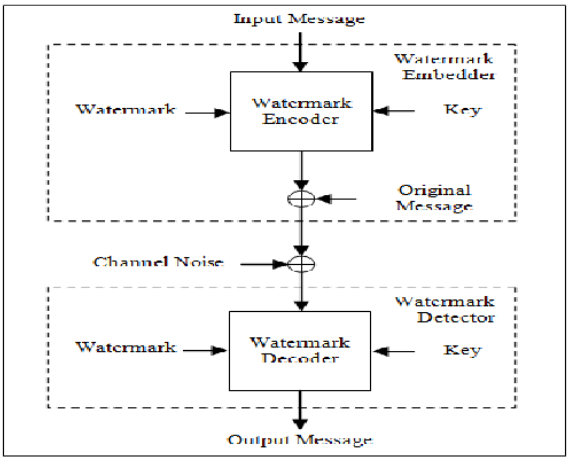

Figure 1 Digital watermarking model

There has been a growing interest in watermarking to protect multimedia signals. The need for effective copyright protection methods for digital images, sounds, and videos has been a significant driver for research in this field. One watermarking application embeds a serial number into the signal to enhance security and enable identification. Consequently, an attacker's objective is to remove the watermark by manipulating the watermarked signal. In order to counter this, the watermark must be pervasive, making it extremely difficult, if not impossible, to erase without the appropriate key, even if it means severely distorting the marked signal. Digital watermarking involves inserting a hidden message into a digital file by transforming it into a watermark domain and modifying its coefficients. The marked signal is then generated by inversely transforming the modified coefficients. The proposed approach aims to improve upon a general class of watermarking methods with the following key characteristics: the watermark data stream consists of binary elements, the host signal (i.e., unmodified multimedia signal) is not accessible or used during watermark extraction, the watermark is duplicated and distributed across different parts of the watermark domain while maintaining uniform distribution throughout the signal. In order to protect digital media, such as images, the technique of digital watermarking is employed [2]. This method involves applying algorithms to digitally broadcasted content, wherein a secret information or watermark is inserted. Subsequently, the concealed data can be extracted using the corresponding algorithm. Digital watermarking serves as a system to provide evidence of data integrity and protect intellectual property. In image watermarking, the image is utilised to hide digital information, which is an effective approach for safeguarding pictures on the web. This process involves adding metadata to an image, which can be read or captured to verify ownership. In order to ensure the effectiveness of watermarking as a robust means of protecting intellectual property, watermarks must exhibit high resilience against various threats. A watermark's robustness can be determined by its ability to withstand attempts at damaging or tampering with it. Robust watermarking is commonly employed to sign the copyright information of digital works, as the embedded watermark remains difficult to decipher even after being subjected to common attacks such as editing, image processing, and lossy compression [3].

A. Applications of Watermarking

The following is a discussion of some active application areas, descriptions of relevant reference technologies and case studies highlighting typical real-world use cases. While digital images are predominantly used as examples, it is important to note that watermarking can also be applied to audio and video files [4].

(a) Copyright Protection: Watermarking is commonly used to secure digital media against unauthorised duplication. In the digital realm, it has become effortless for anyone to copy or edit digital data without compromising its integrity, leading to a surge in copyright violations. By embedding watermarks that identify the original media and specify its authorised uses, digital watermarking strengthens the content protection chain and discourages the illegal distribution of copyrighted content. Devices can detect watermarks during media streaming or copying. If unauthorised use is detected, the file playback or

copying is prevented, accompanied by warning messages. Copyright holders, distributors, and content owners benefit from copyright protection measures, safeguarding their work against piracy threats such as TV camera recording, file sharing, format changing, encryption, and processing conducted through peer-to-peer (P2P) networks [5].

(b) Image Data Security: Each copy of a confidential document will have a digital watermark added to it as it is created and shared. This ensures that any accidentally or maliciously shared information can be traced back to its original source, as each copy carries a watermark with specific information about its intended audience. Businesses implement network detectors and email filters to scan various file types for digital watermarks, informing relevant authorities of any attempt to transmit the data externally (via email or the internet) in case of compromise. Similarly, printers, scanners, and other devices are equipped with watermark detectors to detect watermarks while duplicating confidential documents. In such cases, the watermark triggers actions similar to "do not copy or scan" messages. Therefore, it is crucial to protect sensitive documents and images by generating a unique digital signature for each duplicate of a private file, investigating leaks or accidental sharing of sensitive information, filtering documents before posting them online or forwarding them via email, and avoiding multiple copies or scans of sensitive documents [6].

## II. LITERATURE SURVEY

In Chang et al., the discrete cosine transform (DCT) is mentioned as a method related to the Fourier transform. It uses frequency space instead of amplitude space to represent information, which aligns better with human perception of light and allows for the elimination of unused parts. DCT-based watermarking techniques are known to offer better security compared to spatial domain techniques. These methods can withstand standard image processing adjustments such as brightness, contrast, blurring, and low pass filtering with minimal quality loss. However, they are computationally expensive and vulnerable to geometric attacks like rotation and scaling. DCT watermarking can be applied at the global level or block-based manner. When inserting content into an image, it is advisable to choose areas that won't detract from the viewer's perception of the image [7]. In Wei Zheng et al., a fast discrete cosine transform (DCT) algorithm for JPEG compression is demonstrated. The algorithm's efficiency is discussed, highlighting the effectiveness of the binary DCT in particular. The binary DCT simplifies the transformation process and can be computationally efficient due to replacing multiplication with shifting and adding operations. It is suitable for low-latency, high-throughput, and low-power multimedia processing. The binary DCT algorithm effectively achieves JPEG compression with results comparable to regular JPEG encoding [8]. Giulia Fracastoro et al. proposes a directional discrete cosine transform (DCT) to improve compression results for images with blocks containing arbitrarily shaped discontinuities. The steerable DCT (SDCT) is introduced as an enhancement that matches the directionality of each image block by rotating pairs of basis vectors. The proposed approach utilises rate-distortion (RD) optimisation to determine the ideal rotation angles for SDCT. Iterative methods are employed to find the optimal angles, and a fully functional image encoder is developed for evaluation. Comparisons with DCT and other directional transforms demonstrate the superior performance of SDCT in analytical and numerical tests [9]. H. Dong et al. proposes a secure watermarking scheme for Depth Image-Based Rendering (DIBR) 3D images using the dual-tree complex wavelet transform (DT-CWT). The coefficients of DT-CWT are quantised to create the watermarking scheme. UV filters are applied to consider shift invariance and directional selectivity, properties specific to DIBR. The threshold is set to minimise false positives during watermark extraction. The proposed method shows that the watermark can be reliably removed by considering only the central viewpoint, even when general attacks distort the synthesised left and right views. The method also demonstrates robustness against baseline adjustment and depth image pre-processing [10]. In P. Dabas et al., digital watermarking is discussed as a solution to combat the illegal duplication of digital files, which has become more prevalent with the widespread availability of the internet. The paper examines the three most common watermarking methods and the performance metrics used to assess their effectiveness. By understanding these methods and metrics, novel approaches can be developed to enhance the robustness of watermarking against various attacks [11]. Khan et al. present a weak zero watermarking scheme for detecting and characterising malicious updates to a

database relation. This method leaves no distortion in the database and distinguishes between benign and malicious insertions, deletions, and changes. It constructs a database watermark by generating sub-watermarks based on location-specific properties of digits, length, and range of data in the database. By comparing the watermark of the suspect database to the original database watermark, any updates to the data can be identified. This approach enables the detection and characterisation of database manipulation techniques [12]. In Amirgholipour et al., a novel algorithm for digital image watermarking is proposed, which combines discrete wavelet transform (DWT) with discrete cosine transform (DCT). The watermark is encoded using an Arnold cat map within a 3-level DWT of a numerical image. The DCT transform is applied to each DWT sub-band, with the watermark encoded in the DCT coefficients related to the central frequency. Pre-filters such as sharpening and Laplassian or Gaussian filters enhance the contrast between the host image and the watermark data. The proposed algorithm provides greater robustness against common signal processing attacks and maintains imperceptibility. It outperforms existing watermarking algorithms that rely solely on DWT and DCT [13]. Fotopoulos et al. discuss a sub-band discrete cosine transform (DCT) method for image watermarking. The unique copy of the image is divided into four segments, and DCT is applied to each segment. The watermark is encoded in the DCT coefficients of each segment. This method utilises multiple frequency ranges, each providing a unique detection signal. A more secure watermarking scheme is achieved by averaging the detection rates across all frequency ranges [14]. In Behal et al., the comparison between frequency-domain and spatial-domain watermarking techniques is highlighted. Watermarking is typically performed in the frequency domain using transforms like DCT, DFT, and DWT, as spectral coefficients better represent human sensory system characteristics.

## III. Expected Outcome

In digital watermarking, various techniques have been developed to protect the copyright of multimedia objects, such as images. This paper focuses on the frequency-domain method using discrete cosine transform (DCT). However, the traditional DCT-based approach often exhibits a low peak signal-to-noise ratio (PSNR). We propose a novel method to overcome this limitation to achieve high PSNR, excellent robustness, and the best possible outcomes.

## IV. CONCLUSION

Digital watermarking is a dynamic and evolving field that offers a promising solution for protecting the copyright of multimedia information and ensuring the secure utilisation of multimedia content. This paper has provided an overview of digital watermarking in the spatial domain, highlighting its potential to safeguard digital data such as images, audio, and video from unauthorised access or usage. Furthermore, we have explored various applications of watermarking techniques in the spatial domain. Through extensive literature reviews, it can be concluded that significant research efforts have been dedicated to watermarking in the frequency-domain method. Numerous digital image watermarking models utilising techniques such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) has been investigated to minimise mean square error and improve the peak signal-to-noise ratio (PSNR). While considerable progress has been made in developing efficient digital image watermarking techniques using DCT, there is still room for exploration in areas such as principal component analysis, redundant and feature extraction-based watermarking, and transform-based methods to enhance performance metrics like PSNR and robustness. In conclusion, digital watermarking continues to be a promising field with ongoing research and development efforts. We can effectively protect digital assets and enhance their security in various applications by harnessing the potential of watermarking techniques in both spatial and frequency domains.

## REFERENCES

[1]. Z. Brahimi, H. Bessalah, A. Tarabet, and M. K. Kholladi, “Selective Encryption Techniques of JPEG2000 Codestream for Medical Images Transmission,” WSEAS Transactions on Circuits and Systems, Vol. 7, No. 7, 2008, pp. 718-727.

[2]. Su, J.K., F. Hartung, and B. Girod, "Digital Watermarking of Text, Image, and Video Documents," University of Erlangen- Nuremberg, Erlangen, 1999.

[3]. YI. Khamlichi, M. Machkour, K. Afdel, and A. Moudden, “Medical Image Watermarked by Simultaneous Moment Invariants and Content-Based for Privacy and Tamper Detection,” 6th

WSEAS International Conference on Multimedia Systems & Signal Processing, China, April 16-18, 2006, pp. 109-113.

[4]. O. Cadet, "Methods d'ondelettes pour la segmentation d'images: Applications à l'imagerie médicale et au tatouage d'images." PhD Thesis at the Polytechnic Institute of Grenoble, University of Grenoble, 2004, France.

[5]. M.A Hajjaji, A. Mtibaa, E. Bourennane, "Watermarking of Medical Image: Method Based on 'LSB'," Journal of Emerging Trends in Computing and Information Sciences, Volume 2, Issue 12, December 2011, pp. 714-721.

[6]. Hien TD, Nakao Z, Chen YW. "Robust multi-logo watermarking by RDWT and ICA," Signal Process 2006;86(10):2981–93.

[7]. M. Kaur, S. Jindal, S. Behal, "A Study of Digital Image Watermarking," Volume 2, Issue 2, 2012.

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

[9]. Wei Zheng; Yanchang Liu, "Research in a fast DCT algorithm based on JPEG," Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on, 16-18 April 2011.

[10]. Fracastoro, Giulia, Sophie M. Fosson, and Enrico Magli. "Steerable discrete cosine transforms," IEEE Transactions on Image Processing, vol. 26, no. 1, pp. 303-314, 2016.

[11]. Hee-Dong, Kim, "Robust DT-CWT watermarking for DIBR 3D images," IEEE Transactions on Broadcasting, vol. 58, no. 4, pp. 533-543, 2012.

[12]. P. Dabas, K. Khanna, "A Study on Spatial and Transform Domain Watermarking Techniques," International Journal of Computer Application, vol. 71, no. 14, pp. 38-41, 2013.

[13]. Khan A, Husain SA. "A fragile zero watermarking Scheme to detect and characterise malicious modifications in database relations," The Scientific World Journal, 16 pages, 2013.

[14]. Amirgholipour, Saeed K., and Ahmad R. Naghsh-Nilchi. "Robust digital image watermarking based on joint DWT-DCT," International Journal of Digital Content Technology and its Applications, vol. 3, no. 2, pp. 42-54, 2009.

[15]. V. Fotopulos, A.N. Skodras, "A Subband DCT Approach to Image Watermarking," 10th European Signal Processing Conference 2000 (EUSIPCO'00), Tampere, Finland, September 2000.

[16]. Singh, Neha, Mamta Jain, and Sunil Sharma. "A Survey of Digital Watermarking Techniques," International Journal of Modern Communication Technologies and Research, vol. 1, no. 6, pp. 265852, 2013.

[17]. Guru, Jaishri, and Hemant Damecha. "Digital watermarking classification: a survey," International Journal of Computer Science Trends and Technology (IJCST), vol. 5, pp. 8-13, 2014.

[18]. Nasir, Ibrahim, Ying Weng, and Jianmin Jiang. "A new robust watermarking scheme for the colour image in the spatial domain," 2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, pp. 942-947, 2007.

[19]. Medeni, MB Ould, and El Mamoun Souidi. "A novel steganographic method for grey-level images with four-pixel differencing and LSB substitution," 2011 International Conference on Multimedia Computing and Systems, pp. 1-4, 2011.

[20]. Pandian, Nithyanandam, and Ravichandran Thangavel. "A hybrid embedded steganography technique: optimum pixel method and matrix embedding," Proceedings of the International Conference on Advances in Computing, Communications, and Informatics, pp. 1123-1130, 2012.