International Journal of Current Trends in Engineering and Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 11, Issue: 03 (May -June 2025)

Improved Robust, Invisible Digital Image Watermarking Using Discrete Cosine Transform and PM

Arpit Namdev, Neera Lal
Assistant Professor, Department of IT
University Institute of Technology, RGPV, Bhopal, India
namdev.arpit@gmail.com, neera_smriti@ymail.com

Abstract **-** With technological advancements, the internet has become the primary medium for transferring information across the globe. This medium enables quick, easy, and accurate data transmission. However, transmitting information over the internet also presents significant security threats. In this context, digital watermarking has emerged as a promising technique for ensuring data authentication and integrity. In the proposed approach, the source image is processed in row-major order, and the Discrete Cosine Transform (DCT) is applied to generate low and high-frequency components. One bit of the authenticating image is embedded into each transformed DCT coefficient, excluding the first coefficient, to maintain low perceptual distortion and enhance PSNR. Early work on digital watermarking, including analyses of various schemes and their applications, is discussed to provide background. Unlike many existing methods that emphasize content authentication over strict integrity, this paper introduces a binary value-shifting technique based on the statistical characteristics of image pixels. This method embeds watermark data into the cover image to improve PSNR and enhance image protection. The implementation is carried out on the Windows platform using MATLAB. The proposed technique aims to secure digital images while achieving improved PSNR values. Digital watermarks are also used to verify the reliability and integrity of the signal or image data. The effectiveness of the approach is evaluated using normalized correlation to assess robustness against various attacks.

Keywords: Digital Watermarking, Image Authentication, DCT, PSNR, Image Security, Robustness.

I. INTRODUCTION

Watermarking is a technique used to embed copyright information into digital multimedia data such as images. Various watermarking methods have been developed to hide watermark data in images [1]. With the success of the Internet, the availability of cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service for both wired and wireless networks, it has become easier than ever to create, replicate, transmit, and distribute digital content. Consequently, protecting and enforcing intellectual property rights in digital media has become a significant concern [2]. Digital watermarking is a technology that ensures security, data authentication, and copyright protection for digital media. It involves embedding a signal or secret information (i.e., a watermark) into digital media such as images, audio, or video. Later, the embedded information is detected and extracted to verify the ownership or identity of the media. The advancement of laptop and internet technology has significantly simplified the creation and distribution of images, text, audio, video, and other digital media. However, traditional watermarking techniques may not meet all application requirements. Watermarking has thus emerged as an effective solution for enhancing the security of multimedia documents.

Steganography offers an important alternative for ensuring image integrity and authenticity. It is a form of data hiding that provides another layer of security for digital image data. Unlike traditional encryption, which hides the content of a message, steganography hides the existence of the message itself by embedding it into meaningful cover images without perceptible visual changes. Steganographic messages can be embedded in pictures, videos, or audio files using techniques such as invisible ink or least significant bit (LSB) substitution. Steganography techniques can be classified into two main categories: spatial domain and frequency domain. In spatial domain steganography, hidden information is embedded directly into image pixels. In frequency domain steganography, image pixels are first transformed using techniques such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT), after which the information is embedded.

To enhance security, Genetic Algorithms (GA) have also been integrated with steganography, especially for sensitive applications such as military communications, medical diagnostics, and research institutions. Data hiding refers to the nearly invisible embedding of information within host data (e.g., message, image, or video). A typical example of steganography is a prisoner communicating with the outside world under the watchful eye of a warden. The goal of steganography is to hide a message or image within a source image while preserving the visual properties of the original. Cryptography, on the other hand, hides the content of the message. Common data-hiding techniques use the least significant bit (LSB), masking, filtering, and transformation operations on the source image. The proposed work in this paper facilitates secure message transmission using a block-based data-hiding technique in the transform domain, ensuring minimal visual distortion [2].

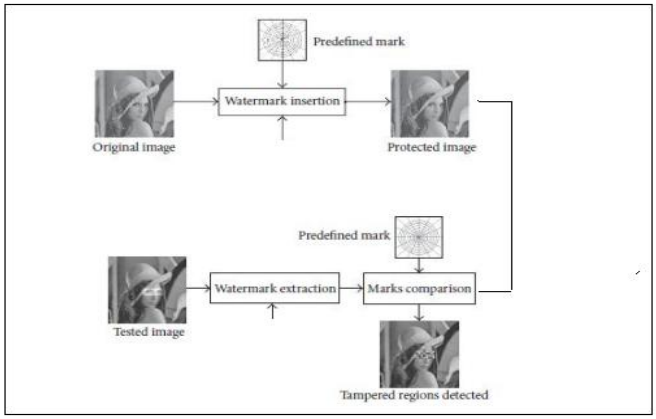

Fig1 watermarking image data hiding

The use of the internet is expanding rapidly. It is an essential medium for communication and data exchange. However, advancements in technology have made it easy to manipulate digital information, increasing the need for authentication to protect against unauthorized access. Watermarking and steganography are two prominent techniques used for this purpose. Watermarking is a widely accepted approach for protecting digital media—including images, video, text, and audio from unauthorized use. In this paper, the focus is on image watermarking. This process requires two images: the host image and the watermark image. The watermark image, containing sensitive or identifying information, is embedded into the host image to prevent misuse. Currently, the standard Discrete Cosine Transform (DCT)-based algorithm used in JPEG compression is widely adopted for colour image compression. However, extremely low bit rates can cause blocking artefacts in reconstructed images, which affect visual quality. Most transform schemes apply a 2D DCT on non-overlapping square blocks of size N×N, implemented using two separate N-point transforms: one along the vertical axis and another along the horizontal axis [2, 13]. This requires N2log2N steps. Vector Quantization (VQ) is a powerful technique for low-bit-rate source coding. It maps k-dimensional vector blocks into representative vectors in a finite Euclidean space, transmitting or storing only the related index. High compression ratios can be achieved with VQ, making it a compelling approach for image coding. However, several improvements have been proposed in the literature [3].

1.1 Requirements of Digital Image Watermarking

Digital image watermarking must satisfy several essential requirements to be effective and reliable. One of the most critical criteria is robustness, which refers to the watermark's ability to endure various signal processing operations such as spatial filtering, scanning, printing, lossy compression, scaling, rotation, and conversions between digital and analogue formats. Since not all watermarking techniques exhibit the same level of robustness, some may withstand incidental modifications while failing under more aggressive or malicious attacks. Based on this, watermarks can be classified into three categories: robust watermarks, which are designed to survive both incidental and intentional attacks and are particularly suitable for applications such as broadcast monitoring, copyright protection, fingerprinting, and copy control; fragile watermarks, which are deliberately sensitive to any form of modification and are primarily used for detecting unauthorized alterations and verifying data integrity; and semi-fragile watermarks, which can tolerate minor, unintentional changes but are disrupted by malicious tampering, making them ideal for image authentication purposes. Another important requirement is imperceptibility, also known as invisibility or fidelity. This refers to the perceptual similarity between the original image and the watermarked image. A good watermarking system should ensure that the watermark remains invisible to human observers, preserving the visual quality of the original content. However, there is often a trade-off between imperceptibility, robustness, and embedding capacity enhancing one may lead to compromises in the others.

1.2 Applications of Watermarking

Digital watermarking serves a wide range of applications. One major application is integrity verification and copyright protection, where watermark information embedded during content creation acts as proof of ownership in cases of dispute. Another use is corruption detection, particularly with fragile watermarking schemes that indicate tampering when the watermark is degraded or destroyed, thus identifying compromised content. Content authentication is also a critical application, wherein fragile or semi-fragile watermarks help detect any modification in digital content, ensuring that even slight alterations can be traced. Additionally, content description is supported through watermarks that carry metadata, such as labels or captions, which require high embedding capacity but not necessarily robustness. Lastly, communication authentication involves the covert embedding of messages within images to facilitate secure communication. In such scenarios, the hidden data must remain undetectable to unintended recipients [8].

II. RELATED WORK

In the study by Abrar et al. [9], the authors highlight that in the present digital era, safeguarding information has become critically important as organizations face increasing challenges in data security due to technological advancements. Managing the exponential growth of data securely and efficiently presents a significant challenge for researchers. As digital content is frequently generated and shared online, verifying its authenticity has become a pressing concern. To address this, a robust authentication watermarking method was proposed for document protection by identifying relevant attributes within the image. The image was divided into blocks, using different block sizes for the inner and outer regions. The watermark

was embedded using the Discrete Wavelet Transform (DWT) for the inner blocks and the Discrete Cosine Transform (DCT) for the outer blocks. Experimental results demonstrated high image quality post-watermarking, with a PSNR value of 35 dB even after JPEG compression. Normalized Cross-Correlation (NCC) values reached 1.0 under no attacks and ranged from 0.9014 to 0.9999 under various attack scenarios, confirming the method's robustness and suitability for critical applications such as copyright protection, secure content distribution, and digital forensics. Siva Jana Kiraman et al. [10] proposed a grey block embedding method in which the least significant bits (LSBs) are modified based on the most significant bit (MSB) plane. The grayscale image is divided into 4×4 blocks, which are further subdivided into 2×2 blocks.

The embedding is performed in two phases: outer and inner embedding. In the outer embedding phase, a reference point is selected in each 2×2 block, and the MSB of that point determines how the secret data is embedded into the remaining pixels. In the inner phase, the reference point values are altered to enhance security. During extraction, the reference point is restored, enabling the recovery of the hidden data. This scheme enhances embedding capacity and complexity, thereby improving security. Cox et al. [11] proposed embedding a watermark in the low-frequency coefficients of an image using the DCT. They selected the "N" highest-magnitude coefficients, excluding the DC component, for watermark insertion. This method improved robustness while preserving image quality. X. Zhang et al. [12] introduced reversible digital watermarking, which allows both the original media and the watermark to be recovered. Their approach uses additive interpolation-error expansion, where residual values—called interpolation errors are generated through an interpolation process and expanded by addition to embed bits. This method offers low distortion and high embedding capacity, making it particularly suitable for high-fidelity applications like military surveillance, medical imaging, and multimedia archiving. Langelaar et al. [13] proposed a watermarking scheme that uses thresholding of DCT coefficients. The image is divided into equal-sized regions, each containing an equal number of blocks. A bit is embedded by creating an energy difference between these regions using high-frequency DCT coefficient nullification. Chi-Man Pun et al. [14] utilized DCT space for watermark embedding, using a 32×32 watermark footprint. Detection requires access to the original image for accurate watermark extraction under various modifications.T. Nirupama et al. [15] developed an algorithm that embedded a watermark encrypted with the DES algorithm.

The watermark is inserted after applying a two-level DWT to the host image, enhancing security through layered transformation and encryption. In 2009, Mei Jiansheng et al. [16] presented a DWT-based watermarking algorithm that leverages human visual system (HVS) characteristics. The watermark image is first transformed using DCT and then embedded into the high-frequency band of the wavelet-transformed host image. S.S. Bedi et al. [17] also used the HVS principle, employing edge detection techniques to embed robust and imperceptible watermarks in the transformation domain. Navnidhi Chaturvedi et al. [18] compared watermarking performance using DWT and a combined DWT-DCT approach, evaluating both methods based on PSNR.Lai et al. [19] proposed a hybrid watermarking technique using DWT and singular value decomposition (SVD). Instead of embedding directly into wavelet coefficients, the watermark is embedded into the singular values of the DWT subbands. This method provides high robustness and imperceptibility under various image-processing attacks.

Jiantao Zhou et al. [20] proposed a reversible data hiding scheme for encrypted images using public key modulation, eliminating the need for a shared secret key. A two-class SVM classifier at the receiver end distinguishes encrypted from non-encrypted patches, allowing joint decoding of the embedded message and the original image using simple XOR operations. Ashwin S. et al. [21] presented a reversible data hiding method that reserves space before encryption using a traditional RDH algorithm. This ensures that the original image can be perfectly reconstructed after extracting the hidden data, thereby enhancing both data transmission and security. M.S. Hwanga et al. [22] introduced a histogram shifting technique for reversible data hiding in high-bit-depth medical images. By leveraging the high correlation among local pixels in anatomical structures, the method builds different histograms across blocks and applies two distinct embedding strategies. The original image can be accurately restored using inverse histogram shifting.T. Wang et al. [23] proposed a reversible watermarking method targeting medical images. Their approach uses recursive dither modulation (RDM) and SVD, with differential evolution (DE), to optimize quantization steps. Experimental results demonstrate high imperceptibility and robustness, outperforming existing methods.L. Dong et al. [24] proposed a novel reversible image data hiding (RIDH) method, leveraging a two-class SVM classifier to separate encrypted and non-encrypted patches. The scheme provides high embedding capacity while enabling lossless recovery of both the message and the original image. Using differential expansion, the approach improves prediction error expansion (PEE) performance, achieving state-of-the-art capacity-distortion trade-offs. Zhaoxia Yin et al. [25] addressed reversible data hiding in encrypted images (RDHEI), which has practical applications in privacy protection and content authentication. They proposed a separable RDHEI framework utilizing Josephus traversal and stream ciphers for encryption. Reversible data embedding is performed via block histogram shifting using self-hidden peak pixels. Depending on key possessions, users can extract either the embedded data, a near-original decrypted image, or the original image with complete accuracy. The proposed

method achieves higher embedding payloads and improved image quality after decryption.

III. SOFTWARE USED

The performance analysis of MATLAB version 13 (R2020), i.e., used for this thesis. The implementation of data mining provides processor-optimized libraries for fast execution and computation, and it is performed on cancer datasets. It uses its JIT (just in time) compilation technology to provide execution speeds that rival traditional programming languages. It can also further take advantage of multi-core and multiprocessor computers. MATLAB provides many multi-threaded linear algebra and numerical functions. These functions automatically execute on multiple computational threads in a single MATLAB to execute faster on multicourse computers. In this thesis, all enhanced efficient data retrieval results were performed in MATLAB 13 (R2020b) to get image processing. MATLAB is a high-level language and interactive environment used by millions of engineers and scientists worldwide. It lets them explore and visualize ideas and collaborate across different disciplines with signal and image processing, communication, and computation of results. MATLAB provides tools to acquire, analyze, and visualize data, enabling you to get insight into your data in a division of the time it would take using spreadsheets or traditional programming languages. It can also document and share the results through plots and reports or as published MATLAB code.

IV EXPERIMENTATION RESULTS ANALYSIS

The experimental analysis conducted in the domain of digital watermarking demonstrates that the proposed methodology yields reliable and secure digital images. The method offers improved robustness, better ownership authentication, and enhanced protection for hidden information. Overall, the proposed approach presents an effective solution for secure digital image watermarking.

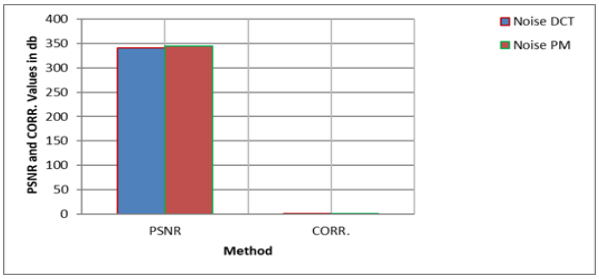

Fig2: Robustness Analysis of previous work and proposed work in noise attack

Figure 2 illustrates the PSNR (Peak Signal-to-Noise Ratio) analysis under a noise attack scenario. It is evident from the graph that the PSNR values obtained using the previous method based on the Discrete Cosine Transform (DCT) are comparatively lower than those achieved using the proposed method (PM). This indicates that the proposed method is more robust against noise interference.

Figure 3 presents the PSNR analysis under the JPEG compression attack. The results clearly show that the PSNR values for the DCT-based method are again lower, while the proposed method maintains higher PSNR values, demonstrating greater resilience against compression artefacts.

Similarly, Figure 4 depicts the PSNR performance under a smoothing attack. As with the previous cases, the proposed method significantly outperforms the traditional DCT-based approach, achieving higher PSNR values and confirming its robustness and effectiveness in preserving image quality even under smoothing operations.

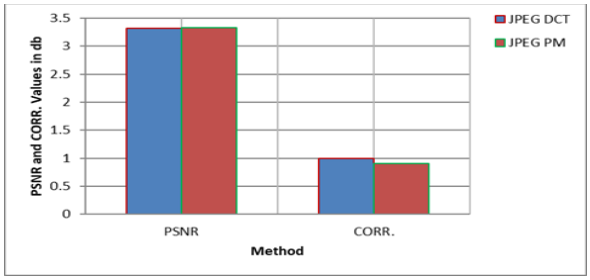

Fig3: Robustness Analysis of previous work and proposed work in JPEG attack

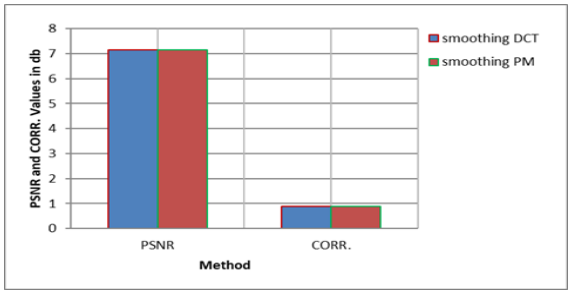

Fig4: Robustness Analysis of previous work and proposed work in smoothing attack

V. CONCLUSION

This research focused on digital image watermarking and presented a comprehensive framework for embedding and detection processes. It began by outlining the fundamental model of a digital image watermarking system and highlighted the essential requirements such systems must fulfil. Additionally, various applications of digital image watermarking were discussed, emphasizing its relevance in areas such as copyright protection, content authentication, and secure communication. The study explored prominent techniques used in both the spatial and frequency domains, followed by an overview of common attacks that

watermarking schemes must withstand. With the growing volume of digitally exchangeable data, the need for advanced information security measures has intensified, particularly for multimedia content like images. To address this, feature-based watermarking methods, in combination with domain-specific embedding strategies, were evaluated for their effectiveness in resisting noise distortions and signal processing attacks. A comparative analysis of different watermarking techniques under various attack scenarios was conducted. The proposed approach, based on an improved robustness-oriented particle shifting scheme and Discrete Cosine Transform (DCT), demonstrated significant advantages over existing methods. It provided higher PSNR values and improved resilience against attacks such as noise, JPEG compression, and smoothing.

Furthermore, the paper presented a performance analysis of embedding time and recovery time. The results showed that while traditional methods had higher embedding and recovery times, the proposed method significantly reduced both metrics. Moreover, the proposed technique achieved superior PSNR values, indicating better preservation of image quality after watermark embedding and extraction. In conclusion, the proposed digital image watermarking method offers enhanced image data authentication, improved robustness, and higher PSNR compared to conventional DCT-based techniques. It proves to be a promising solution for secure and reliable watermarking, especially in scenarios requiring high fidelity and resistance to multiple types of attacks.

REFERENCES

[1]. Soni, Aayush, Kamalpreet Kaur, and Chirag Sharma. "A Review of Artificial Intelligence in Digital Watermarking Techniques." In 2025 International Conference on Automation and Computation (AUTOCOM), pp. 1601-1606. IEEE, 2025.

[2]. Devi, K. Jyothsna, Priyanka Singh, Muhammad Bilal, and Anand Nayyar. "Enabling secure image transmission in unmanned aerial vehicle using digital image watermarking with H-Grey optimization." *Expert Systems with Applications* 236: 121190, 2024.

[3]. Begum, Mahbuba, and Mohammad Shorif Uddin. "Digital image watermarking techniques: a review." Information 11, no. 2: 110, 2020

[4]. Awrangjeb, Mohammad. "An overview of reversible data hiding." In Proceedings of the Sixth International Conference on Computer and Information Technology, pp. 75-79. 2003.

[5]. Varsaki, Eleni, Vassilis Fotopoulos, and A. N. Skodras. "A reversible data hiding technique embedded in the image histogram." Hellenic Open University Journal of Informatics 1, no. 2, 2006.

[6]. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits Systems and Video Technology, Vol. 16, No.3, pp. 354–362, 2006.

[7]. Dixit, Anuja, and Rahul Dixit. "A review on digital image watermarking techniques." International Journal of Image, Graphics and Signal Processing 9, no. 4: 56, 2017.

[8]. Kamaruddin, Nurul Shamimi, Amirrudin Kamsin, Lip Yee Por, and Hameedur Rahman. "A review of text watermarking: theory, methods, and applications." IEEE Access 6: 8011-8028, 2018.

[9]. Abrar, Iram, and Javaid A. Sheikh. "Robust Watermarking Scheme for Digital Image Authentication and Security." 2024 IEEE 21st India Council International Conference (INDICON). IEEE, 2024.

[10]. Siva Janakiraman, Suriya. N, Nithiya. V, Badrinath Radhakrishnan, Janani Ramanathan and Rengarajan Amirtharajan, " Reflective Code for Gray Block Embedding," Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, IEEE, pp: 215-220, 2012.

[11]. J. Cox and Matt L. Miller, "A review of watermarking and the importance of perceptual modelling". In Proc. of Electronic Imaging '97, Fevrier 1997.

[12]. X. Zhang, "Separable reversible data hiding in the encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[13]. G.C. Langelaar, J.C.A. Van der Lubbe, and R.L Lagendijk, "Robust labelling Methods for copy protection of images", In SPIE conference, San Jose, California USA, Janvier 2000

[14]. Chi-Man Pun and Ioi-Tun Lam, "Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright Ownership Authentication", International Journal of Communications Issue 1, Volume 3, 2009.

[15]. Tiwari, Nirupma, Manoj Kumar Ramaiya, and Monika Sharma. "Digital Watermarking using DWT and DES." In *2013 3rd IEEE International Advance Computing Conference (IACC)*, pp. 1100-1102. IEEE, 2013.

[16]. M. Jiansheng, L. Sukang and T. Xiaomei, —*A Digital Watermarking Algorithm Based on DCT and DWT*‖, IOSN 978-952-5726-00-8, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P.R. China, (2009) May 22-24, pp. 104-107

[17]. S. S. Bedi, G. S. Tomar and S. Verma, *Robust Watermarking of the image in the transform domain using edge detection*, UKSim 2009; 11th international conference on computer modelling and simulation.

[18]. N. Chaturvedi and Dr. S. J. Basha, *Comparison of Digital Image Watermarking methods DWT &*

DWT-DCT on the basis of PSNR, International Journal of Innovative Research in Science, Engineering and Technology, vol. 1, Issue 2, (2012) December.

[19]. Lai, Chih-Chin, and Cheng-Chih Tsai. "Digital images watermarking using discrete wavelet transform and singular value decomposition." *IEEE Transactions on Instrumentation and Measurement* 59, no. 11 (2010): 3060-3063.

[20]. Jiantao Zhou, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, "Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation", IEEE transactions on circuits and systems for video technology,2015.

[21]. Ashwin S, Ganesh K, Gokul R and Ranjeeth Kumar C, "Secure Data Transmission Using Reversible Data Hiding", International Journal of Computer Science and Information Technologies, Vol. 5 Issue 2 pp. 861-1863, 2014

[22]. M.S Hwanga, L.Y. Tsengb, LC Huang, "A reversible data hiding method by histogram shifting in high-quality medical images", Journal of Systems and Software, Vol. 86, (3), pp. 716–727, 2013.

[23]. B. Lei, E.L. Tan, S. Chen, D. Ni, T. Wang, H. Lei, "Reversible watermarking scheme for medical image based on differential evolution", Expert Systems with Applications, Vol. 41, (7), pp. 3178–3188, 2014.

[24]. J. Zhou, W. Sun, L. Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441-452, Mar. 2016.

[25]. Zhaoxia Yin, Andrew Abel, Xinpeng Zhang, Bin Luo, "Reversible Data Hiding in Encrypted Image Based on Block Histogram Shifting", IEEE,2016.