A Hybrid Watermarking Scheme Using DWT and Haar Transform for Image Authentication

Sachchidananda Jana, Pabitra Pal, Asim Kumar Mahadani, and Debasis Giri

Abstract The safe transfer and preservation of medical images is crucial in the age of digital healthcare. Watermarking medical images is an essential method of adding patient data, hospital logos, and other pertinent information to these images without compromising their confidentiality, integrity, or validity. To overcome the aforementioned difficulties, this abstract offers a unique and reliable medical image watermarking system that makes use of Particle Swarm Optimization (PSO), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) approaches. There are three main phases to the suggested plan. The medical image is first broken down into its frequency components using DWT, which makes watermark embedding more effective. Subsequently, the PSO method is utilized to maximize the choice of image segments for incorporation, guaranteeing that the watermark remains undetectable and robust against diverse attacks. In the last step, the watermark's strength is increased by using the SVD approach to embed it in the singular values of certain image blocks. Comprehensive tests are conducted to assess the efficacy of the suggested approach, taking into account performance measures like the Structural Similarity Index (SSIM) and Peak Signal-to-Noise Ratio (PSNR), as well as resistance against typical assaults such as noise addition, compression, and cropping. The testing findings show that the method effectively embeds the watermark while maintaining image quality and making sure it is robust to attack. The suggested method is appropriate for clinical and telemedicine applications as it also protects the con-

S. Jana
Department of Computer Science & Applications, Prabhat Kumar College, Contai, Purba Medinipur 721404, West Bengal, India

P. Pal (✉)
Department of Computer Applications, Maulana Abul Kalam Azad University of Technology, Nadia 741249, West Bengal, India
e-mail: pabipaltra@gmail.com

A. K. Mahadani
Department of Computer Science and Engineering, Bankura Unnayani Institute of Engineering, Bankura, West Bengal, India

D. Giri
Department of Information Technology, Maulana Abul Kalam Azad University of Technology, Nadia 741249, West Bengal, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

D. Giri et al. (eds.), *Proceedings of Third International Conference on Advanced Computing and Applications*, Lecture Notes in Networks and Systems 1045,
https://doi.org/10.1007/978-981-97-4799-3_22

fidentiality and integrity of patient data. By advancing the development of effective and safe medical image watermarking methods, this research helps to protect the privacy and veracity of critical healthcare data.

Keywords Medical image watermarking · Particle Swarm Optimization (PSO) · Discrete Wavelet Transform (DWT) · Singular Value Decomposition (SVD)

1 Introduction

Medical image learning, preservation, transmission, and sharing have all undergone significant shifts in the digital era. As digital medical imaging becomes more and more necessary, it is critical to guarantee the confidentiality, integrity, and validity of these images. Medical images frequently include private patient information, and altering or gaining unauthorized access to them might have a negative impact. To preserve an image's validity and integrity, watermarking involves integrating strong, undetectable data into it. When it comes to medical images, watermarking is essential for guaranteeing the validity of clinical and diagnostic information. In medical applications, it is crucial that the watermark be resilient to different image processing techniques, data reduction, and transmission. The integrity and validity of medical images must be preserved due to the growing need for sharing them throughout healthcare systems and organizations. Malicious intent or an incorrect diagnosis might result from unauthorized changes or manipulation. A tool for preserving compliance is watermarking. During storage and transmission, medical images may experience several changes, such as noise reduction, format conversion, and compression. To survive these activities, the watermark needs to be sufficiently robust. Clinical diagnostics and medical research can benefit from watermarked images, as long as the watermark does not degrade the quality of the image.

2 Literature Survey

Islam et al. [8] suggested a strong lifting wavelet transform technique for image watermarking. An SVM classifier is utilized during watermark extraction to achieve increased resilience in various attacking situations. The NC, BER, and PSNR values are 0.8955, 0.0547, and 44.0719 dB, in that order. Hsu et al. [6] created a creative plan for color-blind watermarking. The suggested method incorporates EPA, MPSAM, MM, and PSO using a method based on crisscross inter-block QDFT. 39.3 dB is the PSNR value, while 0.966 is the MSSIM value. Fatahbeygi et al. [5] provided an image watermarking method using visual cryptography (VC) and block categorization. NC and PSNR have respective values of 0.9997 and 35.02 dB. Cu et al. [3] watermarking scheme where watermarking regions on documents are located using a fully convolutional network (FCN). SSIM and PSNR have respective values of

0.97 and 24.46 dB. Zermi et al. [12] suggested using blind watermarking to secure medical images; here the watermark is embedded into the Electronic Patient Records (EPR). Integration of the EPR data and watermark by using the DWT-SVD technique in only DWT, the PSNR of variant_1 is 27.34 and variant_2 is 27.19; in DWT-SVD, the PSNR of variant_1 is 56.12 and variant_2 is 57.41. Anand et al. [2] proposed to develop a dual watermarking system to protect electronic patient records (EPR) for the smart healthcare system. Proposed techniques are DWT, SVD, CTE (Compression Then Encryption) technique: SPIHT, and SIE, which make the method highly robust and imperceptible. The average PSNR is 45.3362 dB, NC is 0.9893, SSIM is 0.9875, NPCR is 0.996, and UACI is 0.3927. Hussan et al. [7] suggested creating a watermarking system that combines social networking and Internet of Things (IoT) principles. By addressing IoT's scalability problems, it envisions improved information exchange. The average PSNR value is greater than 33 dB. Alomoush et al. [1] suggested a technique for watermarking grayscale images that is undetectable and embeds information into the transformation domain. This technique employed a linear modulation algorithm to insert a stego-text into the least significant bit (LSB) of the discrete cosine transformation (DCT) coefficient. The values of SSIM, NC, and PSNR are 0.9899, 1, and 43.30 dB, respectively. Eldaoushy et al. [4] presented a hybrid digital image watermarking system that is effective. There are two Singular Value Decomposition (SVD) phases in it. The value of PSNR is 45.8605 and NC is 0.9975. Kumar et al. [9] provide a unique and reliable watermarking technique that integrates the SPIHT algorithm, the DWT, and the DCT. The highest PSNR value of 42.52 dB and maximum NC value of 0.9999 obtained by the suggested approach demonstrate the great quality and resemblance of the host and watermarked images. Singh et al. [11] suggest a creative digital image watermarking method. An encoder is first used to extract latent characteristics from cover and secret images, which are then concatenated to create a tagged image. The NC values are 0.9996 (32 × 32) and 0.9982 (64 × 64), whereas the PSNR values are 44.48 dB (32 × 32) and 41.1 dB (64 × 64). Rani et al. [10] A secure watermarking technique with medical applications is the subject of the proposed study. The suggested method boosts PSNR values or improves the robustness and transparency of digital image data.

3 Prerequisite

Particle Swarm Optimization (PSO), DWT, and SVD are all employed to enlarge a vigorous medical image watermarking process.

4 Proposed Scheme

The proposed approach for watermarking medical images is discussed in this section. It aims to be undetectable to the naked eye. To meet the requirements for image security and resilience of a watermarked image, an image with a binary watermark is added to the colored green channel of a medical image.

4.1 Watermark Embedding Process

This strategy uses SVD and encryption techniques to change the S matrix inside the LL to incorporate a binary watermark into the host medical image. The PSO method optimizes parameter D which controls the embedding strength to make the watermark undetectable while preserving resilience. The spatial localization of the watermark inside the image is aided by the use of DWT. This scheme's main goal is to insert a binary watermark into a host medical image's green channel. The procedure for embedding a watermark is described in detail below: The input of the method consists of a binary watermark and a host medical image (HOST). Initially, the color components of the host image are divided into three groups: red (HOSTred), green (HOSTgreen), and blue (HOSTblue). Secondly, low-frequency sub-bands (LL, LH, HL, HH) are obtained by applying DWT on the host image's green channel (HOSTgreen). In third, zigzag-chosen 3×3 blocks make up the low-frequency sub-band LL. Several 3×3 sub-blocks are produced as a result. Fourth, the S matrix is obtained by applying singular value decomposition (SVD) to each of these 3×3 sub-blocks. A matrix may be divided into three matrices using the mathematical process of SVD: U, S, and V^T. Fifth, using XOR to embed the binary watermark with a secret key. The encrypted watermark is then run through an "Arnold Cat Map". Sixth, the encrypted watermark bits are multiplied by a parameter D to generate the S' matrix, which is then added to the original S matrix's center element. The population-based optimization approach known as PSO is used to maximize the value of D. In seventh, the changed 3×3 blocks, designated as B'i, are obtained by applying the inverse SVD to the modified S' matrix. In the eighth, the original sub-blocks are replaced with the changed blocks (B'i) organized into the LL sub-band. In the ninth, to reconstruct the modified green channel of the host image (HOST'green), Inverse DWT is applied to the modified LL sub-band together with the LH, HL, and HH sub-bands. Finally, the watermarked image (HOST") is created by combining all three color channels (HOSTred, HOST'green, and HOSTblue).

4.2 Watermark Extraction Process

To extract the binary watermark from the watermarked image, DWT, SVD, PSO optimization, and a number of modifications are used. The parameters D and λ are essential to the watermark extraction process and must be set properly to get the best results. The procedure for extracting a watermark is described in detail below: firstly, the three color components of the watermarked image (HOST”) are distinguished as red (HOST’red), green (HOST’green), and blue (HOST’blue). Secondly, The LL sub-band, along with the LH’, HL’, and HH’ sub-bands, are obtained by applying DWT on the green channel (HOST’green). In the third, a zigzag pattern is used to split the LL’ sub-band into 3×3 chunks. As a result of this process, several 3×3 sub-blocks (B’i) are created. Fourth, to generate the S matrices (U, S, VT), SVD is applied to every 3×3 sub-block. Fifth, to determine the ideal value of D, particle swarm optimization (PSO) is carried out. In the sixth step, the watermark is extracted using the S matrices and the optimal value of D. If the criterion ($S + D < \lambda$, where λ is a threshold) is satisfied, the watermark value (W’img) for each S matrix is set to 1; if not, it is set to 0. The watermark (W’img) is transformed using the Arnold Cat Map transformation in reverse in step seven. During the embedding procedure, the original watermark was altered, and this step aids in restoring it. Lastly, the original binary watermark is recovered by XORing the extracted watermark (W’img) with a key.

5 Experimental Results and Performance Analysis

This section examines the results and looks at the projected work. Tests of the method’s effectiveness have been conducted using a variety of color medical images and binary watermark images. On a Windows 10 computer with 4 GB of RAM and a Core i5 CPU, the suggested task was simulated using Python. As a result, we were able to evaluate the imperceptibility and robustness of the presented method. In addition, the binary watermark measures 64 × 64 pixels. The chosen host medical image measures 512 × 512 pixels. The set of medical images and the watermark are shown in Fig. 1.

Various objectives like imperceptibility and robustness are calculated using PSNR, NC, SSIM, and BER (Bit Error Rate). Table 1 displays the PSNR and SSIM values of the watermarked images in addition to the NC and SSIM values of the recovered watermark. The highest SSIM and PSNR values are 0.9998 and 58.42 dB, respectively. The image with the watermark successfully displays the strong imperceptibility. Additionally, the method for removing watermarks works well. The closeness of the SSIM and NC values to unity indicates the expert performance of the algorithm for extraction.

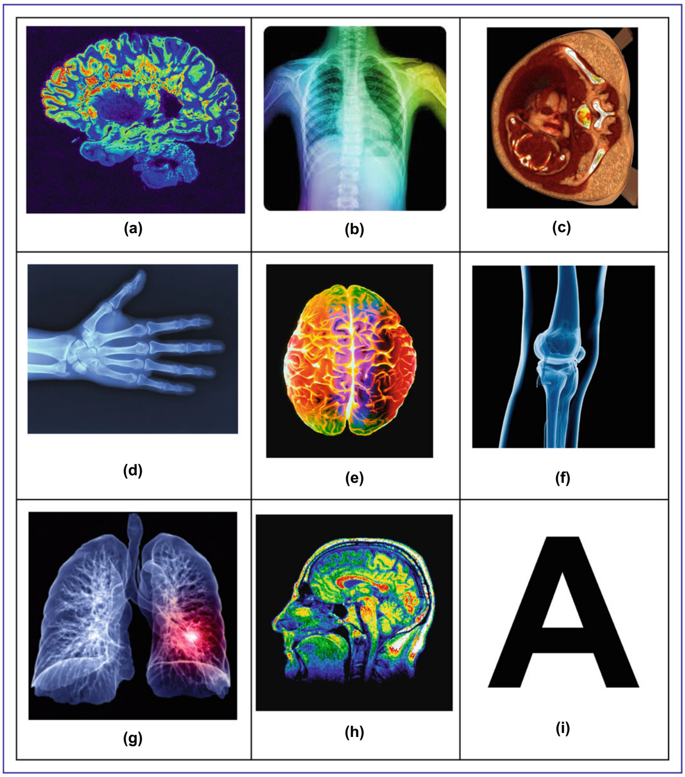

Fig. 1 Different test images

Table 1 PSNR of several colored medical image types, as well as the unattacked SSIM and NC of every retrieved watermark

Image	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
PSNR	58.42	58.10	58.38	58.24	58.18	58.40	58.31	58.27
NC	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
SSIM	0.9997	0.9891	0.9984	0.9987	0.9996	0.9995	0.9998	0.9899

5.1 Imperceptibility Test

The imperceptibility of the proposed method is evaluated with PSNR and SSIM. **PSNR:** For assessing the visual quality of watermarked images, the Peak Signal-to-Noise Ratio (PSNR) is computed by comparing the original images (represented as "M") with the watermarked images (represented as "N"). The PSNR calculation is as follows Eq. 1

Table 2 PSNR comparison between our method and other state-of-the-art methods

Image	Zermi et al. [12]	Anand et al. [2]	Hussan et al. [7]	Singh et al. [11]	Proposed (Average)
PSNR	57.41	45.336	44.17	44.48	58.29

$$PSNR = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{(255)^2}{MSE}dB \tag{1}$$

Here, “n” signifies the minimum number of bits required in the image to represent the maximum possible intensity. The Mean Square Error (MSE) is used to quantify the error and is determined by the Eq. 2.

$$MSE = \frac{1}{U_x V_y}\sum_{i=1}^{U_x}\sum_{j=1}^{V_y}(M_{i,j}-N_{i,j})^2 \tag{2}$$

where Ux and Vy are the dimensions of an image.

The PSNR comparison between our method and other state-of-the-art methods [2, 7, 11, 12] is tabulated in Table 2.

Structural Similarity Index Measure (SSIM): The SSIM is a perceptual model used to assess the similarity between two images, such as a watermarked image and its original counterpart. SSIM quantifies the image degradation caused by malicious attacks and evaluates the resemblance between the original and watermarked images by taking into account factors like pixel variance, covariance, and correlation, while also considering luminance and contrast masking. An effective SSIM score typically falls within the range of 0–1, and it can be calculated using Eq. 3.

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \tag{3}$$

In this context, x and y represent the original images and the watermarked image, μ_x, and μ_y correspond to the local means of x and y, and σ_x and σ_y stand for the variances of x and y. Additionally, C_1 and C_2 are two variables employed to ensure the stability of the division operation when the denominator is weak.

5.2 *Robustness Test*

Normalized Correlation (NC): The Normalized Correlation (NC) is employed as a metric to assess the robustness of a system. It quantifies the resemblance between the original and extracted watermarks even in the presence of distortions and this robustness is calculated using Eq. 4.

Table 3 NC comparison between our method and other state-of-the-art methods

Image	Zermi et al. [12]	Anand et al. [2]	Hussan et al. [7]	Singh et al. [11]	Proposed (average)
NC	0.998	0.989	0.995	0.999	1.000

$$NCC = \frac{\sum_{i=1}^{n_L} \sum_{j=1}^{n_K} \left(\left| W(i,j) + W'(i,j) \right| / 2 \right)}{n_L * n_K} \tag{4}$$

W and W' represent to binary original and extracted watermark images, while nL and nK denote the width and length of the host image, respectively.

The NC comparison between our method and other state-of-the-art methods [2, 7, 11, 12] is tabulated in Table 3.

Bit Error Rate (BER): The BER is utilized to quantify the ratio of the Number of error bits and the Total number of watermark bits implanted. The most commonly encountered non-geometrical attacks in signal processing involve the introduction of indistinguishable multiple noises and noise additives. In our suggested scheme, we conducted experiments to evaluate its performance when subjected to Salt & Pepper, Speckle, and Gaussian noise. Salt & Pepper noise arises from pixel errors during data transmission, manifesting as corrupted pixel values that are either reset to the highest value or with just one bit swapped.

NC values at different noise densities of restoring watermark images are shown in Table 4. As a multiplicative noise, speckle noise is classed, as characterized by its

Table 4 Results of tests conducted against various attacks on the image

Attacks	NC	BER	SSIM
Salt & pepper noise 0.020 0.090 0.001	0.9877 0.8975 1.0000	0	0.9892 0.9662 0.9983
Gaussian noise with mean = 0, variance - 0.020 0.001 0.002	0.9891 0.9982 0.9964	0	0.8999 0.9988 0.9957
Median filter [3 3] [4 4]	0.9891 0.9662	0.8332	0.9989 0.9998
JPEG compression (QF = 60 and QF = 90)	0.9868 0.9998	0	0.9986 0.9998
Histogram equalization	0.9998	0.7896	0.8993
Cropping	0.9891	2.24	0.8990
Speckle noise with density = 0.02, 0.03 and 0.005	0.9998 0.9989 1.0000	0	0.998 0.994 0.999

Table 5 Robustness comparison with the author [11, 12]

Attacks	Zermi et al. [12]	Singh et al. [11]	Proposed scheme
Salt & pepper noise attack	0.9782	0.9912	1.0000
Gaussian noise-attack	0.9707	0.9634	0.9982
Median filter	0.9603	0.9566	0.9891
JPEG compression (QF = 90)	0.9238	0.8952	1.0000
Histogram equalization	0.9873	0.9935	0.9998
Cropping	0.7913	0.8992	0.9891
Speckle noise attack	0.9197	0.9942	1.0000
Rotation	0.8611	0.8911	0.9990
Average filtering	0.9595	0.9921	0.9999

intrinsic granular nature. Each pixel's variance correlates to the regional region's variation centered around that pixel. NC values at various noise density levels of retrieved watermark imagery appear in Table 4. At various density levels like 0.02, 0.03, and 0.005, the corresponding NC values are 0.9998, 0.9989, and 1.0000, respectively, at a gain factor of 0.1. The SSIM values are 0.999, 0.998, and 0.994 based on density level. A common statistical noise processing technique is Gaussian noise, and its intensity is adjusted through variance while maintaining a mean of zero. To enhance robustness, we introduced this statistical noise to the watermarked images in our approach. We conducted experiments involving the addition of Gaussian noise with various variances as part of our proposed method. The NC values are 0.9891, 9982, and 0.9964 at noise densities of 0.02, 0.001, and 0.002 for the retrieved watermark images displayed in Table 4. According to density level, SSIM values are 0.8999, 0.8899, and 0.9957. Medical image conversions are never as good as the originals. As a result, JPEG compression has quickly established itself as a fundamental and essential tool in the world of image processing. Table 4 shows the retrieved watermark images that we looked at using different quality parameter scales (60 and 90). Also displays the NC and SSIM values that we discovered throughout our research. For both quality factors 60 and 90, the NC values are 0.9868 and 0.9998. On the other hand, for quality factors 60 and 90, the resulting SSIM values were 0.9986 and 0.9998. The acquired findings show that the proposed technique outperformed expectations in the face of a JPEG compression assault. The watermark image's histogram equalization attack is displayed in Table 4. Since the PSNR is bigger than that of other current techniques, the watermarked image quality is appropriate for diagnosis. In some scenarios, the suggested scheme's resilience is determined to be superior to similar, already-existing methods. Nonetheless, its performance is rather similar to specific attacks. The Arnold transform is used to increase the security of the embedded watermark.

Comparing our approach with other state-of-the-art methods [11, 12] when it comes to exposing different attacks is done in Table 5.

6 Conclusion

Modern healthcare systems depend on digital medical image watermarking to maintain diagnostic quality and guarantee the quality, validity, and protection of medical images. The suggested technique provides a strong and efficient way to handle these crucial needs. It integrates PSO, DWT, and SVD. The plan effectively adds watermarks to medical images without compromising their diagnostic value. Physicians may rely on images for correct diagnosis and study because of the watermark's imperceptibility. By utilizing DWT, SVD, and PSO, the approach improves the watermark's resilience. Even after data compression, image processing, and other attacks, the watermark may still be seen. One crucial component of the plan is the watermark's spatial localization. Through meticulous region selection for watermark embedding, the approach guarantees that the watermark stays out of critical diagnostic regions. To discover the best settings for watermark extraction and embedding, PSO is essential. The total effectiveness of the watermarking technique is improved by the algorithm's capacity to adjust these settings. Security precautions are included in the plan to prevent illegal removal or modification of the watermark. It contributes to the preservation of medical image integrity. Even if the suggested method is a big advancement in medical image watermarking, there are still a number of obstacles to overcome and research possibilities to be explored. Establishing uniform procedures and policies for watermarking medical images is crucial to guaranteeing uniformity and interoperability between healthcare systems. Examine techniques for adaptive watermarking that may be tailored to certain image properties or therapeutic requirements. Medical images may contain sensitive patient data, thus permission, data protection, and secure handling are important ethical issues. The efficacy of the plan has to be evaluated in actual healthcare environments. Working together with medical professionals and institutions might yield insightful comments.

References

1. Alomoush W, Khashan OA, Alrosan A, Attar HH, Almomani A, Alhosban F, Makhadmeh SN (2023) Digital image watermarking using discrete cosine transformation based linear modulation. J Cloud Comput 12(1):1–17
2. Anand A, Singh AK, Lv Z, Bhatnagar G (2020) Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE Multimedia 27(4):133–143
3. Cu VL, Nguyen T, Burie JC, Ogier JM (2020) A robust watermarking approach for security issue of binary documents using fully convolutional networks. Int J Doc Anal Recogn (IJDAR) 23:219–239
4. Eldaoushy AF, Desouky MI, El-Dolil SA, El-Fishawy AS, El-Samie FEA (2023) Efficient hybrid digital image watermarking. J Optics 1–15
5. Fatahbeygi A, Tab FA (2019) A highly robust and secure image watermarking based on classification and visual cryptography. J Inf Secur Appl 45:71–78
6. Hsu LY, Hu HT (2020) Blind watermarking for color images using emmq based on qdft. Expert Syst Appl 149:113225

7. Hussan M, Parah SA, Gull S, Qureshi G (2021) Tamper detection and self-recovery of medical imagery for smart health. Arab J Sci Eng 46:3465–3481
8. Islam M, Roy A, Laskar RH (2020) Svm-based robust image watermarking technique in lwt domain using different sub-bands. Neural Comput Appl 32:1379–1403
9. Kumar C (2023) Hybrid optimization for secure and robust digital image watermarking with dwt, dct and spiht. Multimedia Tools Appl 1–22
10. Rani A, Purohit A, Boghey R (2023) Improve secured digital image watermarking with discrete cosine transform and abct. In: 2023 8th international conference on communication and electronics systems (ICCES), pp 1761–1767. IEEE
11. Singh HK, Singh AK (2023) Digital image watermarking using deep learning. Multimedia Tools Appl 1–16
12. Zermi N, Khaldi A, Kafi R, Kahlessenane F, Euschi S (2021) A dwt-svd based robust digital watermarking for medical image security. Forensic Sci Int 320:110691