Robust Watermarking of Digital Color Pictures using the DT-CWT and DFT

B.Jagadish
21951A0463
B.Tech. student, Dept. of ECE Institute of Aeronautical Engineering Hyderabad, India
21951a0463@iare.ac.in

S.Arrshith Reddy
21951A0425
B.Tech. student, Dept. of ECE
Institute of Aeronautical Engineering Hyderabad, India
21951a0425@iare.ac.in

M.Karthik
21951A0470
B.Tech. student, Dept. of ECE
Institute of Aeronautical Engineering Hyderabad, India
21951a0470@iare.ac

Mr.V.Prasannajaneya Reddy
Assistant professor, Dept. of ECE
Institute of Aeronautical Engineering Hyderabad, India
Prasanna.vajrala@gmail.com

ABSTRACT - Image watermarking is the process of invisibly hiding secret data in the cover image to preserve the original image's copyright. In this paper, we offer a new framework for robust digital watermarking for colour photos that combines the Discrete Fourier Transform (DFT) and Dual Tree Complex Wavelet Transform (DTCWT). The cover image is initially separated into three channels: Y, U, and V. The Y channel is then converted using DFT and partitioned into ring forms. Using an embedding key, we create pseudo-random patterns to represent the watermark. These patterns are additionally modified and partitioned. The pattern selection watermark is then integrated into the DFT coefficient rings. We also incorporate a rectification watermark into the U channel,DTCWT is used to achieve geometric distortion robustness. Watermark identification and extraction can be completed effectively on the recipient's end. Compared to earlier techniques, the proposed method is more effective at preserving image quality. Meanwhile, the robustness against typical attacks is stronger

Keywords:*Digital watermarking, image processing, robustness, DTCWT, image correction.*

I. INTRODUCTION

Because of the rapid rise of social networks and communications in everyday life, capturing and sharing photographs on a regular basis has become a common activity, with a wonderful division of current portable phones and laptops, as well as digital cameras, handling high resolution imaging. However, transferring the aforementioned photographs from one device to another substantially exposed to the hazards of security, manipulation, and copyright attacks, unless it has been carefully taken care of by embedding the data into the media contents through watermarking. In order to safeguard multimedia files from a range of undesirable actions and unlawful interferences, including distribution and manipulation, watermarking is an essential tool[1]. As such, in order to ensure dependable performance, watermark generators must produce smooth, robust, and secure watermarks that can manage massive amounts of data. In the sections that follow, the aforementioned characteristics of watermarking methods will be covered in further detail. The resilience of the multimedia data produced by a watermarking method against potential attacks using image processing techniques is one of its most crucial features.In addition, the watermark must be undetectable, which means it must alter the information included in the original picture. Additionally, data capacity—which refers to the maximum quantity of data that may move through the algorithm while maintaining the cover image's visual appearance—is a key factor in evaluating the effectiveness of a watermarking process. Finally, security is a critical component of a watermarking technique since it indicates how resistant the system is to being discovered, embedded, or removed by outside parties.

The three main kinds of watermarking systems that have been studied and described in the literature thus far are non-blind, semi-blind, and blind[2]. The underlying idea of the previous perception is that, in semi-blind watermarking, only the watermark image is required, and in the blind variant, neither of them is required. In non-blind watermarking, both the original image and the watermark are required for embedding and extraction.

Alternately, watermarking methods can be categorized by the domain in which they function, such as the spatial domain or frequency, the latter of which modifies the parameter values in accordance with the cover image's frequency-domain representation.Conversely, watermarking in the spatial domain updates the pixel values, requiring a comparatively lower computational complexity and cost. However, this approach has the drawback that a comparatively smaller amount of information can be embedded into the cover image, potentially making it less resilient to signal processing operations.

The protection of communication networks has become more important in recent years due to the rapid advancement of technology and the growing usage of the internet for data transport. where it is now nearly hard to control and secure private or sensitive information and photos. As a result, several information security approaches, like digital watermarking and encryption, are fundamental to the modern world[3].

One of the most effective methods for identifying stolen information and securing copyright protection for digital content—such as texts, photos, audio files, and videos—against unauthorized modifications is digital watermarking. The practice of immediately embedding or concealing digital data so that it may be extracted again onto digital content (multimedia) is known as digital watermarking. Additionally, it has other qualities, including cryptography, an invisible watermark that doesn't detract from the visual appeal of digital content, and resilience to various attacks, including those that include compression, rotation, and scaling when watermarking digital images[4].

Therefore, characteristics like robustness, transparency, and capacity are used to evaluate the technique's quality. When the watermark remains unaffected by a variety of attacks, such as compression, scaling, rotation, and noise, then the watermarking approach is considered resilience.The size of the watermark that is added to the original data is referred to as its capacity. Greater capacity enables it to conceal vast amounts of data.

In this thesis, we propose a novel method for hiding the watermark image into the original image for grayscale and color images in different space (RGB, YIQ, and YCbCr) using digital image watermarking. This method is based on three techniques: DCT, DWT, and SVD. In this case, an encryption technique known as Arnold transformation has been employed to guarantee the watermark image, ensuring that only authorized users can access the watermark.

A method for adding data to digital multimedia without compromising the original multimedia's quality is called digital watermarking. As a result, this method is now helpful for content authentication, copyright protection, and steganography.Since digital watermarking technology makes it possible to add an imperceptible or invisible watermark to multimedia files in accordance with requirements to detect harmful data tampering or to identify the rightful owner, it plays a significant role in preventing copyright violations[5].

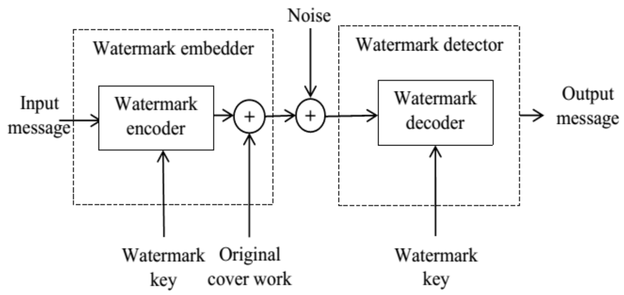

Fig.1 Standard model for watermarking

A watermark encoder uses a watermark key to encode an input message in the watermark embedder, as seen in Figure 1.1. The original cover artwork will incorporate the watermark or encoded message. The noisy watermarked cover is received by a watermark decoder in the watermark detector, which uses the same key to decode it and extract the output message**.**

II. LITERATURE SURVEY

Digital watermarking has emerged as a key method for protecting multimedia files, especially photos. Spatial domain techniques, in which watermarks are incorporated directly into the pixel values, were among the first watermarking methods. Nevertheless, these techniques are extremely susceptible to even the simplest attacks, including compression and noise addition. Researchers turned to frequency domain approaches to improve robustness. The Discrete Fourier Transform (DFT), which allows embedding in the image's frequency coefficients, is one of the popular frequency-based techniques. Watermarks embedded in the DFT domain provide protection against geometric attacks such rotation and scaling, as shown by Cox et al. (1997). However, the imperceptibility and resilience to sophisticated attacks of this methodology alone are limited, which is what spurred the creation of hybrid approaches.

Because it can represent an image at multiple resolutions, multi-resolution analysis—in particular, the Discrete Wavelet Transform (DWT)—has been extensively investigated for picture watermarking. Researchers discovered that adding watermarks to DWT's lower frequency subbands improves robustness, particularly against noise and image compression assaults. Expanding on this idea, Selesnick et al. presented the Dual-Tree Complex Wavelet Transform (DT-CWT), which provides phase information and directional selectivity for a more sophisticated multi-resolution analysis that is more useful for watermarking applications[6]. Since DT-CWT-based watermarking preserves edge information and fine details, it is more resistant to geometric distortions and compression than typical DWT approaches, as shown by several investigations (Wang et al., 2009).

Using many frequency domains together, like DT-CWT and DFT, improves watermark robustness even more. Hybrid watermarking strategies that combine the benefits of several transformations to increase resilience and imperceptibility have been studied recently. A technique combining DFT and DT-CWT was given by Patel and Chawla (2016), demonstrating a notable improvement in resistance to attacks like as noise, rotation, and cropping. Their method produced greater robustness without sacrificing image quality by adjusting the DFT coefficients and putting the watermark in particular subbands of the DT-CWT. Combining several transforms is a strategy that shows promise for the development of watermarking schemes since it strikes a balance between strong attack resilience and imperceptibility.

N. Provos and P. Honeyman asserted that although all three methods conceal information, steganography is completely distinct from watermarking and cryptography. Steganography conceals the information, whereas cryptography conceals information that has been encoded. Watermarking is similar to steganography in that it conceals information within another image; however, it needs to be fairly resilient against attempts to erase it. Multimedia content's copyright can also be safeguarded by extending the information masking technique. Techniques like steganography and watermarking can be used to hide secrets and preserve information's copyright. Solachidis Vassilios In this research, a unique watermarking approach for high dynamic range (HDR) photographs is proposed. The used embedding technique is predicated on a bracketing process that breaks down the original HDR representation into several low dynamic range (LDR) images. The available contributions are combined into a single HDR object to produce the final output once the chosen watermark has been added into each LDR component. Our method is able to produce a watermarked HDR image that is visually identical to the original one while detecting embedded information in both the marked HDR image and its LDR counterpart, obtained through tone-mapping operators or by other techniques. This is achieved by taking advantage of some of the well-studied properties of digital watermarking for standard LDR images[7].

Finally, it may be worthwhile to consider switching to non-blind watermarking, which is likely to be another useful application situation for HDR image watermarking. This would allow us to select which blocks to embed, avoiding those that are difficult to watermark; for this purpose, a thorough analysis of feature variability could be quite useful in deciding which zone of the image the watermarking method is most effective in.

III. EXISTING SYSTEM

In existing systems, the Discrete Wavelet Transform (DWT) is extensively used for digital watermarking. DWT separates the image into several frequency components, allowing the watermark to be embedded in low, middle, or high frequency regions. However, DWT frequently suffers from disadvantages such as inadequate resilience against attacks like as compression, noise addition, or filtering. an IR sensor and GSM module, presents several notable challenges that compromise its effectiveness and reliability.

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

IV. PROPOSED SYSTEM

Assume the colored cover picture **I** is of the size mr × mc, and the to-be-embedded watermark is designated by W. We divide **I** into three channels: Y, U, and V. The independent channels are created by transforming the image's R, G, and B channels. The embedding technique is divided into two stages: embedding a watermark in the Y channel and embedding some rectification information in the U. The V channel of the cover image remains untouched. The next sections cover watermark embedding and extraction. Figure 1 depicts an overview of the embedding method.

The same information is available in the android application through a smart mobile phone. The complete process is presented in the block diagram depicted in figure:1 below.

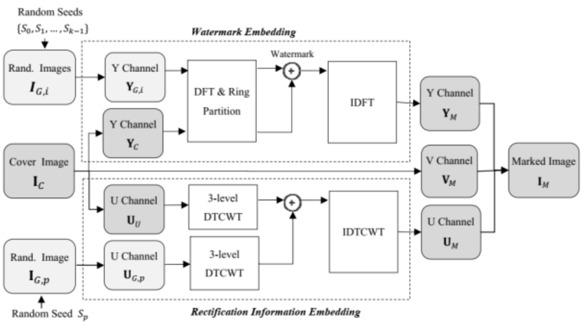

Figure 1: Block diagram of proposed system

A. DTCWT

The "DTCWT" acronym stands for Dual-Tree Complex Wavelet Transform. It is an expansion of the discrete wavelet transform (DWT) that improves directional selectivity and shift-invariance. Here are some important points concerning DTCWT are
1. Directional Selectivity: DTCWT can successfully differentiate between different directions in the signal, making it helpful for image processing tasks such as edge identification, texture analysis, image denoising.
2. Shift Invariance: Unlike the DWT, the DTCWT is almost shift-invariant. This means that minor changes to the input signal have little effect on the output, making it more suitable for certain applications.
3. Complex Coefficients: The DTCWT uses complex coefficients, which allow it to capture both amplitude and phase information of the signal. This can be particularly useful for analyzing signals with oscillatory components.

4. Redundancy: In one dimension, the DTCWT is usually two times more redundant than the DWT, and in two dimensions, it is four times more redundant. Although this redundancy increases computational complexity, it can enhance the performance of signal processing systems.

5. Applications: DTCWT finds use in signal denoising, texture classification, image processing, and feature extraction, among other areas.

B. DFT:

A mathematical method for converting discrete signals from the time domain to the frequency domain is the Discrete Fourier Transform (DFT). A sequence of numbers can be broken down into components of different frequencies using the DFT, which gives information on the frequency spectrum of the signal. In signal processing, picture analysis, and data compression, where knowing a signal's frequency content can be crucial, this transformation is especially helpful. To represent the amplitude and phase of the signal's frequency components, the DFT is defined for a sequence of (N) complex numbers and transforms them into another sequence of (N) complex numbers. Although the DFT and the continuous Fourier transform are closely related, the DFT was created especially for discrete data, which makes it ideal for digital applications[8].
The Fast Fourier Transform (FFT), which dramatically lowers the computational complexity from (O(N^2)) to (O(N log N)), is one of the most effective techniques for computing the DFT. The FFT is a key component of contemporary digital signal processing because of its efficiency. The DFT is widely used in many different fields, such as telecommunications, where it helps with signal modulation and demodulation, and audio signal processing, where it assists with sound frequency analysis. By adjusting the frequency components of images, the DFT is also utilized in image processing to filter and compress pictures. The DFT offers a strong way to examine periodicity and spectrum properties while being discrete; it serves as a link between the time-domain and frequency-domain representations of signals.

V. RESULTS AND DISCUSSION

In order to embed the watermark into the cover image and obtain the necessary psnr and msme values, we used the cover image as the source image in this project.

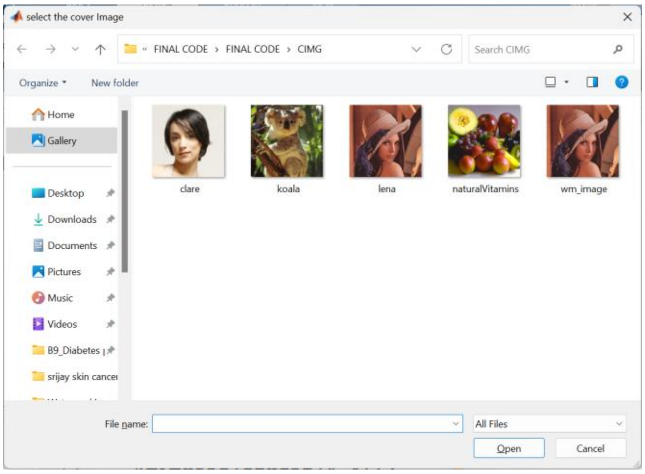

Fig.1 Selecting the cover image

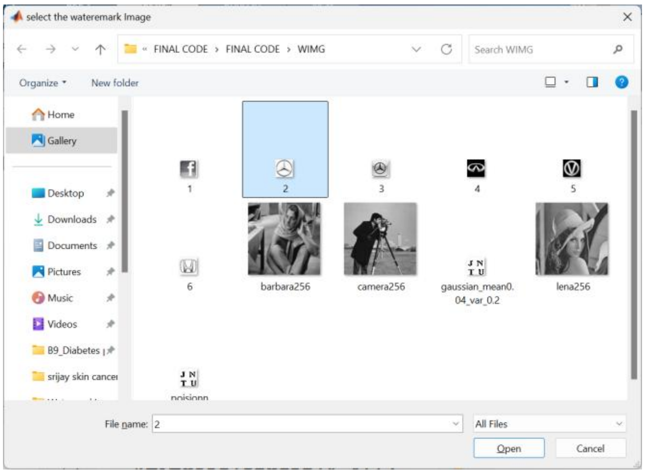

Fig.2 Select watermark image

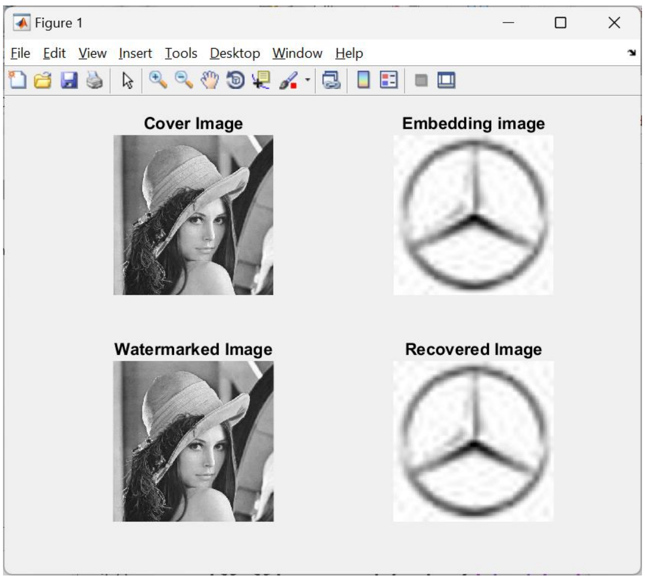

Fig.3 Results of watermarked image and Recovered image

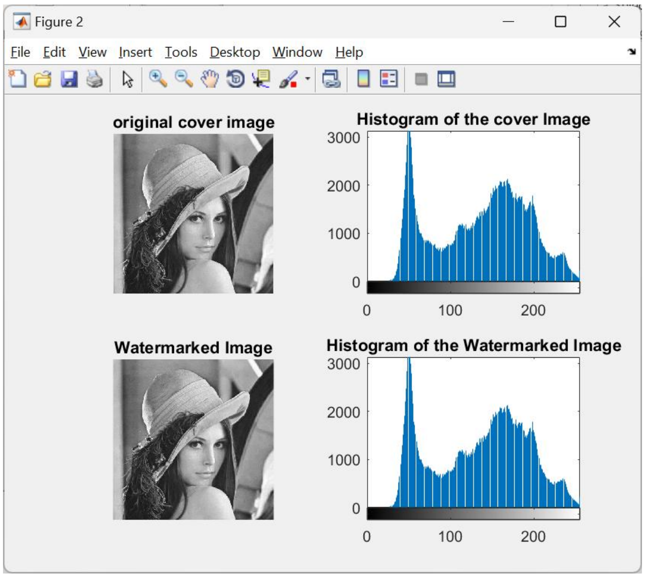

Fig.4 Histograms of cover image and watermarked image

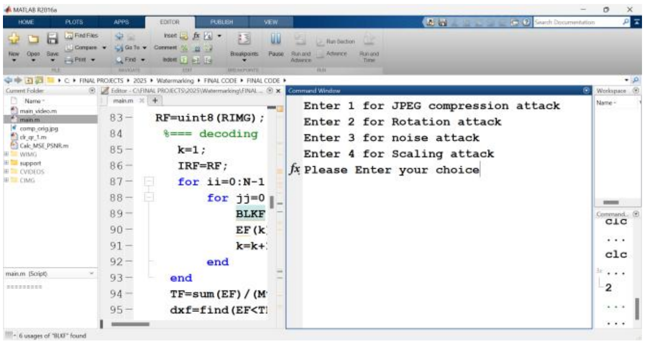

Fig.5 Selection of attacks from the user

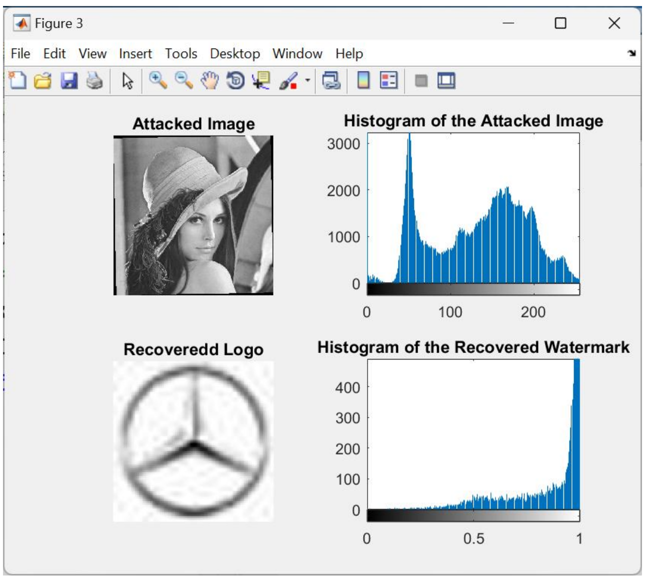

Fig.6 Results after attack

Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

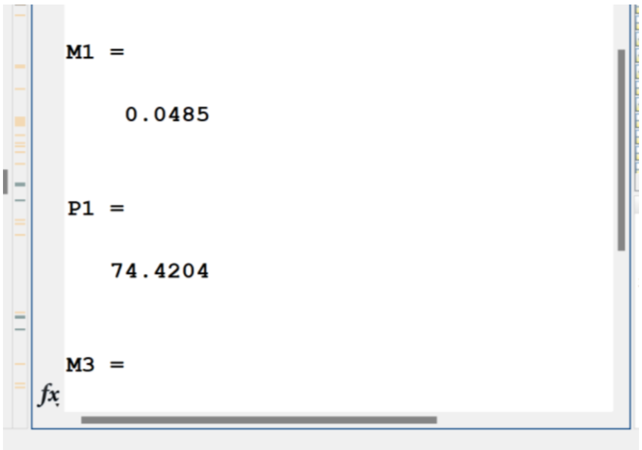

Fig.7 PSNR and MSME values

VI. CONCLUSION

To sum up, this study provides a strong digital watermarking method for color photos by using the Combined Discrete Fourier Transform (DFT) and Dual-Tree Complex Wavelet Transform (DT-CWT) domains. The suggested method successfully inserts and removes watermarks without compromising the cover image's aesthetic appeal, making it appropriate for uses where a high degree of imperceptibility and resilience is needed. By combining the advantages of both domains, DT-CWT and DFT improve resistance against different types of attacks, including noise, rotation, scaling, compression, and noise..

VII. FUTURE SCOPE

Enhancing resistance against increasingly complex attacks, like cropping, geometric distortions, and even AI-based manipulation, can be the main goal of future research. Enhancing watermarking methods to withstand or adjust to these kinds of attacks would further strengthen the system.The existing watermarking system might be made more efficient for real-time processing, which would make it appropriate for multimedia applications, live video streaming, and real-time image sharing where watermark extraction and embedding need to happen fast without compromising robustness or quality.

VIII. REFERENCES

[1] In 2001, Barni, M., Bartolini, F., and Piva, A. "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking." 783–791, IEEE Transactions on Image Processing, 10 (5)

[2] N. G. Kingsbury. (1998). "The Dual-Tree Complex Wavelet Transform: A New Technique for Shift Invariance and Directional Filters." IEEE Workshop on Digital Signal Processing, 319-322.

[3] Cox, I.J., Miller, M.L., and Bloom, J.A. (2002). Digital Watermarking. Morgan Kaufmann..

[4] Wang, Y., Doherty, J. F., & Van Dyck, R. E. (2002) IEEE Transactions on Image Processing, 11(2), 77-88. "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images."

[5] In 2000, Pitas, I., and Nikolaidis, A. published "Region-based Image Watermarking." 10(11), 1726–1740 IEEE Transactions on Image Processing

[6] Mohanty, S. P., Ramakrishnan, K. R., and Ramasubramanian, S. (2005). "A Robust DWT-SVD Domain Watermarking Scheme for Color Images." 18th International Conference on VLSI Design Proceedings, 351-356.

[7] Huang, D.-C., Wang, F.-H., and Shieh, J.-S. (2007). "Wavelet-based Watermarking in Color Images Using the Mixed Moments of Characteristic Functions." Electronic Imaging Journal, 16(3), 033002

[8] Vetterli, M. and Do, M. N. (2005). "The Contourlet Transform: An Efficient Directional Multiresolution Image Representation." 14(12), 2091-2106, IEEE Transactions on Image Processing.