Anjali Kumari, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Robust Digital Image Watermarking in Frequency Region by LSB Embedding

Anjali Kumari[1], Sujeet Gautam[2]
[1]Research Scholar, Department of Cse, Pcst 0128 Bhopal Mp India
[2]Assistant Professor, Department of Cse, Pcst 0128 Bhopal Mp India

Abstract- Medical image watermarking has emerged as an important technique for protecting the confidentiality, integrity, authenticity, and ownership of digital medical images. This paper proposed a model that takes input a image a secret message in form of watermark for the validation of the sending image. In order to protect image form attacks proposed work embedded secret watermark into the carrier image by invisible watermarking approach. Discrete cosine transform was used in the model for finding the safe region in image where embedded information stay for long time. Further model embedded the information by using Least significant bit position in the image. It was found that use of DCT coefficient region based watermarking image get robust against various noise and filter attacks. Experiment was done on real image dataset and result shows that proposed model has maintain the PSNR value, while reduces the MSE value.

Keywords: Digital Image Processing, Watermarking, Healthcare Data, Embedding, Extraction.

I. INTRODUCTION

The rapid development of digital healthcare systems, Picture Archiving and Communication Systems (PACS), telemedicine, cloud-based medical services, and electronic health records has substantially increased the generation, transmission, and storage of medical images in digital form. Medical imaging modalities such as magnetic resonance imaging (MRI), computed tomography (CT), ultrasound, X-ray, positron emission tomography (PET), and digital pathology are routinely exchanged between hospitals, diagnostic centers, physicians, and remote healthcare platforms. Although digital communication improves accessibility and clinical efficiency, it also increases the possibility of unauthorized access, manipulation, duplication, interception, and incorrect association of medical images with patient information. Consequently, protecting the confidentiality, integrity, authenticity, and ownership of medical images has become an important requirement in modern healthcare information systems.

Security requirements for medical images are particularly stringent because an alteration that may appear visually insignificant can potentially influence clinical interpretation and consequently affect diagnosis or treatment. Furthermore, medical images frequently contain personally identifiable and sensitive health information. Conventional cryptographic techniques can protect an image during transmission or storage; however, after decryption, the image itself generally no longer carries an inherent mechanism for authentication or integrity verification. Digital watermarking has therefore emerged as a complementary security mechanism in which authentication data, patient information, ownership information, cryptographic hashes, or other auxiliary information is embedded directly within the medical image [1], [2].

The requirement for imperceptibility is especially important in medical applications. Unlike ordinary multimedia watermarking, modifying diagnostically important anatomical structures may be unacceptable because embedded information should not interfere with clinical interpretation. For this reason, medical images are commonly divided into a Region of Interest (ROI) and a Region of Non-Interest (RONI). The ROI contains diagnostically significant information, while the RONI generally contains areas of comparatively lower clinical importance. Early and subsequent medical watermarking approaches therefore attempted either to embed information exclusively within the RONI or to apply reversible embedding methods when modification of the ROI was necessary [3], [4].

Researchers have also extensively investigated transform-domain watermarking to improve robustness and perceptual quality. Instead of modifying image pixels directly, transform-domain methods embed watermark information into coefficients generated by mathematical transformations such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) [5]. Such techniques provide greater control over the spatial-frequency characteristics of watermark embedding and can offer improved resistance to image-processing operations compared with simple spatial-domain approaches [6].

In traditional watermarking, which was usually founded on spatial and transform domain, such as DCT, DWT, and SVD, has been shown to provide reasonable trade-offs between imperceptibility and robustness with multiple image manipulations [7].

However, these classical methods often lack adaptability to modern adversarial attacks and are not easily scalable to large-scale or real-time applications. Consequently, deep learning techniques, particularly CNNs, have gained traction in the watermarking domain due to their powerful feature learning capabilities and superior resilience to diverse image transformations. CNNs can effectively learn spatial correlations and encode watermarks in complex, high-dimensional feature spaces, making the watermark more robust and imperceptible under compression, noise, and geometric attacks [8]. Spatial-domain methods operate directly on pixel intensities through filtering, contrast adjustment, or morphological operations.

II. RELATED WORK

Nawaz et al. in [9], proposed a deep learning–based zero-watermarking method that integrates MobileNetV2 with DWT–DCT feature extraction and chaos-based encryption, achieving robustness without altering the host image. Deep learning-based watermarking methods have demonstrated promising performance in terms of robustness and automatic feature extraction. However, they suffer from several limitations, including the reliance on large labeled datasets, high computational costs, and complex network architectures.

Wang, R. et. al. in [10], proposed an efficient, robust, secure digital watermarking scheme for medical images. The proposed method integrates Dual-Tree Complex Wavelet Transform (DTCWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) to extract image features. Particle Swarm Optimization (PSO) is then employed to adaptively adjust the watermark embedding parameters, enhancing imperceptibility and robustness. Moreover, Henon chaotic mapping is introduced to generate pseudo-random sequences for watermark encryption, further enhancing security.

Aulia Arham et. al. ikn [11], proposed a reversible watermarking technique that supports high-capacity data embedding while preserving diagnostic quality and enabling authentication and recovery. The image is divided into three regions: the ROI, where patient records are reversibly embedded using a multi-layer difference expansion scheme; the RONI, where semi-fragile 2D-DE embedding enables tamper localization and recovery; and the border region, which stores auxiliary information using simple, non-robust LSB encoding that does not affect diagnostic content.

R, A. et. al. in [12], done work in three phases. In the first phase, the medical image is visibly watermarked with the image using region-of-interest (ROI), invisibly using discrete wavelet transforms (DWT), and with a text using a logistic mapping approach. It involves embedding text and image watermarks in medical images using a deep-learning model. The second phase involves applying noise attacks to images and evaluating their performance by estimating peak signal-to-noise ratio (PSNR) values. In the third phase, the model is used to extract the watermarks. Optimization of the model is done using the Adam optimizer (AOA) and stochastic gradient descent (SGD) algorithms.

Khare et al. in [13] introduces an innovative approach for medical image watermarking (MIW) that integrates key features of Hough Transform (HT),

Redundant Discrete Wavelet Transform (RDWT), and Singular Value Decomposition (SVD) transformations. The watermark embedding within the reflectance component ensures improved robustness and perceptual invisibility. To fortify resistance against attacks, a combination of RDWT and SVD is utilized. The technique incorporates a dual-layer security mechanism for the watermark image by employing chaotic mapping to safeguard critical diagnostic medical data against manipulation or unethical activities. Furthermore, the performance of the proposed technique is evaluated across several wavelet families. The experimental results notably demonstrate the superior robustness and perceptibility achieved by the proposed scheme, as various performance metrics exhibit enhanced values.

L. Prasanna Meda et. al. in [14], study suggests a multi-layered approach to improve colour medical imaging interference discovery and retrieval for telemedicine security. Strong watermarking techniques will be employed to insert secure identities in medical photos for tamper detection. ormalizing pixel intensity levels reduces variability and boosts the efficiency of algorithms. The Gaussian-Adaptive Bilateral Filter (GABF) improves image quality by maintaining edges while lowering noise, which helps with precise tamper finding and salvage in colour medical imaging. The Adaptive Dynamic Inertia Weight and Acceleration Coefficient Optimization (ADIWACO) algorithm enhances telemedicine security by optimizing tamper detection, improving image recovery, refining feature extraction, and increasing accuracy in identifying unauthorized modifications in colour medical imaging. ML algorithms will analyse image integrity and spot anomalies indicative of manipulation. A blockchain framework will maintain an immutable, transparent record of all picture alterations.

III. PROPOSED WORK

This work centers around the digital picture invisible information concealing algorithm. Here entire work is isolate into embedding and extraction steps. For imperceptible embedding was done in such a manner that visibility of the information hiding by naked eyes isn't conceivable. If there should be an occurrence of extraction information ought to be effectively recover from the received information with no data loss of the embedded information and in addition information [7, 8]. In Fig. 4.2 whole embedding block diagram is explained. While Fig. 4.3 whole extraction block diagram is explained.

Pre-Processing

Read a picture implies making a matrix of a similar measurement of the picture at that point fill the framework compare to the pixel dimensions at the cell in the lattice.

In this progression picture is resize in settle measurement. As various picture have distinctive measurement. So change of each is done in this progression. This can be comprehend as picture have a measurement of the 30x30 and other picture has the measurement of 29x28 then it have to resize it either in 30x30, with the goal that it framework activity can be effortlessly perform on both grid.

Embedding of Watermark

The watermark is represented as a binary matrix in which each pixel belongs to one of two classes: a black pixel is represented by 0, whereas a white pixel is represented by 1. Before the embedding process, the low-frequency (LL) coefficient matrix of the cover image is rearranged into an $N \times 8$ matrix, such that the total number of elements corresponds to the LL sub-band. Each watermark pixel is then embedded by modifying the arrangement of coefficients in one row of this matrix.

When a black watermark pixel (0) is selected for embedding, one row containing eight coefficients is read from the $N \times 8$ matrix. The coefficients are transformed so that the four values on the left-hand side are increased or arranged to represent the binary class 0. Conversely, when a white watermark pixel (1) is encountered, the next row is selected and the four coefficients on the right-hand side are increased or rearranged. In this manner, the relative distribution of coefficients within each eight-element row represents the corresponding watermark bit.

The embedding operation is repeated sequentially for all pixels of the watermark. Thus, each watermark bit is associated with a corresponding row of eight LL coefficients. For a watermark containing 1024 pixels, the required rows of the LL-band coefficient matrix are processed accordingly. This controlled modification of the low-frequency coefficients allows the watermark information to be embedded into the cover image while limiting unnecessary changes to its visual content.

DCT (Discrete Cosine Transform)

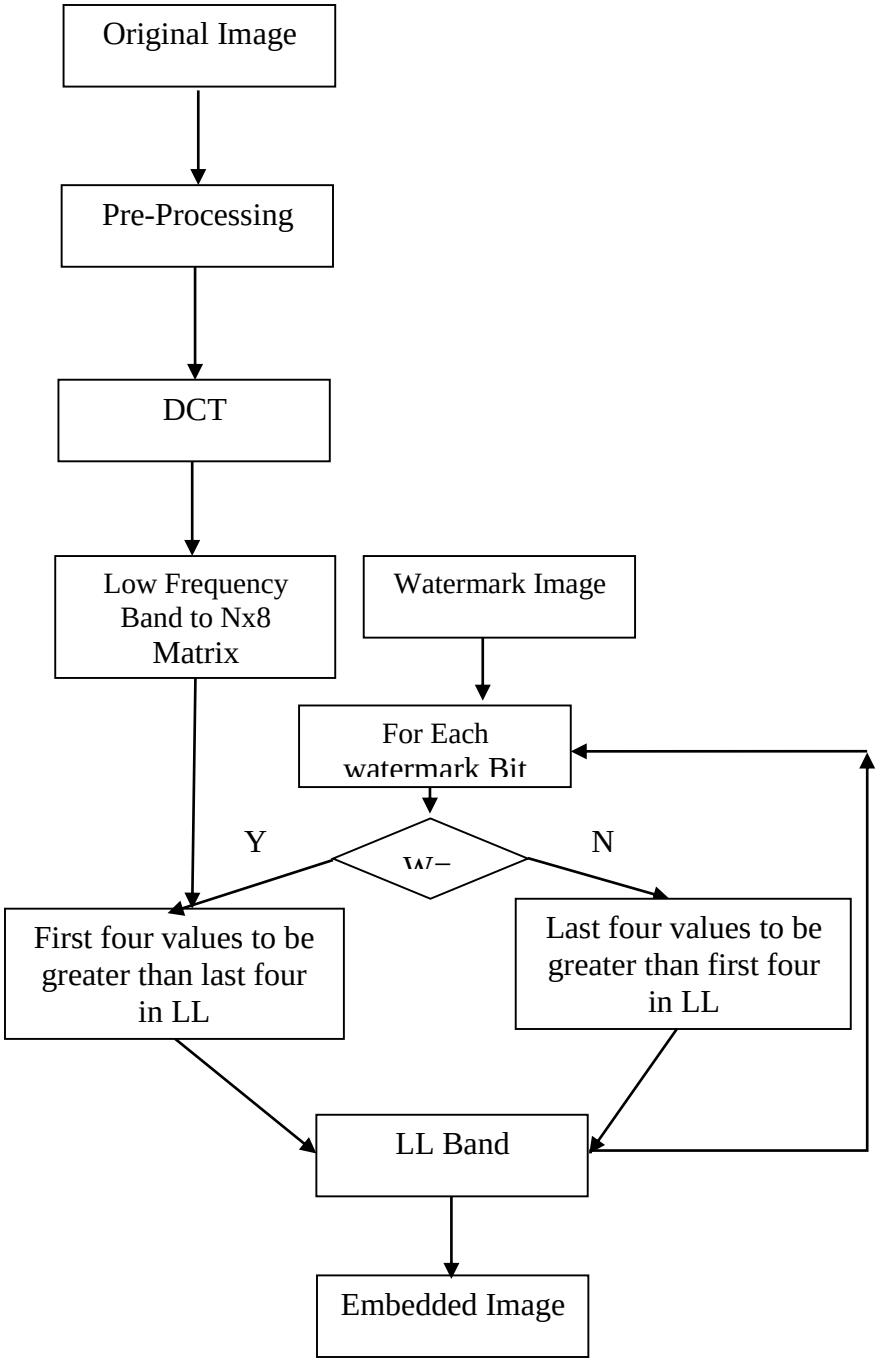

Fig. 1 Block Diagram of Proposed work.

In frequency domain, the image is decomposed into many frequency components with most of the image information being concentrated in a part of those components. This property of energy compaction along with the removal of redundancy are the main reasons why it is often preferred to process images in the frequency domain. The DCT is one of the most popular frequency transformations in image and video processing due to its simplicity and high energy compaction. For an image block x of size $N \times N$, the type II 2-D DCT is defined as

$$X(k_1, k_2) = \frac{2}{N} u(k_1) u(k_2) \sum_{n_1=1}^{N} \sum_{n_2=1}^{N} x(n_1, n_2) cos\left(\frac{\pi(2n_1 + 1k_1}{2N}\right) cos\left(\frac{(2n_2 + 1)k_2}{2N}\right)$$

Where $k_1, k_2 = 1, 2, 3, \ldots\ldots\ldots\ldots N$, $u(k)=1$ for $k \neq 1$ and $u(1)= \frac{1}{\sqrt{2}}$

Extraction of Image

In this extraction steps receiver can extract data and image by using above block diagram. This segment of proposed work is for picture extraction at recipient side. Here DCT feature again extract and convert into block of impage whuch are further process to find difference between the left hande side value with right hand side value. So if LHS values are greater than consider watermark bit as 1, while if RHS values are higer than 0 is consider. Hence this section of proposed work is for data extraction at receiver side. Along these lines all the blocks bits are join to make secret information or watermark by converting ASCII values into corresponding character.

IV. EXPERIMENT AND RESULTS

Dataset

Analysis done on the standard pictures, for example, mandrilla, lena, tree, and so forth. These are standard pictures which are gotten from http://sipi.usc.edu/database/?volume=misc. Framework is tried on everyday pictures also.

The results presented in Table 1 demonstrate that the proposed method achieves substantially better PSNR performance than the previous approach reported in [29] under ideal conditions. For all three test images, the proposed method produces considerably higher PSNR values, indicating improved quality of the processed images. The incorporation of DCT-based processing and shuffling operations in the proposed embedding procedure contributes to this improvement by reducing the distortion introduced during watermark embedding.

Table 1 PSNR Based Comparison between

PSNR Based Comparison		
Images	Proposed Work	Previous Work
Tiger	44.8874	3.39217
Pepper	44.2648	1.1929
Madrilla	36.6561	3.41885

Table 2. MSE based comparison between proposed and previous work.

Salt & Pepper Attack Based PSNR Comparison		
Images	Proposed Work	Previous Work
Tiger	28.0331	3.41766
Pepper	27.9089	1.22455
Madrilla	27.5202	3.46544

Table 2 compares the proposed and previous methods [29] in terms of MSE under ideal conditions. The proposed technique records significantly lower MSE values for Tiger, Pepper, and Madrilla images. Since a smaller MSE represents reduced reconstruction error and better image fidelity, these results indicate the effectiveness of the proposed approach. The use of DCT together with the shuffling mechanism minimizes the embedding distortion and consequently reduces the error compared with the previous method.

Table 3. PSNR Based Comparison between proposed and previous work.

Salt & Pepper Attack Based PSNR Comparison		
Images	Proposed Work	Previous Work
Tiger	28.0331	3.41766
Pepper	27.9089	1.22455
Madrilla	27.5202	3.46544

Table 3 presents the PSNR performance of both methods after applying a salt-and-pepper noise attack. The proposed technique maintains PSNR values above 27 dB for all evaluated images, whereas the previous approach [29] produces considerably

lower values. This improvement indicates that the proposed watermarking technique provides greater resistance to noise-induced degradation. The combination of DCT, shuffling, and key-based operations strengthens the embedding procedure and helps preserve image quality even in the presence of salt-and-pepper noise.

Table 4. MSE Based Comparison between proposed and previous work.

Salt & Pepper Attack Based MSE Comparison		
Images	Proposed Work	Previous Work
Tiger	102.276	29601.6
Pepper	105.243	49048.5
Madrilla	115.095	29277.6

The MSE results under salt-and-pepper noise are summarized in Table 4. Compared with the previous method [29], the proposed approach generates substantially smaller MSE values for all three test images. These lower error values indicate that the proposed embedding technique is capable of preserving a greater amount of image information following the noise attack. The DCT and shuffling operations contribute to minimizing the distortion caused by noise, thereby improving the robustness of the proposed method.

Table 5. PSNR Based Comparison between proposed and previous work.

Filter Attack Based PSNR Comparison		
Images	Proposed Work	Previous Work
Tiger	33.1216	3.41442
Pepper	30.1834	1.21962
Madrilla	20.8267	3.54188

As shown in Table 5, the proposed technique provides improved PSNR performance under filtering attacks compared with the previous method [29]. The Tiger and Pepper images achieve PSNR values of 33.1216 dB and 30.1834 dB, respectively, while the Madrilla image records 20.8267 dB. In each case, the proposed results remain substantially higher than those obtained by the earlier technique. The DCT-based embedding, shuffling procedure, and selected key operation collectively enhance the ability of the method to withstand filtering operations.

Table 6. MSE Based Comparison between proposed and previous work.

Filter Attack Based MSE Comparison		
Images	Proposed Work	Previous Work
Tiger	31.6902	29623.7
Pepper	62.3356	49104.2
Madrilla	537.534	28766.9

Table 6 evaluates the MSE performance under filtering attacks. The proposed approach obtains considerably lower error values than the previous technique [29] across all three test images. Although the Madrilla image shows a comparatively higher MSE of 537.534 within the proposed results, it remains substantially below the corresponding value of 28766.9 obtained by the previous method. These findings demonstrate that DCT-based embedding and shuffling improve the ability of the proposed approach to retain image information following filtering operations.

VI. CONCLUSION

The proposed work introduces a distinct image-based data protection technique designed to provide secure information transmission under different attack conditions. A carrier image is employed for data embedding, where the low-frequency coefficients obtained through the Discrete Cosine Transform (DCT) are utilized. The proposed technique effectively embeds secret information while preserving the visual quality and security of the carrier image. Under ideal conditions, the proposed algorithm successfully reconstructs the embedded data at the receiver side while maintaining the quality of the carrier image.

Experimental findings demonstrate that the method provides an effective balance between image quality and robustness. The utilization of DCT frequency-domain features improves the PSNR performance compared with the DCT-based techniques. Experimental results indicate that the developed embedding strategy achieves lower MSE values and improved data extraction performance under noise attacks compared with the previous approaches. Overall, the obtained PSNR, MSE, and extraction results demonstrate that the proposed technique

preserves image quality while providing improved robustness against noise and filtering attacks.

REFERENCES

1. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. Burlington, MA, USA: Morgan Kaufmann, 2008.
2. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.
3. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," in Proceedings of the IEEE International Conference on Information Technology Applications in Biomedicine, 2000, pp. 250–255.
4. V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005, pp. 709–716. doi: 10.1109/INDIN.2005.1560462.
5. A Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Secure and efficient health data management through multiple watermarking on medical images," Medical & Biological Engineering & Computing, vol. 44, pp. 619–631, 2006. doi: 10.1007/s11517-006-0081-x.
6. G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 2, pp. 158–165, 2009. doi: 10.1109/TITB.2008.2007199.
7. Hosny, K. M., Magdi, A., ElKomy, O. & Hamza, H. M. Digital image watermarking using deep learning: A survey. Comput. Sci. Rev. 53, 100662.
8. Singh, H. K. & Singh, A. K. Digital image watermarking using deep learning. Multimed Tools Appl. 83(1), 2979–2994.
9. Nawaz SA, Li J, Bhatti UA, Shoukat MU, Li D, Raza MA (2024) Hybrid watermarking algorithm for medical images based on digital transformation and mobilenetv2. Inf Sci 653:119810
10. Wang, R., Liu, L., Li, X. et al. A medical image watermarking method based on the combination of DTCWT and PSO optimization. J. King Saud Univ. Comput. Inf. Sci. 38, 77 (2026).
11. Aulia Arham, Teguh Bharata Adji, Syukron Abu Ishaq Alfarozi, Hanung Adi Nugroho, Reversible watermarking for medical images using ROI-based tamper localization and recovery, Franklin Open, Volume 15, 2026.
12. R, A., C, M. Enhancing the protection of medical images using watermarking technology processed with deep learning algorithms. Multimed Tools Appl 84, 3339–3368 (2025).
13. Awasthi, D.; Khare, P.; Srivastava, V.K. Multiple Image Watermarking in YCbCr Color Space Using Schur-SVD-DCT in Wavelet Domain and its authentication using SURF. In Proceedings of the 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), Delhi, India, 23–24 March 2023; pp. 192–197.
14. L. Prasanna Meda and E. Rayachoti, "Enhancing Telemedicine Security in Advanced Methods for Tamper Detection and Recovery in Color Medical Imaging," in IEEE Access, vol. 13, pp. 217542-217555, 2025.
15. http://sipi.usc.edu/database/?volume=misc