



A robust and secured fusion based hybrid medical image watermarking approach using RDWT-DWT-MSVD with Hyperchaotic system-Fibonacci Q Matrix encryption

M. Sajeer¹ · Ashutosh Mishra¹

Received: 21 July 2022 / Revised: 28 September 2022 / Accepted: 22 February 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Digital image watermarking, the process of marking a host image with a watermark, is generally used to authenticate the data. In the medical field, it is of utmost importance to verify the authenticity of the data using Medical Image Watermarking (MIW), especially in e-healthcare applications. Recently, MIW with image fusion, the merging of multimodal images to improve image quality, is being widely utilized to make diagnosis more accessible and precise with the verified data. This paper offers a durable and secure fusion-based hybrid MIW approach. The method initially used Fast Filtering (FF) to merge two medical images from different modalities to form the cover image. A first-level Redundant Discrete Wavelet Transform (RDWT) is employed on this host image to locate the component with the highest entropy. Then a single-level Discrete Wavelet Transform (DWT) is applied to it. It performed a Multi-resolution Singular Value Decomposition (MSVD) on the wavelet decomposed component and the embedding watermark. Finally, a Hyperchaotic System-Fibonacci Q Matrix (HFQM) encryption system was utilized, which increases the watermarked image's security. Here, using various medical images, the performance of the proposed technique is evaluated. Without any attacks, the approach achieved a maximum Peak Signal to Noise Ratio (PSNR) of 90.31 dB and a Structural Similarity Index Matrix (SSIM) of value 1. Various watermarking assaults were employed to test the proposed method's resilience. The suggested technique achieved a perfect value of 1 for the Normalised Correlation (NC) for almost all attacks with acceptable imperceptibility, which substantially improves over current procedures. The suggested technique's average embedding and extraction times are 0.3958 and 0.4721 seconds, respectively, which are pretty short compared to existing approaches.

Keywords Medical Image Watermarking (MIW) · Fast Filtering (FF) · RDWT · DWT · MSVD · Hyperchaotic system-Fibonacci Q Matrix (HFQM) encryption

✉ Ashutosh Mishra
ashutosh@nitc.ac.in

M. Sajeer
sajeer@sctce.ac.in

¹ Department of ECE, National Institute of Technology, Calicut, Kerala, India

1 Introduction

In this pandemic, telemedicine has been widely used worldwide, enabling a patient to consult global experts from the comfort of his home. The medical records are processed using cloud computing or transmitted over an open network. In this situation, the main issue is to preserve the security, privacy, and integrity of e-records. The data during transmission may be altered or hacked by unauthorized users leading to misdiagnosis, delay in treatment, or even the patient's death. Encryption can be used for the protection of medical data [11]. But the hacker can modify the data if it is decrypted. The scenario, as mentioned above, can be effectively handled using the MIW [28]. Here a watermark is inserted into the carrier data by a sender, and later it is retrieved by the receiver, which authenticates the data integrity. There is always a trade-off between three crucial characteristics of a MIW system- robustness, imperceptibility, and capacity. The ability to survive watermark attacks is referred to as robustness, while imperceptibility refers to whether the implanted watermark is visible or invisible to the rest of the world. The amount of information that can be inserted into the original data is the system's capacity [26]. Another essential characteristic of the MIW system is the reversibility (lossless), where the original data and the watermark will be restored on the receiving side [35].

MIW can be either spatial or transform in nature. In the spatial domain, the pixel value of the original data is changed to embed the secret information [24, 32]. The critical disadvantage of this design is that it is less resistant to attacks. In the case of a transform domain type, modification is done in the transformed coefficients of the host image [2, 10]. It has the potential to compensate for the drawbacks of spatial domain approaches. Most researchers nowadays focus on hybrid domain techniques, which combine transform domain with spatial domain techniques, which have both advantages. Recently, fusion-based MIW is gaining popularity, improving diagnostic accuracy [12].

1.1 Contributions

This paper presented a fusion-based medical image watermarking scheme using the RDWT-DWT-MSVD method. Here the host image is generated by the fusion of computed tomography (CT) and magnetic resonance imaging (MRI) scans, or T1-weighted and T2-weighted MRI scan, using the FF algorithm [36]. This fusion process improves the diagnostic accuracy of the host medical image. RDWT is employed in the fused cover image, decomposing it into low-frequency and high-frequency elements (LL, HL, LH, and HH). Then select the component with the highest entropy, less sensitive to Human Visual System (HVS). DWT is applied to this high entropy component to form the approximation and detailed components (CA, CH, CV, and CD). Then select the element with the highest entropy, and single level MSVD is employed to form the low and high-frequency components (XLL, XLH, XHL, and XHH). MSVD is also applied to the watermark to create various low and high-frequency components (WLL, WLH, WHL, and WHH). The embedding is done in the experimentally selected high-frequency HL subband since it is less sensitive to the human visual system, using an embedding rule. The hybrid domain enhances the invisibility and robustness of the scheme [30]. Finally, the watermarked image is encrypted using the HFQM algorithm, which uses a six-dimensional hyper-chaotic system with a Fibonacci Q matrix, further improving security [15]. The results indicate that the system has an excellent performance in imperceptibility, robustness, and security than the existing techniques with less computational time and can be used for e-healthcare applications. The contributions of the suggested scheme can be summarized as follows.

1. The suggested method utilizes fusion-based watermarking, which uses the FF algorithm to generate carrier images, increasing diagnostic accuracy.
2. RDWT, DWT, and MSVD are the general techniques used in watermarking. Since DWT has different advantages like multi-scalability, multi-resolution, and sparse frequency localization, it can improve the watermarking system's imperceptibility. It also has good robustness against noise and compression attacks. But it has shift sensitivity and poor directionality, which RDWT can eliminate. RDWT has the advantages like shift invariance and high embedding capacity. It is also robust to additive noise attacks. MSVD has the benefits like less computational complexity and provides robustness against geometrical attacks. Here we used the RDWT-DWT-MSVD hybrid method for watermarking, which offers excellent invisibility and robustness with less computational time.
3. The hybrid scheme retrieves the original image and watermark with less loss.
4. The watermarked image is encrypted using the HFQM algorithm. It uses 6D hyperchaotic system, which enhances the encryption performance and raises the security level due to its complex high-dynamic behaviors and two positive Lyapunov exponents. It also uses a Fibonacci Q matrix, which makes the encryption system faster.
5. The suggested method provides better imperceptibility and robustness with lower computational time than the current state-of-the-art technologies.

The following is how the rest of the paper is structured. Complementary works are in Section 2, and background preliminaries are discussed in Section 3. Section 4 delves into the proposed plan. Discussion on the experimental results in Section 5, along with a comparison study, and the article concluded in Section 6.

2 Complementary works

Many academics presented various MIW methods based on image fusion. Anand and Singh [4] used the Non-subsampled shearlet transform (NSST) to merge CT and MRI scans. Watermarking uses the Dual tree complex wavelet transform (DTCWT) - Singular value decomposition (SVD) technique. Finally, the data is encrypted using the chaotic map-random permutation-SVD technique. They tested the method's effectiveness using several watermark attacks. The authors created a MIW system in [7] that uses a non-subsampled contourlet transform (NSCT) to get the fused carrier image. The method used NSCT, QR decomposition, and Schur decomposition along with the Electronic Patient Record (EPR) Data for the watermarking. They used Deoxyribonucleic acid (DNA), chaotic maps, and a hash function in the encryption technique. The authors implemented various situations to assess the system's imperceptibility and resilience. The MIW strategy was presented by Hemdan [14] using Wavelet fusion, DWT, and SVD approaches. The technique used chaotic, and Arnold transforms to the watermarked image to improve the method's security. The author experimented with the scheme's performance by using various watermarking attacks. Tokhy [12] created a MIW algorithm in which the fused radiography image serves as the host image. The author employed the Ridgelet transform (RT) and the backtracking search optimization method for the watermarking approach to achieve the best balance of robustness and image imperceptibility. The technique used different watermarking attacks for the performance evaluation. Anand et al. [8] introduced a fusion-based MIW system. The technique used NSCT for the fusion of medical images. They incorporated NSCT,

fast Walsh- Hadamard Transform, and Schur decomposition for the watermarking. The watermarked image is finally encrypted with a hyperchaotic and DNA scheme to improve security. Singh et al. [31] designed a MIW strategy for telemedicine applications. The cover image is encrypted using a key-based encryption scheme. The technique utilized RDWT and RSVD for the watermarking. El-Shafai and Hemdan [13] developed a fusion-based watermarking system for color images. Here the color watermark image is separated into RGB components. Three gray images are fused to each of the separated RGB components to form a fused watermark image using a wavelet-based fusion scheme. Finally, DWT and SVD are utilized to embed the watermark into the RGB parts of the color host medical image. Mahto et al. [21] proposed a fusion-based watermarking scheme. The technique used NSCT for the fused watermark image. The contourlet transform and RSVD hybrid approach are used to embed encrypted watermark images into the blue channel of the cover image.

MIW has been used in a variety of ways recently, according to various authors. Anand and Singh [9] used RDWT, Hessenberg Decomposition (HD), and Randomized SVD (RSVD) to create an algorithm for the security of covid-19 patient records. They used distinct watermarks to boost the level of protection and used lightweight encryption for the final scrambled watermarked image. The scheme employed different matrices to evaluate the performance. Khare and Srivastava [19] introduced a MIW scheme based on homomorphic transform-RDWT-SVD. They tried 2-D Chaotic Arnold transform as an encryption technology to provide confidentiality to the system. The authors performed different evaluation matrices to check the performance of the implemented system. Based on NSCT-MSVD, Anand and Singh [5] developed a technique for the preservation of medical images. Shamir's technique protects data to be safely kept and communicated. In the technique [6], the authors generated the dual watermark using DWT and Turbo encoding. The embedding procedure employs RDWT, RSVD, and optimization approaches. They encrypted the watermarked image with an algorithm for added protection. For the evaluation, the approach deployed a variety of measuring parameters. Soualmi et al. [34] proposed a blind MIW technique for inserting encrypted watermarks based on Schur Decomposition, with the chaotic sequence as the scrambling mechanism. The technique used various evaluation matrices to verify the scheme's performance. The authors of [3] developed a multi-MIW technique based on the DWT-SVD approach, using the hamming code method for text encryption and various compression methods for data transmission. They used various evaluation methodologies to verify the system's performance. Kahlessenane et al. [17] devised a method for safeguarding medical images. Their study combined DWT, NSST, NSCT, and DCT with Schur decomposition. The watermarks are implanted in the medium frequency band to improve robustness and imperceptibility. They practiced several matrix parameters to test the scheme's performance.

The security of transmitted medical data is also essential during the transmission through open networks. Various authors proposed different works to resolve this. In [18], the authors utilized 5D-dimensional hyper chaotic with compressive sensing to transmit medical data over the Internet of Things Networks. The authors used a blockchain system for secure medical data transmission by incorporating neural networks in [23]. Nisha Rajeeva et al. [25] developed a security system for transmitting Electro Cardio Grams using triple data encryption standard and is optimized with water cycle optimization. In [27], the authors proposed a medical data security system using blockchain technology. For authentication, the system uses an access control mechanism.

3 Background preliminaries

3.1 DWT

The DWT offers multi resolutions of an image representation, which aids in analyzing image data. It decomposes an image into low frequency (approximate) and high frequency (detailed) sub-bands. It has the advantages like high imperceptibility and good robustness against noise and compression attacks [20]. Since it consists of a downsampling block, it has the property of shift variance. The DWT decomposition can be implemented using the Fig. 1. Here $f[n]$ is the input data, and $f'[n]$ is the reconstructed data using DWT.

3.2 RDWT

RDWT has shift-invariance property due to the lack of down-sampling and up-sampling blocks. Here, the image is also decomposed into approximate and detailed components but the same size as the host image. Hence the embedding capacity is improved [33]. It is also robust against additive noise. The implementation of RDWT is shown in the Fig. 2, where $f[n]$ is the input data, and $f'[n]$ is the reconstructed data using RDWT.

3.3 MSVD

SVD will take the place of FIR filters thanks to MSVD. MSVD disintegrates an image like wavelets. While wavelet and advanced wavelet transforms supply local and directional information, MSVD does not. Since it requires less computing than SVD, it is more suited for real-time applications. Compared to wavelets, MSVD's decomposition is data-set-dependent rather than relying on any basis functions. Like wavelets, signals are individually filtered using low and high pass finite impulse responses. The output is eventually decimated by two to reach the first level of decomposition. The abovementioned process can be repeated to get the subsequent levels. MSVD offers excellent robustness against geometrical attacks [29]. It is comparable to wavelet decomposition in that MSVD can be applied at multiple levels to watermark images, which makes it appropriate for image watermarking.

3.4 Entropy

According to [1], high entropy parts of an image have a higher information density, which leads to higher complexity and uncertainty. Because of the reduced visual sensitivity brought on by the increased complexity, the Just Noticeable Threshold (JND) thresholds

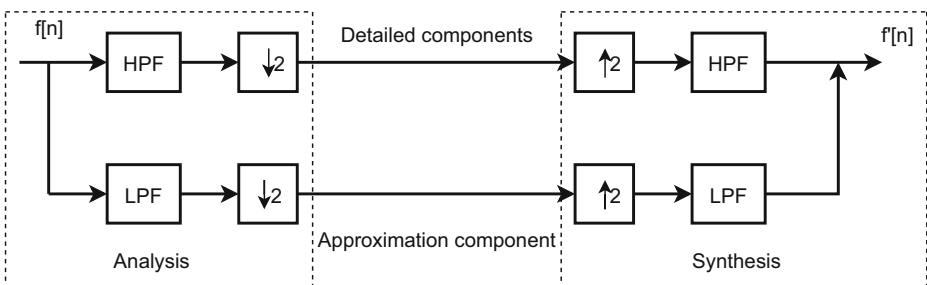


Fig. 1 Decomposition of DWT

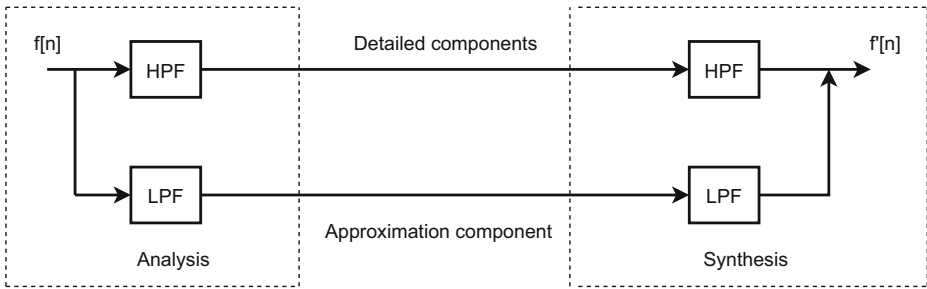


Fig. 2 Decomposition of RDWT

also increase. The JND thresholds dictate where and how strongly a watermark signal can be used without lowering the image quality. Hence more prominent energy watermarks can be implanted into the image in high entropy regions less sensitive to Human Visual System, thus improving the imperceptibility of the system.

4 Proposed scheme

This section explains the proposed RDWT-DWT-MSVD-based robust and secure MIW scheme. The three divisions of the completed work are (1) The generation of a carrier image by fusing multimodal images, (2) Incorporating and extracting a medical watermark image into the fused cover image, and (3) Watermark image encryption

4.1 The generation of a carrier image by fusing multimodal images

The proposed scheme used the FF technique to merge multimodal images, resulting in a fused host image with increased information richness, which is particularly valuable for medical diagnostics [36]. Algorithm 1 shows the procedures for creating a host image using the FF technique. Initially, image gradient magnitude is employed to determine image sharpness and contrast. Then, a fast morphological closing operation is applied to the image gradient magnitude to bridge gaps and fill holes. The multimodal image gradient is used to create the weight map and is filtered using a fast structure-preserving filter. A weighed-sum rule is then employed to build the fused image. Figure 3 represents the fused result. Table 1 explains all the notations used in the algorithms.

4.2 Incorporating and extracting a medical watermark image into the fused cover image

The suggested strategy applied the RDWT-DWT-MSVD approach for the watermarking. Here we used a thorax-CT image as a watermark, as shown in Fig. 4. Figure 5 depicts the complete embedding steps. The procedure used a one-level RDWT to create high and low-frequency components on C_FUSED . From this, select the element with the highest entropy. DWT is applied to this component, yielding approximation and detailed features. The scheme employed MSVD to the highest entropy DWT component. MSVD is also used for the medical watermark W . The HL sub-band is selected experimentally for watermarking since high-frequency components are less sensitive to the human visual system, which

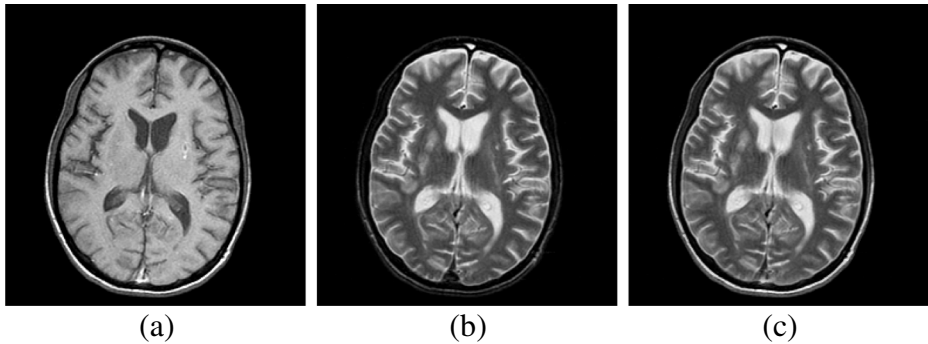


Fig. 3 (a) T1-weighted MR image (b) T2-weighted MR image (c) Fused image

Input: $MR_IMAGE[M \times N]$, $CT_IMAGE[M \times N]$ of radius r and parameter λ

Output: C_FUSED

begin

Step 1: Element number calculation in box window

1. $N \leftarrow \text{boxfilter}(\text{ones}[M, N], R)$;

Step 2: Calculation of image sharpness and contrast using gradient magnitude GM

Step 3: Normalization of GM

2. $D \leftarrow \text{Normal}(GM)$;

Step 4: Apply dilation and closing operation

3. $D_DIL \leftarrow \text{Dilate}(D)$;

4. $g \leftarrow \text{Close}(D_DIL)$;

Step 5: Repeat the steps 2 to 4 for both the images

Step 6: Calculation of weight matrix wm

Step 7: Smoothing of wm

Step 8: Calculate the mean of wm

Step 9: Calculate the variance of wm

Step 10: Apply structure preserving filter

Step 11: Obtain fused image

return C_FUSED

Algorithm 1 FF based image fusion.

increases the system's invisibility. The watermark W is put into the C_FUSED using an embedding rule given in step 3 of Algorithm 2. Apply inverse MSVD, DWT, and RDWT to make the watermarked image W_M .

For recovering W , apply RDWT to the decrypted watermarked image $W_M_DECRYPTED$. Find the frequency component with the highest Entropy, and DWT is applied. MSVD is applied to the maximum entropy DWT component to obtain four frequency components. The watermark can be retrieved using the extraction rule given in step 4 of Algorithm 3, and IMSVD is employed to obtain the watermark. The original host image can be retrieved by applying IMSVD, Inverse DWT, and Inverse RDWT. The extraction steps are shown in Fig. 6. Algorithms 2 and 3 explain the complete procedure.

Table 1 The notations with their explanations used in the algorithms

Notations	Explanation
MR_IMAGE	MRI Input image
CT_IMAGE	CT Input image
C_FUSED	Fused image after fusion operation
r	Radius of image
M x N	Image size
GM	Gradient Magnitude
D	Normalized GM
D_DIL	D after dilation
g	D_DIL after closing operation
wm	Weight matrix
W	Watermark image
G	Gain factor
W_M.ENCRYPTED	Encrypted watermarked image
LL,LH,HL,HH	1 level components of C_FUSED using RDWT
ELL,ELH,EHL,EHH	Entropy of 1 level components of C_FUSED
CE_MAX	Component with maximum entropy of C_FUSED
CA,CH,CV,CD	1 level components of CE_MAX using DWT
ECA,ECH,ECV,ECD	Entropy of 1 level components of CE_MAX
CR_MAX	Component with maximum entropy of CE_MAX
XLL,XLH,XHL,XHH	Components after applying MSVD to CR_MAX
WLL,WLH,WHL,WHH	Components after applying MSVD to W
XHL_NEW	Modified component after applying MSVD to W
W_M.DWT	Image after applying inverse MSVD
W_M.RDWT	Image after applying inverse DWT
W_M	Watermarked image
W_M.DECRYPTED	Decrypted watermarked image
RLL,RLH,RHL,RHH	Components of W_M.DECRYPTED using RDWT
ERLL,ERLH,ERHL,ERHH	Entropy components of W_M.DECRYPTED
RCE_MAX	Max. entropy component of W_M.DECRYPTED
RA,RH,RV,RD	Components of RCE_MAX using DWT
ERA,ERH,ERV,ERD	Entropy components of RCE_MAX
ECR_MAX	Maximum entropy component of RCE_MAX
RXLL,RXLH,RXHL,RXHH	Components of ECR_MAX using MSVD
RXHL_NEW	Retrieved watermark component using G
L[M N]	New sequences generated using chaotic system
Vector [s]	Vector obtained by ascending L[M N]
R	Permuted vector
R'[M N]	Converted R to MXN matrix
SB[2 2]	Sub-block conversion of R'[M N] of size [2 2]
W_M.E	Matrix obtained by SB[2 2]* Fibonacci matrix

Fig. 4 Thorax-CT watermark image



4.3 Watermark image encryption

To strengthen the security of the watermark images, we used the HFQM [15] encryption technique, which employs a six-dimensional hyper-chaotic system with a Fibonacci Q matrix. Due to its complex, highly dynamic behaviors, and two positive Lyapunov exponents, the

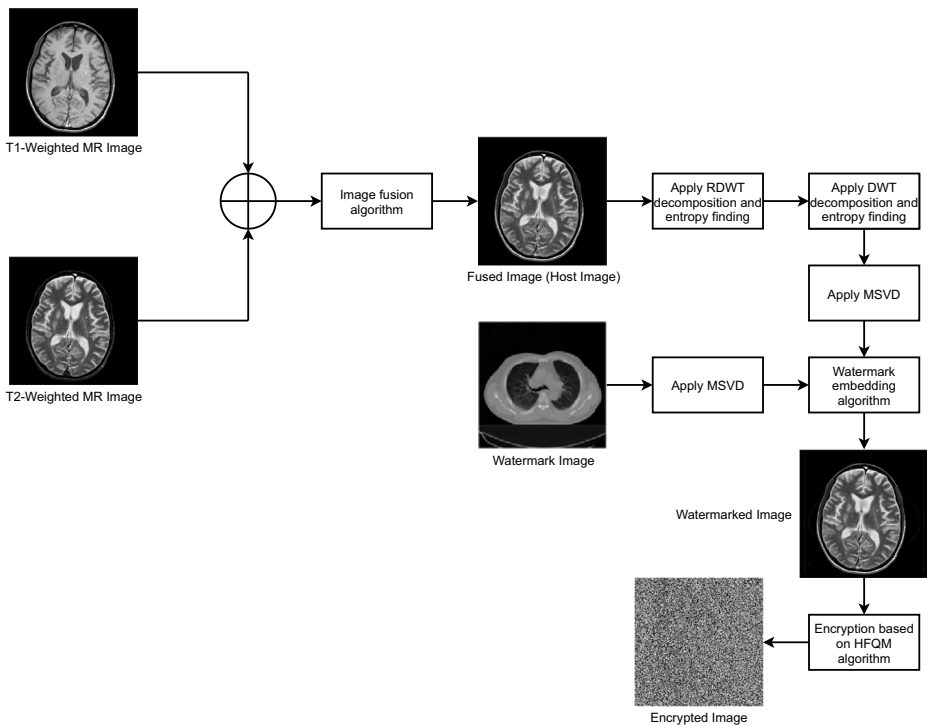


Fig. 5 Watermark embedding process with encryption

Input: C_FUSED, W, G

Output: $W_M_ENCRYPTED$

begin

Step 1: 1 level decomposition of C_FUSED using RDWT and entropy calculation

1. $[LL, LH, HL, HH] \leftarrow RDWT(C_FUSED)$;
2. $[ELL, ELH, EHL, EHH] \leftarrow Entropy(LL, LH, HL, HH)$;
3. $CE_MAX \leftarrow Maximum(ELL, ELH, EHL, EHH)$;

Step 2: 1 level decomposition of CE_MAX and W using DWT and MSVD

4. $[CA, CH, CV, CD] \leftarrow DWT(CE_MAX)$;
5. $[ECA, ECH, ECV, ECD] \leftarrow Entropy(CA, CH, CV, CD)$;
6. $CR_MAX \leftarrow Maximum(ECA, ECH, ECV, ECD)$;
7. $[XLL, XLH, XHL, XHH] \leftarrow MSVD(CR_MAX)$;
8. $[WLL, WLH, WHL, WHH] \leftarrow MSVD(W)$;

Step 3: Watermark insertion using G

9. $XHL_NEW \leftarrow XHL + G * WHL$;

Step 4: Apply IMSVD, IDWT, and IRDWT

10. $W_M_DWT \leftarrow IMSVD(XLL, XLH, XHL_NEW, XHH)$;
11. $W_M_RDWT \leftarrow IDWT(W_M_DWT)$;
12. $W_M \leftarrow IRDWT(W_M_RDWT)$;

Step 5: Apply encryption HFQM to W_M

13. $W_M_ENCRYPTED \leftarrow HFQM(W_M)$;

return $W_M_ENCRYPTED$

Algorithm 2 Watermark embedding with encryption.

6D hyperchaotic architecture improves encryption performance and elevates security levels. The scrambled image can be generated easily, quickly, and effectively using the Fibonacci Q-matrix. There are two stages to encryption: confusion and diffusion. In each of these procedures, the arrangements and values of the pixels are altered. The 6D hyperchaotic system is the basis of the confusion step. The system's initial condition is first calculated based on the plain image. The hyperchaotic procedure is then iterated to produce a new vector, after which we choose three sequences (x_1 , x_3 , and x_5). This vector has been sorted. The arrangement of the numbers in the sorted order is used to confuse the plain image. The diffusion process is carried out to obtain the encrypted image after confusing the plain image. Algorithm 4 explains the encryption technique.

5 Experimental analysis and performance evaluation

We implemented the described technique using an Intel Core i3, 8GB RAM processor, in MATLAB 2022a and carried out the trials with 256x256 MRI, CT scans [16], and a 128x128 thorax-CT watermark medical image [22]. Finding performance parameter matrices such as PSNR and SSIM [3] were used to assess the method's imperceptibility, given by (1) and (4) respectively. PSNR measures the visual similarity between the original and marked images and should have a high value, preferably greater than 30 dB. The structural similarity between the cover image (i) and the marked image (w) is quantified using SSIM,

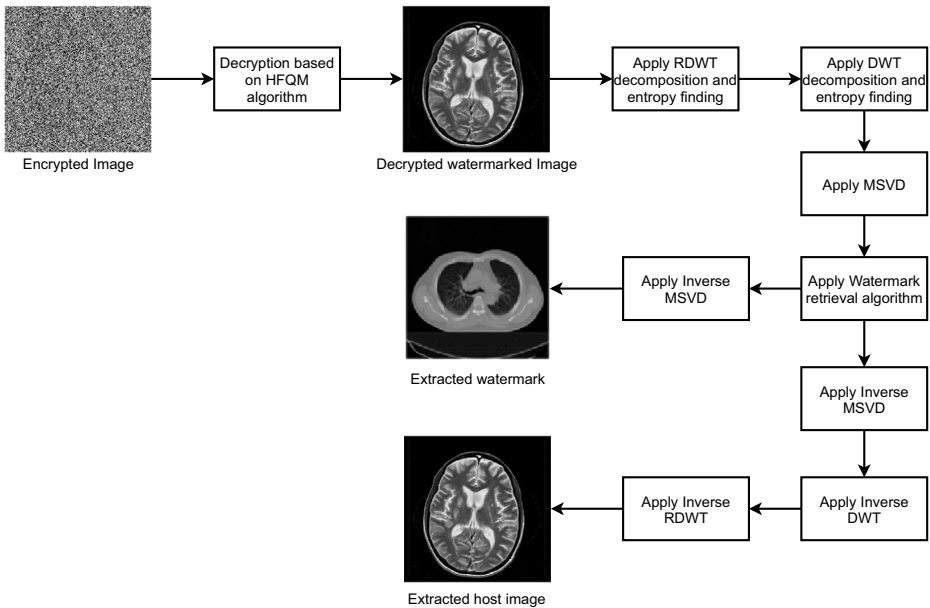


Fig. 6 Watermark retrieval process with decryption

Input: $W_M_ENCRYPTED, G$

Output: W

begin

Step 1: Apply decryption to $W_M_ENCRYPTED$ using HFQM

1. $W_M_DECRYPTED \leftarrow HFQM(W_M_ENCRYPTED)$;

Step 2: 1 level decomposition of $W_M_DECRYPTED$ using RDWT and entropy calculation

2. $[RLL, RLH, RHL, RHH] \leftarrow RDWT(W_M_DECRYPTED)$;

3. $[ERLL, ERLH, ERHL, ERHH] \leftarrow Entropy(RLL, RLH, RHL, RHH)$;

4. $RCE_MAX \leftarrow Maximum(ERLL, ERLH, ERHL, ERHH)$;

Step 3: 1 level decomposition of RCE_MAX using DWT and MSVD

5. $[RA, RH, RV, RD] \leftarrow DWT(RCE_MAX)$;

6. $[ERA, ERH, ERV, ERD] \leftarrow Entropy(RA, RH, RV, RD)$;

7. $ECR_MAX \leftarrow Maximum(ERA, ERH, ERV, ERD)$;

8. $[RXLL, RXLH, RXHL, RXHH] \leftarrow MSVD(ECR_MAX)$;

Step 4: Watermark retrieval using G

9. $RXHL_NEW \leftarrow (RXHL - XHL)/G$;

Step 5: Apply IMSVD

10. $W \leftarrow IMSVD(WLL, WLH, RXHL_NEW, WHH)$;

return W

Algorithm 3 Decryption with watermark retrieval.

Input: W_M

Output: $W_M_ENCRYPTED$

begin

1. Initialize $i = 1$;

Step 1: Generation of initial key of the chaotic system

2. $[MN] \leftarrow size(W_M)$;

3. $Vector[P] \leftarrow W_M([MN])$;

4. Calculate $X1 = \sum_{i=1}^{MN} \frac{P(i)+MN}{2^{23}+MN}$

Step 2: Formulation of 6D chaotic system and finding 3 new sequences

5. $X_i = mod(X_{i-1} * 10^6, 1), i = 2, 3..6$;

6. $L[MN] \leftarrow X1, X3, X5$;

7. $Vector[S] \leftarrow Ascend(L[MN])$;

Step 3: Calculation of permuted vector

8. $R \leftarrow P(Si), i = 1 : MN$;

Step 4: Conversion of R to $M \times N$ matrix and divide into sub-blocks of size 2×2 for each

9. $R[MN] \leftarrow R$;

10. $SB[22] \leftarrow sub - blockdivision(R[MN])$;

Step 5: Multiply each sub-block with Fibonacci matrix (Q^{10} matrix)

11. $W_M_E \leftarrow SB[22] * Q^{10}$;

Step 6: Repeat 2 to 5 steps two times, $i \leq 2$ to get final encrypted output $W_M_ENCRYPTED$

12. $W_M_ENCRYPTED \leftarrow W_M_E$;

return $W_M_ENCRYPTED$

Algorithm 4 Encryption of watermarked image.

and the optimum value is 1. The NC [3] was used to analyze the scheme's susceptibility to attacks, and its optimal value is 1, given by (3).

$$PSNR = 10 \log \frac{255^2}{MSE} \quad (1)$$

where MSE is the Mean Square Error and is given by

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (f_w(i, j) - f(i, j))^2 \quad (2)$$

$$NC = \frac{\sum_{i=1}^{M1} \sum_{j=1}^{N1} I_w(i, j) I(i, j)}{\sqrt{\sum_{i=1}^{M1} \sum_{j=1}^{N1} |I(i, j)|^2 (I_w(i, j))^2}} \quad (3)$$

here $f_w(i, j)$, $f(i, j)$, $I_w(i, j)$, $I(i, j)$ are the watermarked image, original cover image, extracted mark, and original mark respectively.

$$SSIM(i, w) = \frac{(2\mu_i \mu_w + c_1)(2\sigma_{iw} + c_2)}{(\mu_i^2 + \mu_w^2 + c_1)(\sigma_i^2 + \sigma_w^2 + c_2)} \quad (4)$$

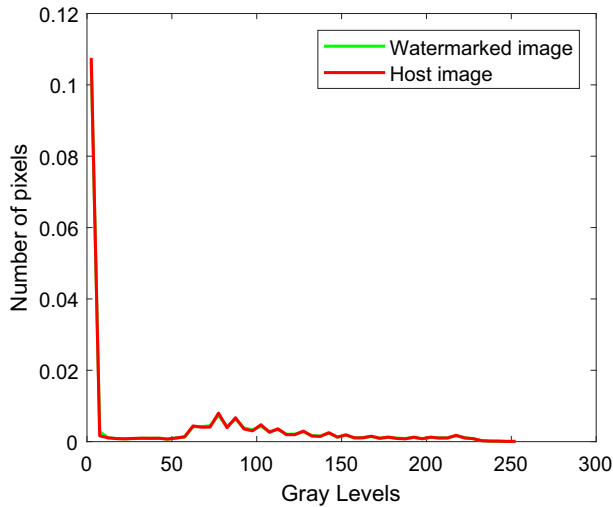


Fig. 7 Difference in histogram distribution of original host image and watermarked image

$\mu_i, \mu_w, \sigma_i, \sigma_w$ are the mean and variance values of the cover image and the watermarked image respectively. σ_{iw} represents the cross covariance between host image and watermarked image, c_1, c_2 are the constants with small values.

Table 2 Performance of the proposed scheme at various gain factors

Gain Factor	PSNR(dB)	SSIM	NC	NPCR	UACI
0.03	90.31	1	0.8969	0.9794	0.3599
0.04	75.76	1	0.9299	0.979	0.3597
0.05	70.26	0.9999	0.9491	0.9774	0.3587
0.07	66.25	0.9995	0.9706	0.9823	0.3604
0.09	65.15	0.9995	0.9805	0.9819	0.3593
0.1	64.59	0.9994	0.9837	0.9821	0.3583
0.3	54.55	0.9939	0.9978	0.9843	0.357
0.5	50.14	0.9847	0.9992	0.9867	0.3569
0.7	47.34	0.975	0.9995	0.9858	0.3552
0.9	45.11	0.9645	0.9997	0.9875	0.3564
1	44.22	0.9599	0.9997	0.9877	0.3537
1.3	41.94	0.9467	0.9999	0.9888	0.3545
1.5	40.73	0.939	0.9999	0.9897	0.3537
1.7	39.64	0.9318	0.9999	0.9889	0.3537
1.9	38.67	0.9251	0.9999	0.9893	0.3521
2.3	37.02	0.9129	0.9999	0.9907	0.353
2.4	36.66	0.91	1	0.9904	0.3525
2.6	35.97	0.9048	1	0.9908	0.3519
3	34.73	0.8948	1	0.9916	0.351

The encryption scheme's performance was tested by determining characteristics such as the Number of Changing Pixel Rate (NPCR), Unified Averaged Changed Intensity (UACI) [3], and Entropy (randomness) [31] given by (5), (7), and (8) respectively.

$$NPCR = \frac{1}{M \times N} \sum_{i,j} C(i, j) \quad (5)$$

$$C(i, j) = \begin{cases} 0, & \text{if } C(i, j) = C'(i, j) \\ 1, & \text{if } C(i, j) \neq C'(i, j) \end{cases} \quad (6)$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C(i, j) - C'(i, j)|}{255} \quad (7)$$


























$$E = - \sum_{k=1}^{255} (P(I_k) \times \log_2 P(I_k)) \quad (8)$$

where $P(I_k)$ is the probability of pixel I_k

5.1 Imperceptibility and robustness analysis

Figure 7 shows the difference in the histogram distribution of the original host image and the watermarked image using the devised scheme. The graphs overlapped, indicating that the cover and watermarked images were visually similar. Thus the suggested plan has excellent imperceptibility.

Table 3 Performance evaluation of the proposed technique

Input image 1	Input image 2	Fused image	Marked image	Extr. mark	PSNR (dB)	SSIM	NC
					52.44	0.9904	0.9973
					52.77	0.9920	0.9946
					52.64	0.9912	0.9954
					52.11	0.9897	0.9987
					53.60	0.9929	0.9971
Average					52.71 dB	0.9912	0.9966

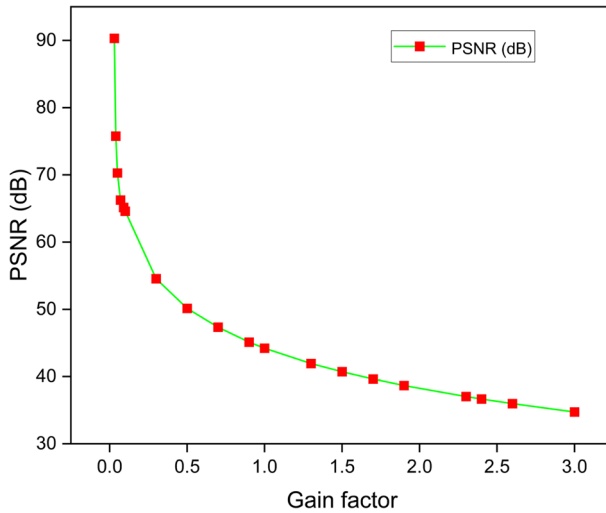


Fig. 8 Variation of PSNR (dB) with Gain factor

Table 2 shows the performance of the described system at various gain factors. The maximum PSNR, SSIM, and NC are 90.31 dB, 1, and 1, respectively. The optimum value of the gain factor is 0.3, at which the suggested technique has high importance in terms of all the above parameters. Figure 8 illustrates the variation of PSNR with the gain factor; its values fall as the gain factor rises. As the gain factor grows, the value of NC increases, eventually reaching an optimal value of 1, as shown in Fig. 9.

Table 3 illustrates the performance of the developed approach with various sets of images at a gain factor of 0.1. We obtained average PSNR, SSIM, and NC values of 52.71

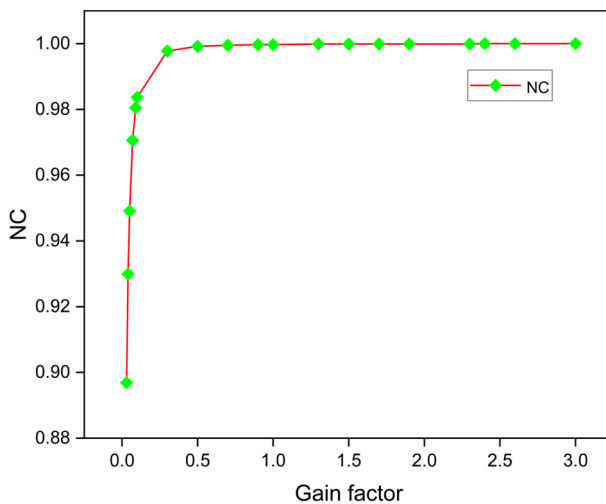




























Fig. 9 Variation of NC with Gain factor

dB, 0.9912, 0 and 0.9966 for different clinical scans. The method also obtained the maximum SSIM value of 0.9987 between the original carrier image and the extracted cover image, indicating less loss during the process, which is essential for MIW. The values show

Table 4 Robustness evaluation of the proposed scheme

Type of attacks	Attacked marked image	Extr. mark	NC
Salt & Pepper Noise(0.5)			0.9996
Gaussian noise(0.5)			0.9996
Speckle noise(0.5)			0.9999
Gaussian LP filter(1)			1
Median filter [3 3]			1
Average filter [3 3]			1
Gaussian filter [3 3]			1
Rotate45°			1
Jpeg($Q = 60$)			1
Sharpen			1
Histogr. equal.			1
Cropping			1
Translate			1

that the suggested scheme performs exceptionally well in imperceptibility, robustness, and confidentiality.

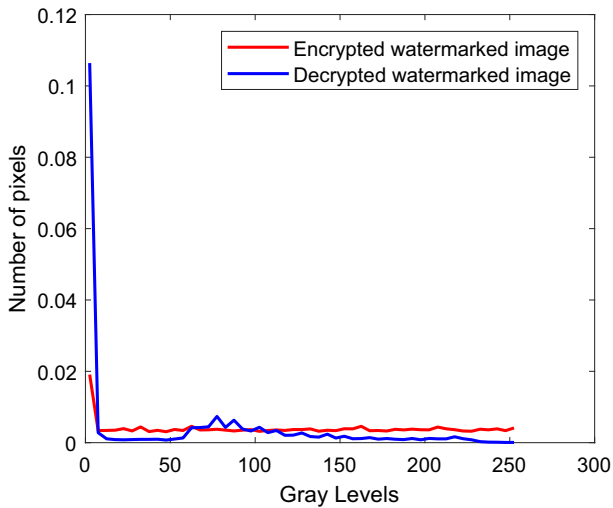
Tables 4 and 5 show the technique's robustness against several image processing assaults. Using the developed hybrid scheme, it can withstand the common watermarking attacks like noise addition, compression, geometrical watermarks, etc. The method's NC value is 1 for practically all attacks and close to 1 for the others, which indicates that the developed hybrid technique is exceptionally resistant to various watermarking attacks.

Table 5 Performance of the proposed scheme against various image processing attacks

Type of attacks	NC
Salt and pepper noise($Noisedensity = 0.0001$)	1
Salt and pepper noise($Noisedensity = 0.001$)	1
Salt and pepper noise($Noisedensity = 0.1$)	0.9999
Gaussian noise ($Var = 0.0001$)	1
Gaussian noise ($Var = 0.001$)	1
Gaussian noise ($Var = 0.1$)	0.9998
Speckle noise($Var = 0.0001$)	1
Speckle noise($Var = 0.001$)	1
Speckle noise($Var = 0.5$)	0.9999
Gaussian lowpass filter($Var = 0.4$)	1
Gaussian lowpass filter($Var = 0.6$)	1
Gaussian lowpass filter($Var = 1.0$)	1
Median filter [1 1]	1
Median filter [3 3]	1
Average filter [1 1]	1
Average filter [3 3]	1
Gaussian filter [1 1]	1
Gaussian filter [3 3]	1
Rotation(1 degree)	1
Rotation(45 degree)	1
Rotation(90 degree)	1
Jpeg compression ($Q = 10$)	1
Jpeg compression ($Q = 50$)	1
Jpeg compression ($Q = 90$)	1
Sharpening (0.01)	1
Sharpening (0.1)	1
Histogram equalization	1
Motion blur	1
Image scaling(0.5)	1
Image scaling(2)	1
Image cropping[20 20 100 100]	1
Translation [20 20]	1
Combinational attack (Gaussian noise(0.0002)+Rotation(90°) +Jpeg compression($Q = 70$))	1

Table 6 Performance of the encryption scheme

Image set	NPCR	UACI	Entropy	Diagonal	Vertical	Horizontal
1	0.987	0.3554	7.6627	0.0053	0.007	0.0851
2	0.9893	0.3531	7.791	0.0005	-0.003	0.0696
3	0.9929	0.3476	7.879	0.0031	-0.0004	0.0396
4	0.9838	0.3553	7.6852	0.0032	0.013	0.1017
5	0.9719	0.3633	7.4856	0.0042	0.0003	0.1165
Average value	0.985	0.3549	7.7007	0.0033	0.0034	0.0825

**Fig. 10** Difference in histogram distribution of encrypted and decrypted watermarked image**Table 7** Comparison of the proposed scheme with existing techniques

Type of attacks	Ref [7]	Ref [19]	Ref [5]	Proposed
Salt and pepper noise(<i>Noisedensity</i> = 0.0001)	1	0.9993	0.9945	1
Salt and pepper noise(<i>Noisedensity</i> = 0.001)	0.9982	0.9987	0.9945	1
Median filter [2 2]	0.9687	0.9981	0.9906	1
Jpeg compression ($Q = 10$)	0.9855	0.9995	0.9821	1
Jpeg compression ($Q = 50$)	0.9934	0.9993	0.9835	1
Jpeg compression ($Q = 90$)	0.9939	0.9997	0.9935	1
Sharpening	0.9913	0.9862	0.9999	1
Histogram equalization	0.9989	0.9988	0.9888	1
Image scaling	0.9488	0.9994	0.9839	1
Image cropping	0.9986	0.9982	0.9927	1

The bold entries indicate the best values

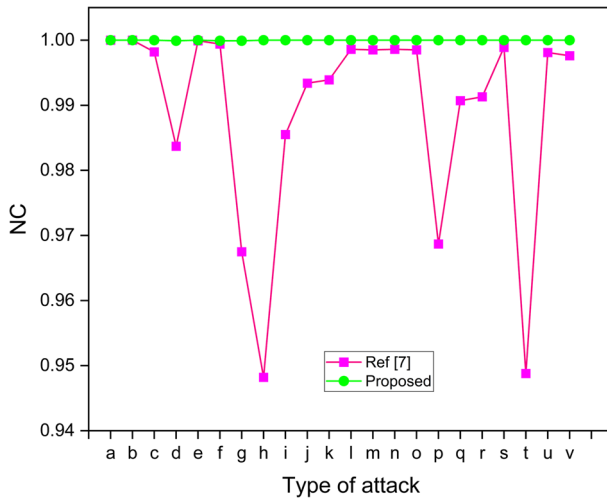


Fig. 11 Robustness comparison of proposed scheme with Ref [7]:(a)salt & pepper(0.0001) (b)salt & pepper(0.0005) (c)salt & pepper(0.001) (d)salt & pepper(0.01) (e)Gaussian noise(0.0005) (f)Gaussian noise(0.005) (g)Gaussian noise(0.05) (h)Rotation(1°) (i)Jpeg compression($Q = 10$) (j)Jpeg compression($Q = 50$) (k)Jpeg compression($Q = 90$) (l)Gaussian lowpass filter(0.4) (m)Gaussian lowpass filter(0.6) (n)cropping[20 20 400 480] (o)Median filter[1 1] (p)Median filter[2 2] (q)sharpening mask(0.01) (r)sharpening mask(0.1) (s)Histogram equalization (t)Image scaling(2) (u)speckle noise(0.001) (v)speckle noise(0.005)

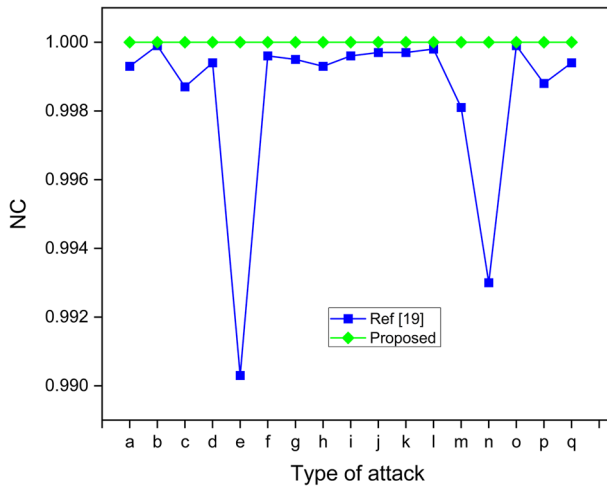


Fig. 12 Robustness comparison of proposed scheme with Ref [19]:(a)salt & pepper(0.0001) (b)salt & pepper(0.0002) (c)salt & pepper(0.001) (d)Gaussian noise(0.0002) (e)Gaussian noise(0.001) (f)Rotation(2°) (g)Jpeg compression($Q = 10$) (h)Jpeg compression($Q = 50$) (i)Jpeg compression($Q = 70$) (j)Jpeg compression($Q = 80$) (k)Jpeg compression($Q = 90$) (l)speckle noise(0.0001) (m)Median filter[2 2] (n)Median filter[3 3] (o)sharpening mask (p)Histogram equalization (q)Image scaling

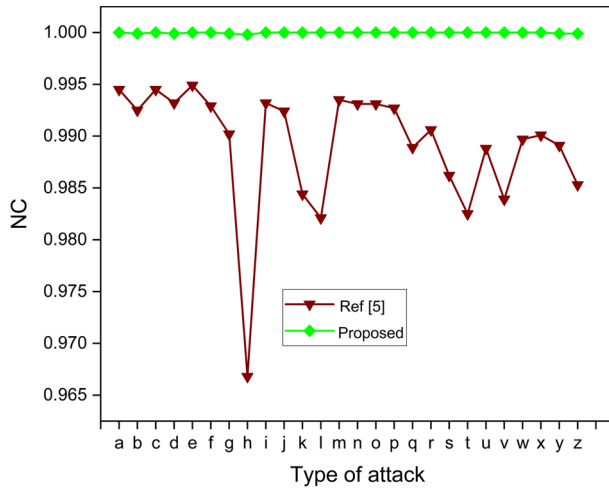


Fig. 13 Robustness comparison of proposed scheme with Ref [5]:(a)salt & pepper(0.0001) (b)salt & pepper(0.1) (c)salt & pepper(0.001) (d)salt & pepper(0.01) (e)Gaussian noise(0.0001) (f)Gaussian noise(0.001) (g)Gaussian noise(0.01) (h)Gaussian noise(0.1) (i)Rotation(1°) (j)Rotation(45°) (k)Rotation(90°) (l)Jpeg compression($Q = 10$) (m)Jpeg compression($Q = 90$) (n)Gaussian lowpass filter(0.4) (o)Gaussian lowpass filter(0.6) (p)cropping[20 20 400 480] (q)Median filter[3 3] (r)Median filter[2 2] (s)sharpening mask(0.01) (t)sharpening mask(0.1) (u)Histogram equalization (v)Image scaling(2) (w)Image scaling(0.5) (x)speckle noise(0.001) (y)speckle noise(0.05) (z)speckle noise(0.5)

5.2 Encryption analysis

The difference in histogram distribution between the encrypted and decrypted watermarked images is depicted in Fig. 10; they are uncorrelated, which indicates that the proposed technique has a high level of security. Further, the performance of the encryption algorithm is evaluated using the parameters NPCR, UACI, Entropy, Diagonal, Vertical, and Horizontal correlation coefficients [15] as shown in Table 6. The average NPCR and UACI values are 0.985 and 0.3549, respectively, close to ideal (0.996034 and 0.3346, respectively), indicating the excellent robustness of the encryption algorithm. The average Entropy between the plain and encrypted images is 7.7007 (the perfect value is 8), showing the encryption scheme's unpredictability. The average values of the Diagonal, Vertical and Horizontal correlation coefficients are 0.0033, 0.0034, and 0.0825, close to the ideal value (zero), reducing the correlation in the ciphered image. Thus the suggested encryption scheme enhances the security of the system.

Table 8 Comparison of the proposed technique with existing techniques in terms of average embedding time and extraction time (in seconds)

Watermarking process	Ref [7]	Ref [19]	Proposed
Image fusion	0.7696	–	0.8251
Watermark embedding	0.8953	4.2794	0.3958
Encryption	0.9383	–	0.4366
Decryption	0.7526	–	0.3181
Watermark extraction	0.6340	4.2582	0.4721

5.3 Comparison analysis

Table 7 shows the comparison result of the proposed scheme's performance to that of [5, 7, 19]. Figures 11, 12, and 13 depict the results. Compared to state-of-the-art approaches, the proposed scheme outperforms them in every way. Table 8 evaluates the embedding and extraction times of the developed technique to the existing methods. The image fusion takes an average of 0.8251 seconds, including 0.3958 seconds for embedding, 0.4366 seconds for encryption, 0.3181 seconds for decryption, and 0.4721 seconds for extraction, which are very low compared to existing procedures. Thus the established technology can be successfully used in e-health care applications utilizing cloud computing techniques.

6 Conclusion

This hybrid MIW approach is based on image fusion. It leverages the FF algorithm for multi-modal image fusion and results in a fused image with increased medical information, which serves as the host image. The proposed technique utilized RDWT-DWT-MSVD methodology for the watermark insertion and retrieval procedure, producing excellent results in imperceptibility and robustness for the system. The HFQM encryption algorithm added much more protection. The comparison results with other strategies indicate that the suggested technique is superior to the state of art techniques. As a result, the presented process can successfully implement MIW for e-healthcare applications employing cloud computing techniques. This method's reach can include multiple color MIW approaches with increased information capacity.

Funding and/or Conflicts of interests/ Competing interests The authors have no relevant financial or non-financial interests to disclose. The authors have no competing interests to declare that are relevant to the content of this article. All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript. The authors have no financial or proprietary interests in any material discussed in this article.

Data Availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

References

1. Akhbari B, Ghaemmaghami S (2005) Watermarking of still images using multiresolution singular value decomposition. In: 2005 international symposium on intelligent signal processing and communication systems. IEEE, pp 325–328
2. Ali M, Ahn CW, Pant M (2018) An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional fourier transforms. *Multimed Tools Appl* 77(10):11751–11773
3. Anand A, Singh AK (2020) An improved dwt-svd domain watermarking for medical information security. *Comput Commun* 152:72–80
4. Anand A, Singh AK (2021) Health record security through multiple watermarking on fused medical images. *IEEE Trans Comput Soc Syst* 9(6):1594–1603
5. Anand A, Singh AK (2021) Secret sharing based watermarking for copy-protection and ownership control of medical image. In: 2021 12th international conference on computing communication and networking technologies (ICCCNT). IEEE, pp 1–07
6. Anand A, Singh AK (2021) Hybrid nature-inspired optimization and encryption-based watermarking for e-healthcare. *IEEE Trans Comput Soc Syst* pp: 1–8, <https://doi.org/10.1109/TCSS.2022.3140862>
7. Anand A, Singh A (2021) Sdh: secure data hiding in fused medical image for smart healthcare. *IEEE Trans Comput Soc Syst* 9(4):1265–1273

8. Anand A, Singh AK (2022) A method for authenticating digital records for healthcare systems. *Sustain Comput Inf Syst* 33:100621
9. Anand A, Singh AK (2022) Dual watermarking for security of covid-19 patient record. *IEEE Trans Depend Secur Comput* 20(1):859–866
10. Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of dwt based on svd and abc. *Pattern Recogn Lett* 94:228–236
11. Chuying Y, Li J, Li X, Ren X, Gupta BB (2018) Four-image encryption scheme based on quaternion fresnel transform, chaos and computer generated hologram. *Multimed Tools Appl* 77(4):4585–4608
12. El Tokhy MS (2021) Development of optimum watermarking algorithm for radiography images. *Comput Electric Eng* 89:106932
13. El-Shafai W, Hemdan EE-D (2021) Robust and efficient multi-level security framework for color medical images in telehealthcare services. *J Amb Intell Human Comput*:1–16
14. Hemdan EE-D (2021) An efficient and robust watermarking approach based on single value decomposition, multi-level dwt, and wavelet fusion with scrambled medical images. *Multimed Tools Appl* 80(2):1749–1777
15. Hosny KM, Kamal ST, Darwish MM, Papakostas GA (2021) New image encryption algorithm using hyperchaotic system and fibonacci q-matrix. *Electronics* 10(9):1066
16. Johnson KA, Becker JA (2023) The whole brain atlas. <https://www.med.harvard.edu/aanlib/home.html>. Accessed: May 13, 2022
17. Kahlessenane F, Khaldi A, Kafi R, Euschi S (2021) A robust blind medical image watermarking approach for telemedicine applications. *Cluster Comput* 24(3):2069–2082
18. Kaur M, Singh D, Kumar V, Gupta BB, El-Latif AAA (2021) Secure and energy efficient-based e-health care framework for green internet of things. *IEEE Trans Green Commun Netw* 5(3):1223–1231
19. Khare P, Srivastava VK (2021) A secured and robust medical image watermarking approach for protecting integrity of medical images. *Trans Emerg Telecommun Technol* 32(2):e3918
20. Li Z, Zhang H, Liu X, Wang C, Wang X (2021) Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on rhfm and dwt-dct. *Digit Sign Process* 115:103062
21. Mahto DK, Om PS, Singh AK (2022) Fusiwi: fusion-based secure rgb image watermarking using hashing. *Multimed Tools Appl*:1–17
22. MedPix Database of medical images (2023) <https://medpix.nlm.nih.gov/home>. Accessed: May 13, 2022
23. Nguyen GN, Viet NHL, Elhoseny M, Shankar K, Gupta BB, El-Latif AAA (2021) Secure blockchain enabled cyber-physical systems in healthcare using deep belief network with resnet model. *J Parallel Distrib Comput* 153:150–160
24. Qingtang S, Chen B (2018) Robust color image watermarking technique in the spatial domain. *Soft Comput* 22(1):91–106
25. Raheja N, Manocha AK (2022) Iot based ecg monitoring system with encryption and authentication in secure data transmission for clinical health care approach. *Biomed Sign Process Control* 74:103481
26. Sajeer M, Mishra A, Sathidevi PS (2022) Recent advances in transform and hybrid domain digital watermarking techniques—a survey. *Soft Comput Secur Appl*:841–857
27. Sharma P, Borah MD, Namasudra S (2021) Improving security of medical big data by using blockchain technology. *Comput Electr Eng* 96:107529
28. Singh AK, Kumar B, Dave M, Ghrera SP, Mohan A (2016) Digital image watermarking: techniques and emerging applications. In: *Handbook of research on modern cryptographic solutions for computer and cyber security*, pp 246–272
29. Singh KU, Kumar A, Singh T, Ram M (2022) Image-based decision making for reliable and proper diagnosing in nifti format using watermarking. *Multimed Tools Appl*:1–27
30. Singh R, Nigam S, Singh AK, Elhoseny M (2020) Integration of wavelet transforms for single and multiple image watermarking. In: *Intelligent wavelet based techniques for advanced multimedia applications*, pp 51–63
31. Singh KN, Om PS, Singh AK, Agrawal AK (2022) Watmif: multimodal medical image fusion-based watermarking for telehealth applications. *Cognit Comput*:1–17
32. Singh D, Shivani S, Agarwal S (2013) Self-embedding pixel wise fragile watermarking scheme for image authentication. In: *International conference on intelligent interactive technologies and multimedia*. Springer, pp 111–122
33. Singh AK et al (2022) Fastmie: faster medical image encryption without compromising security. *Measurement* 196:111175
34. Soualmi A, Altı A, Laouamer L (2022) A novel blind medical image watermarking scheme based on schur triangulation and chaotic sequence. *Concurr Comput Pract Exp* 34(1):e6480

35. Turuk MP, Dhande AP (2016) A novel reversible multiple medical image watermarking for health information system. *J Med Syst* 40(12):1–13
36. Zhan K, Xie Y, Wang H, Min Y (2017) Fast filtering image fusion. *J Electron Imaging* 26(6):063004

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.