Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

Implementation and Analysis of Hybrid DCT-DWT Digital Watermarking

Amirth Raj Puramcheriyil
Computer Science and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu

***Abstract*—The easy sharing of multimedia has been made possible by technological advancements in the last two decades. As a result, the challenge of attacking and manipulating digital material has become a crucial issue. Various solutions have been developed to safeguard such shared media files against illegal access to such data and media in order to avoid this. Digital watermarking is now widely utilized in practically every industry to secure and safeguard one's data' copyright and protection.**

***Keywords*—**DCT, DWT, Digital watermarking, attacks, authentication

I. INTRODUCTION

In the era of rapid technological advancements, the seamless sharing of multimedia has become an integral part of our daily lives. However, this convenience brings forth a pressing challenge – the vulnerability of digital material to unauthorized access and manipulation. As a response to this challenge, various solutions have emerged to protect shared media files from illicit use and infringement. Among these, digital watermarking has risen to prominence, offering a robust mechanism to secure data copyright and safeguard digital assets.

Digital watermarking involves the embedding of a digital code or image, whether visible or covert, within multimedia content. This practice has found widespread application across diverse industries, serving as a crucial tool in verifying the authenticity and ownership of digital media. At its core, digital watermarking acts as a security measure, acting as a deterrent against piracy while facilitating the traceability of copyright infringements through embedded source tracking codes.

The effectiveness of a digital watermark depends on a myriad of features and capabilities, each tailored to its intended purpose. Whether seamlessly integrated into the image itself or applied as part of the signal processing, the design and placement of watermarks play a pivotal role in ensuring their successful enforcement. To enhance their robustness, modern digital watermarks often incorporate a blend of signal amplitude, large bandwidth sizes, and short message lengths. Additionally, the integration of mixed domain techniques, combining spatial and frequency domain watermarks, is considered a strategic approach to fortify watermarks against hacking attacks.

An intriguing aspect of digital watermarks lies in their imperceptibility under specific conditions, requiring algorithms for detection. The effectiveness of a digital watermark hinges on its ability to remain inconspicuous while withstanding attempts at removal or distortion. Unlike traditional watermarks applied to visible media, such as images or videos, digital watermarks can be embedded in a diverse range of signals, including audio, pictures, video, texts, or 3D models. Notably, a single signal may carry multiple watermarks simultaneously without altering the size of the carrier signal.

This research paper delves into the realm of hybrid digital watermarking, exploring the integration of various techniques to enhance the robustness and versatility of digital watermarks. Through the implementation and analysis of hybrid approaches, this study aims to contribute valuable insights into the evolving landscape of digital content protection, addressing the challenges posed by modern multimedia sharing environments.

II. LITERATURE SURVEY

The literature survey encompasses a range of papers on digital image watermarking techniques. In "Digital Colour Image Watermarking using DWT-DCT Coefficients in RGB Planes" (Chaitanya et al., 2020), the authors employ DWT and DCT on RGB channels, demonstrating effectiveness in authenticity identification. However, its dependency on RGB color could be limiting. "A Study on Digital Watermarking Techniques" (Robert et al., 2009) reviews various methods, focusing on spatial frequencies. The heavy reliance on pixels poses a vulnerability to distortion. In "Intelligent Image Watermarking" (Ziabari, 2015), genetic algorithms enhance robustness, yet dependency on RGB color and security concerns are noted. "Digital Watermarking Based on DWT and DCT" (Hazim, 2018) finds that combining DWT and DCT yields superior results, although robustness remains an issue for individual methods. Feng et al. (2010) present a robust DWT-DCT algorithm, albeit with interoperability challenges. "Digital Image Watermarking Techniques: A Review" (Begum and Uddin, 2020) evaluates DCT, SVD, DWT, DFT, and LSB, with DCT emerging as the most robust, yet a trade-off among robustness, imperceptibility, and capacity persists. "Digital Color Image Watermarking In RGB Planes Using DWT-DCT-SVD Coefficients" (Chaitanya et al., 2014) combines SVD with DWT and DCT, excelling in robustness but facing interoperability issues. Anilkumar et al. (2011) compare DCT and DWT, revealing efficient compression techniques, though performance reliability varies. "Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform" (Saxena, 2011) demonstrates robustness against various attacks but is susceptible to noise. "Framework of Hybrid Methods of Digital Image Watermarking" (Afrakhteh et al., 2009) combines multiple transform domain methods,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

offering copyright protection but exhibiting less robustness against certain attacks. Various other papers, such as "Design Requirements and Classification of Hybrid Image Watermarking" (Dayananda and Institutions, 2013) and "Digital Watermarking Based on DWT and DCT" (Hazim Barnouti et al., 2018), contribute to the understanding of digital watermarking techniques, highlighting strengths and limitations. Each paper provides valuable insights into the evolving landscape of digital image watermarking.

III. OVERVIEW OF PROPOSED SYSTEM

In an era marked by the pervasive sharing of multimedia content, the necessity for robust methods to protect digital assets against unauthorized access and manipulation has become paramount. This research introduces a sophisticated hybrid watermarking system that amalgamates the capabilities of the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). The proliferation of digital media has given rise to challenges pertaining to copyright infringement and data integrity, necessitating innovative solutions. The proposed system employs a meticulous algorithmic approach, commencing with a two-step DWT decomposition that dissects the cover host image into four non-overlapping sub-bands, capturing both spatial and frequency information. The subsequent integration of DCT within the chosen sub-band further refines the watermarking process, transforming spatial details into frequency components. The algorithm meticulously embeds a grayscale watermark into the mid-band DCT coefficients of 4x4 blocks, guided by two uncorrelated pseudorandom sequences. This not only enhances security but also ensures that the watermark remains imperceptible under specific conditions. The modular structure of the system encompasses key modules, such as DWT Embedding, DWT Extraction, DCT Embedding, and DCT Extraction, each serving a specific role in the watermarking process. This hybrid approach operates in a blind fashion, alleviating the need for the original host image during watermark extraction, thus augmenting its practicality in real-world scenarios. The versatility of the algorithm makes it applicable to a range of data types, offering a robust and secure solution to the challenges posed by the dynamic landscape of multimedia sharing environments.

A. Proposed Methodology

The proposed hybrid watermarking system comprises several intricately designed modules to seamlessly integrate Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) techniques, ensuring a comprehensive and robust approach to secure digital data. In the initial module, "DWT Embedding," users have the liberty to select a watermark according to their preferences, taking into consideration the nature of the data (original or compressed) and the desired visibility of the watermark. The system then meticulously executes the following steps: first, applying DWT to decompose the host image into four non-overlapping sub-bands (LL, LH, HL, HH); second, choosing a sub-band (HL2 or HH2) and dividing it into 4 x 4 blocks; third, applying DCT to each block; fourth, formulating the grayscale watermark into a binary vector; fifth, generating two uncorrelated pseudorandom sequences (PN_0 and PN_1) with the number of elements matching the mid-band elements of the DCT-transformed sub-bands; sixth, embedding the sequences with a gain factor in the mid-band DCT coefficients of the selected sub-band based on the watermark bit (0 or 1); seventh, applying inverse DCT to modify the mid-band coefficients; and finally, applying inverse DWT to produce the watermarked host image.

Moving on to the "DWT Extraction" module, the system skillfully decomposes the watermarked image into frequency channels (LL, LH, HL, HH) at the first level of the DWT domain. This process, achieved through a series of well-defined steps, allows for the extraction of the embedded watermark. The system's adaptability and versatility are enhanced by the optional modules "DCT Embedding" and "DCT Extraction." In "DCT Embedding," the focus is on several key areas, particularly data authentication. Fragile watermarks are employed, ensuring that the watermark cannot be extracted if the data is corrupted. The module involves partitioning the image pixel matrix into blocks of size and representing data in frequency space through DCT. In "DCT Extraction," the system further refines the watermark extraction process, emphasizing the detection of modifiers or processing in the image. Leveraging the orthogonality of the transformation and fast computation algorithms, the system excels in converting the image into its equivalent frequency domain.

In essence, the proposed hybrid watermarking system not only provides users with flexibility in watermark selection but also ensures a meticulous and adaptive integration of DWT and DCT techniques throughout the embedding and extraction processes. The system's optional DCT modules cater to applications requiring heightened security and authentication, demonstrating a sophisticated and comprehensive solution for the protection of digital content.

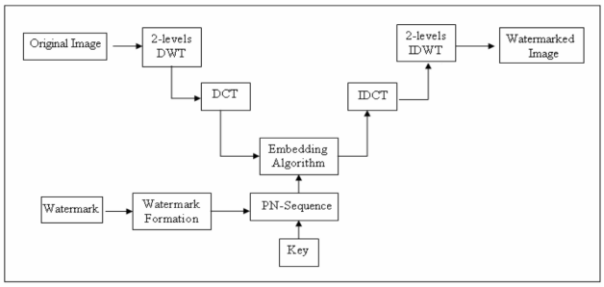

Fig. 1. Hybrid DCT & DWT Embedding Procedure.

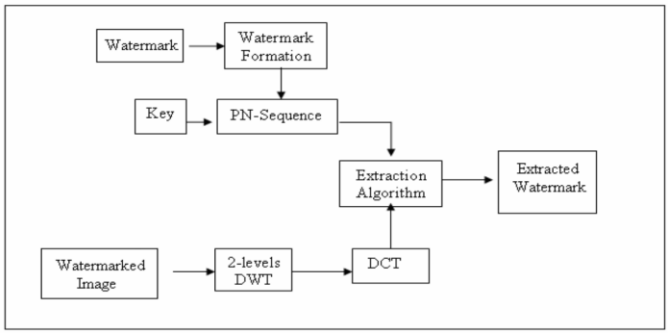

Fig. 2. Hybrid DCT & DWT Extraction Procedure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

B. Algorithm

- Step 1: Apply DWT to decompose the cover host image into four non-overlapping multi-resolution sub-bands: LL1, HL1, LH1, and HH1.
- Step 2: Apply DWT again to sub-band HL1 to get four smaller sub-bands and choose the HL2 sub-band. Or apply DWT to sub-band HH1 to get four smaller sub-bands and choose the HH2 sub-band.
- Step 3: Divide the sub-band HL2 (or HH2) into 4 x 4 blocks.
- Step 4: Apply DCT to each block in the chosen sub-band (HL2 or HH2).
- Step 5: Re-formulate the grey-scale watermark image into a vector of zeros and ones.
- Step 6: Generate two uncorrelated pseudorandom sequences. One sequence is used to embed the watermark bit 0 (PN_0) and the other sequence is used to embed the watermark bit 1 (PN_1). Number of elements in each of the two pseudorandom sequences must be equal to the number of mid-band elements of the DCT-transformed DWT sub-bands.
- Step 7: Embed the two pseudorandom sequences, PN_0 and PN_1, with a gain factor, in the DCT transformed 4x4 blocks of the selected DWT sub-bands of the host image. Embedding is not applied to all coefficients of the DCT block, but only to the mid-band DCT coefficients. If we donate X as the matrix of the midband coefficients of the DCT transformed block, then embedding is done as follows: If the watermark bit is 0 then X ' = X + * PN_0 (3) otherwise, if the watermark bit is 1 then, X ' = X + * PN_1 (4)
- Step 8: Apply inverse DCT (IDCT) to each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.
- Step 9: Apply the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the watermarked host image. The combined DWT-DCT algorithm is a blind watermarking algorithm, and thus the original host image is not required to extract the watermark.

IV. RESULTS AND DISCUSSION

In this study, we began by implementing a digital watermark on an original image to verify and authenticate its originality. To assess the resilience of the watermark against cyber attacks, we subjected the watermarked image to various distortion techniques simulating real-world scenarios. The evaluation involved calculating Peak Signal-to-Noise Ratio (PSNR) values before and after applying attacks, providing a quantitative measure of image quality. The comparison of PSNR values between the original and watermarked images enabled us to gauge the efficacy of the digital watermark in preserving image fidelity.

The following table displays the PSNR value of the recovered image to original image after various attacks on image like rotation, cropping and blurring.

TABLE I. COMPARISON OF PSNR VALUE OF RECOVERED TO ORIGINAL IMAGE

S.No	Comparison of PSNR Value of Recovered to Original Image	
	Type of Attack	**PSNR Value**
1	No attack	40.483
1	90 degree attack	33.010
2	180 degree rotation	33.007
3	Blur	38.520
4	Cropping	34.078

Different types of attacks and their PSNR values

The steganography algorithm employed in this study demonstrates a mix of positive and nuanced aspects in its performance under different attack scenarios. On a positive note, the algorithm showcases commendable robustness, evidenced by a high PSNR value of 40.483 in the absence of any attack, indicating its success in maintaining fidelity during information recovery. However, under specific challenges like a 90-degree rotation, 180-degree rotation, blur, and cropping, the PSNR values decrease to 33.010, 33.007, 38.520, and 34.078, respectively, signaling a slight reduction in image quality. While these fluctuations suggest some sensitivity to certain attacks, the algorithm remains relatively resilient overall. This indicates that while the steganography algorithm is effective in preserving hidden information under typical conditions, users should be mindful of its response to specific adversarial scenarios. These findings provide valuable insights into the algorithm's strengths and areas for potential improvement, contributing to a more informed consideration of its suitability for applications requiring secure information concealment.

V. CONCLUSION AND FUTURE WORKS

In conclusion, our project has successfully achieved its primary objective. Through the hybrid implementation of diverse image watermarking algorithms, we have effectively secured images by embedding a digital watermark. This watermark serves as a robust ownership identity, ensuring exclusive rights for the original copyright owner. The implemented strategy not only fortifies image security but also provides a valuable asset for copyright claims, especially in legal contexts. Overall, our project's outcome underscores the significance of digital watermarking in safeguarding image rights and establishing ownership authenticity.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

REFERENCES

[1] Chaitanya, K., Reddy, E. S., & Rao, K. G. (2013). Digital Color Image Watermarking using DWT-DCT Coefficients in RGB Planes. Global Journal of Computer Science and Technology.
[2] Katharotiya, A., Patel, S., & Goyani, M. (2011). Comparative analysis between DCT & DWT techniques of image compression. Journal of information engineering and applications, 1(2), 9-17.
[3] Ziabari, S. S. M. (2015, November). Intelligent image watermarking robust against cropping attack. In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI) (pp. 1203-1206). IEEE.
[4] Robert, L., & Shanmugapriya, T. (2009). A study on digital watermarking techniques. International journal of Recent trends in Engineering, 1(2), 223.
[5] Begum, M., & Uddin, M. S. (2020). Digital Image Watermarking Techniques: A Review. Information, 11, 110.
[6] Barnouti, N. H., Sabri, Z. S., & Hameed, K. L. (2018). Digital watermarking based on DWT (discrete wavelet transform) and DCT (discrete cosine transform). International Journal of Engineering & Technology, 7(4), 4825-4829.
[7] Feng, L. P., Zheng, L. B., & Cao, P. (2010, July). A DWT-DCT based blind watermarking algorithm for copyright protection. In 2010 3rd International Conference on Computer Science and Information Technology (Vol. 7, pp. 455-458). IEEE.
[8] Saxena, D. (2011). Digital watermarking algorithm based on singular value decomposition and Arnold transform.23
[9] Chaitanya, K., Reddy, E. S., & Rao, K. G. (2013). Digital Color Image Watermarking using DWT-DCT Coefficients in RGB Planes. Global Journal of Computer Science and Technology.
[10] Begum, M., & Uddin, M. S. (2020). Analysis of digital image watermarking techniques through hybrid methods. Advances in Multimedia, 2020.
[11] Parashar, P., & Singh, R. K. (2014). A survey: digital image watermarking techniques. International Journal of signal processing, image processing and pattern recognition, 7(6), 111-124.
[12] Gupta, G., & Khunteta, A. (2017, September). Hiding text data in image through image watermarking using DCT & DWT: A research paper. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 447-450). IEEE.
[13] Barnouti, N. H., Sabri, Z. S., & Hameed, K. L. (2018). Digital watermarking based on DWT (discrete wavelet transform) and DCT (discrete cosine transform). International Journal of Engineering & Technology, 7(4), 4825-4829.
[14] Dowling, J., Planitz, B. M., Maeder, A. J., Du, J., Pham, B., Boyd, C., ... & Crozier, S. (2007, December). A comparison of DCT and DWT block based watermarking on medical image quality. In International Workshop on Digital Watermarking (pp. 454-466). Springer, Berlin, Heidelberg.