Cognitive Computation
https://doi.org/10.1007/s12559-022-10040-4

WatMIF: Multimodal Medical Image Fusion-Based Watermarking for Telehealth Applications

Kedar Nath Singh[1,2] · Om Prakash Singh[1] · Amit Kumar Singh[1] · Amrit Kumar Agrawal[3]

Received: 8 April 2022 / Accepted: 20 June 2022

Abstract

Over recent years, the volume of big data has drastically increased for medical applications. Such data are shared by cloud providers for storage and further processing. Medical images contain sensitive information, and these images are shared with healthcare workers, patients, and, in some scenarios, researchers for diagnostic and study purposes. However, the security of these images in the transfer process is extremely important, especially after the COVID-19 pandemic. This paper proposes a secure watermarking algorithm, termed WatMIF, based on multimodal medical image fusion. The proposed algorithm consists of three major parts: the encryption of the host media, the fusion of multimodal medical images, and the embedding and extraction of the fused mark. We encrypt the host media with a key-based encryption scheme. Then, a nonsubsampled contourlet transform (NSCT)-based fusion scheme is employed to fuse the magnetic resonance imaging (MRI) and computed tomography (CT) scan images to generate the fused mark image. Furthermore, the encrypted host media conceals the fused watermark using redundant discrete wavelet transform (RDWT) and randomised singular value decomposition (RSVD). Finally, denoising convolutional neural network (DnCNN) is used to improve the robustness of the WatMIF algorithm. The simulation experiments on two standard datasets were used to evaluate the algorithm in terms of invisibility, robustness, and security. When compared with the existing algorithms, the robustness is improved by 20.14%. Overall, the implementation of proposed watermarking for hiding fused marks and efficient encryption improved the identity verification, invisibility, robustness and security criteria in our WatMIF algorithm.

Keywords Medical images · Multimodal fusion · Watermarking · Encryption · Security · DnCNN

Introduction

Over recent years, the volume of big data has drastically increased for medical applications. Such data are shared by cloud providers for storage and further processing. Medical data in the form of images, contain sensitive information, and these images are shared with healthcare workers, patients, and, in some scenarios, researchers for diagnostic and study purposes [1]. Additionally, cloud computing in healthcare becomes an important solution for the storage, processing, and continuous availability of data supplied by multiple sources. However, an increasingly serious concern is the illegal copying, modification, and forgery of medical records [2]. Furthermore, the issue of identity theft and copyright protection is becoming more prevalent by the day [3, 4]. The integrity of data must be safeguarded against unauthorised users. Encryption is a popular technique for protecting data confidentiality and privacy [5, 6]. It can be considered an a priori protection in the sense that data are

✉ Amit Kumar Singh
amit.singh@nitp.ac.in

Kedar Nath Singh
knsinghait@gmail.com

Om Prakash Singh
omprakash7667@gmail.com

Amrit Kumar Agrawal
agrawal.amrit4@gmail.com

[1] Department of Computer Science & Engineering, National Institute of Technology Patna, Patna, Bihar, India

[2] Department of CSE, Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India

[3] Department of Computer Science & Engineering, Galgotias College of Engineering & Technology, Greater Noida, Uttar Pradesh, India

Published online: 07 July 2022

protected until they are decrypted. Furthermore, once data are decrypted, several security questions arise. Watermarking is a popular solution to handling the security issue of any encryption scheme [7]. It involves embedding a secret mark in the host media as a form of identification [8, 9]. The primary aim of watermarking is to enhance three features—invisibility, capacity, and robustness—that should be maintained to ensure a secure system [8]. Presently, multimodal image fusion is the technique of merging information from two or more image modalities into a single composite image that is better suited for diagnosis and assessment. However, the security of fused medical information in the transfer process is extremely important, especially after the COVID-19 pandemic.

This paper proposes a secure watermarking algorithm based on multimodal medical image fusion. The main contributions are as follows:

1. Advantages of image fusion: An NSCT-based fusion scheme is employed to fuse MRI and CT scan images, generating the fused mark image. This fused mark image has rich information, which is better suited for diagnostic and assessment than an individual image;
2. Encryption of host media before watermarking: A key-based encryption scheme is used to ensure the security of the watermarking system. The encryption scheme is fast without compromising the security of medical images, which is suitable for a telehealth scenario;
3. Embedding of the fused image through RDWT and RSVD: The fusion of RDWT and RSVD is utilised to perform an imperceptible marking of the fused image within the encrypted media. This combination offers not only high robustness and imperceptibility, but also increases the mark capacity with linear complexity. RDWT is shift-invariant and offers all the desirable properties of discrete wavelet transform (DWT) [10]. Additionally, RSVD [10] can be used to embed the mark data in the source image for reducing the amount of calculation, i.e. the computational cost;
4. Improved robustness: We have improved the robustness of the algorithm through DnCNN [11]. From the simulation, it is inferred that the WatMIF algorithm exhibits improved robustness compared to existing schemes.

The rest of the article is organised as follows: the following section presents the existing work related to image fusion-based watermarking; the Methodology Section discusses the proposed WatMIF algorithm; the Experiments Section demonstrates the experimental evaluation of the WatMIF algorithm; the Conclusion Section contains the concluding remark.

Related Works

For the last few years, different fusion-based watermarking mechanisms have been proposed for telehealth scenarios. For example, Singh and Singh [8] proposed a data hiding scheme using the NSCT, SVD, and Hessenberg decomposition techniques. They utilised the pseudo-magic cubes approach for large data embedding and the reduction of distortion. Furthermore, chaotic maps, deoxyribonucleic acid (DNA), and MD5 are used to enhance security. Experimental results show that the proposed scheme has high robustness and better hiding efficiency when compared to the existing scheme. Anand and Singh [12] proposed a novel joint spatial-transform domain technique to embed a fused medical image watermark with the cover image. Chaotic sequencing and singular value decomposition (SVD) are used to encrypt the marked medical image. The findings suggest that the approach has a greater robustness effect than previous techniques, with outstanding invisibility and payload. However, other security features, like statistical analysis, key space, and key sensitivity of the scheme, need to be verified. Bhardwaj [13] presented a dual image reversible data hiding method with great capacity. Paillier cryptography is used to encrypt both cover image and secret data. Encrypted secret data is embedded into the encrypted cover image. Furthermore, a fragile watermark is utilised for content verification on the beneficiary side. Experimental findings show that the scheme is robust, secure, has high embedding capacity, and can embed data at a high resolution. However, the embedding time of the scheme is higher than others. Vaidya [14] suggested the lifting wavelet transform (LWT)-DWT domain-based watermarking technique for medical image privacy. Arnold Cat map is utilised to enhance the security of watermarked images. The scheme achieved superior imperceptibility and robustness. However, the encryption method used in this scheme was not much secure. Sayah et al. [15] propounded a watermarking technique to ensure the integrity of the watermark. The medical image of the patient is first compressed, and patient information is embedded into it by DWT. A hash code of patient information is generated using the MD5 algorithm and also integrated to ensure integrity. Furthermore, the RC4 encryption scheme is used to encrypt the watermarked image. The suggested technique preserves a good quality of watermarked images and a strong resilience against numerous assaults. Ramzan et al. [16] presented a medical image watermarking scheme to preserve the integrity and authorisation of medical images. Watermark embedding is done by using Weber local descriptor (WLD) and discrete cosine transform (DCT), and its integrity is verified by Bioshashing code. Despite the fact that the proposed approach is resistant to a variety of assaults, the retrieved watermark image is noisy, and the

Table 1 Notation and explanation

Notation	Explanation	Notation	Explanation	Notation	Explanation
Cov_{img}	Cover image	Fus_{img}	Image after fusion	$a1, b1, c1, d1$	RDWT coefficients of encrypted image
X_p	Confusion key	RDWT	Redundant-discrete wavelet transform	$a2, b2, c2, d2$	RDWT coefficients of fused mark image
X_d	Diffusion key	RSVD	Randomised-singular value decomposition	Wat'_{img}	Received encrypted marked image
Enc_{img}	Encrypted cover image	IRDWT	Inverse RDWT	USV	U and V are orthogonal and S is singular matrix
Per_{img}	Confused image	Wat_{img}	Encrypted marked image	S_{emb}	Modified singular value
img1, img2	CT and MRI images	Fus'_{img}	Extracted fused mark image	$L()$	Precision limited logistic map
r_i	i^{th} iteration value of the integrated map	$S()$	Precision limited skew tent map	I_0, J_0,K_0	Initial values for $L()$ and two $S()$
NSCT	Non-subsampled contourlet transform	Cov'_{img}	Decrypted cover image	C_1, C_2	Parameters for two $S()$

embedding time of the scheme is also high. Manikandan and Amirtharajan [17] designed secret embedding of patient information into encrypted medical images. The encryption process involves the Bülban map, Le Gall 5/3 Transform, confusion, and diffusion. The proposed scheme has good security features and low computational complexity; however, the robustness of the scheme needs to be verified. Singh et al. [18] offered medical image watermarking, based on DWT-SVD. Firstly, they divide the image into regions of interest (ROI) and regions of noninterest (RONI). For secrecy and payload, the electronic patient record is first compressed and then encrypted by human coding and a secret key, respectively. Watermarked image is generated by the embedding of a recovery bit, QR code, and cipher electronic patient record into RONI. The proposed scheme achieves good robustness against various attacks. Daoui et al. [19] offered copyright protection systems based on zero-watermarking and encryption techniques for images. They introduced modified logistic maps for image encryption. The ROI of the encrypted image is selected, and the XOR with QR code generates the zero-watermark. The suggested technique has a high level of security and is resistant to typical attacks, but it also has a high level of computing complexity.

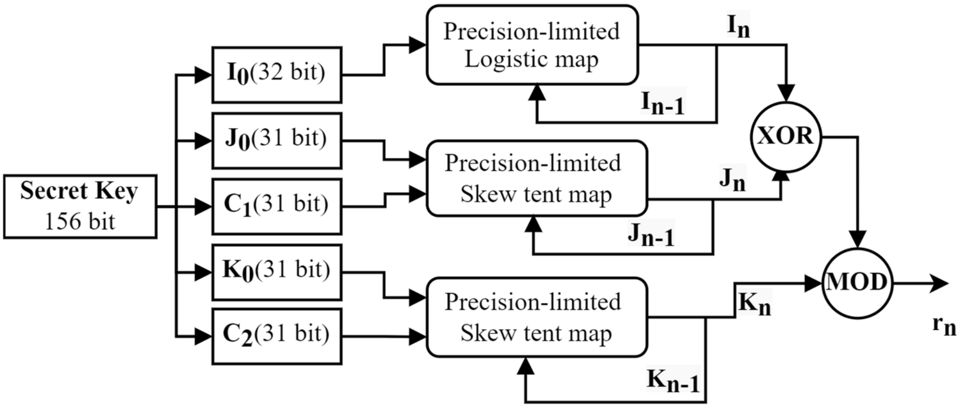
Methodology

The proposed WatMIF algorithm consists of three major parts: the encryption of host media, the fusion of multimodal medical images, and the embedding and extraction of the fused mark. The stepwise procedures for each phase are illustrated in Algorithm 1 to Algorithm 7, respectively. Some commonly used notations in these algorithms are listed in Table 1.

The Encryption of Host Media

In this section, we will introduce a number of previous studies as the basis for the encryption scheme. First, we introduce a simplified process of an encryption scheme in terms of key initialisation and generation. Second, we will describe the confusion and diffusion processes in detail. Initially, this

Fig. 1 Proposed chaotic key generation framework



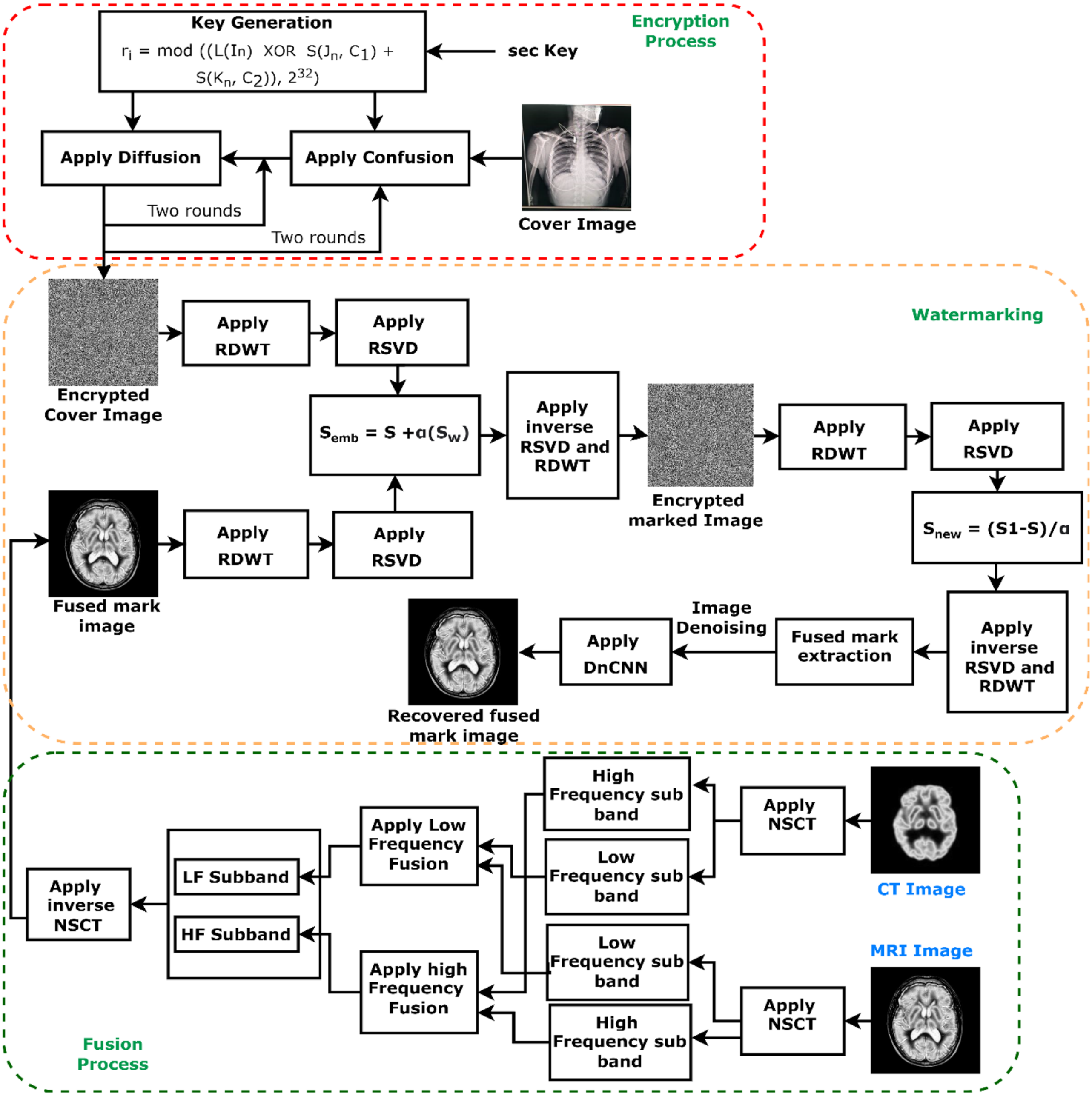


Fig. 2 The framework of proposed scheme

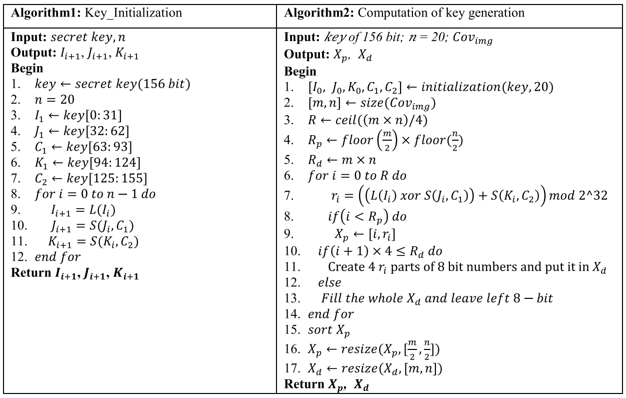
encryption scheme is proposed by Li et al. [20]. However, our key generation method is totally different from the scheme proposed in [20]. The proposed encryption technique offers improved security characteristics, such as large key space, high key sensitivity, and low computing cost. It can also withstand differential, statistical, and other common security attacks.

In the encryption stage, a precision-limited logistic map and skew tent map are combined to generate a new chaotic sequence. Two random 156-bit secret keys are used to generate the two 32-bit keys, which are used for confusion and diffusion. The simplified procedure of key generation process and proposed WatMIF algorithm is shown in Figs. 1 and 2, respectively.

Key Initialization and Generation Procedure Key initialization is a very important step for any chaotic-based encryption because they are very sensitive to initial values. We first choose a secret key of 156 bit for initialising the value of precision limited logistic map (LM) and skew tent map (STM).

This secret key is divided into five parts $I_0, J_0, C_1, K_0,$ andC_2 and used to initialize the initial values and parameters for the LM and STM. I_0 is the initial value for LM. $J_0 and C_1$ are the initial and parameter value for the first STM and $K_0 and C_2$ are the initial value and parameter value for the second STM. The encryption process is repeated twice, so two pseudo random number generators (PRNG) are initialised. The PRNG is initialised after 20 iterations. Furthermore, the key generation step involves the generation of two different sequences X_p and X_d for confusion and diffusion purpose, respectively. Each repetition of the precision-limited LM and STM yields a 32-bit sequence.

For the cover image of size $m \times n$ a random number of length $R = \lceil (m \times n)/4 \rceil$ is generated. If the size of the image is not multiple of 2 then the size of X_p is calculated as $\mathrm{Rp} = \lfloor (m/2) \times \mathrm{floor}(n/2) \rfloor$. The detailed procedure is key initialization and generation and is described in Algorithms 1 and 2, respectively.



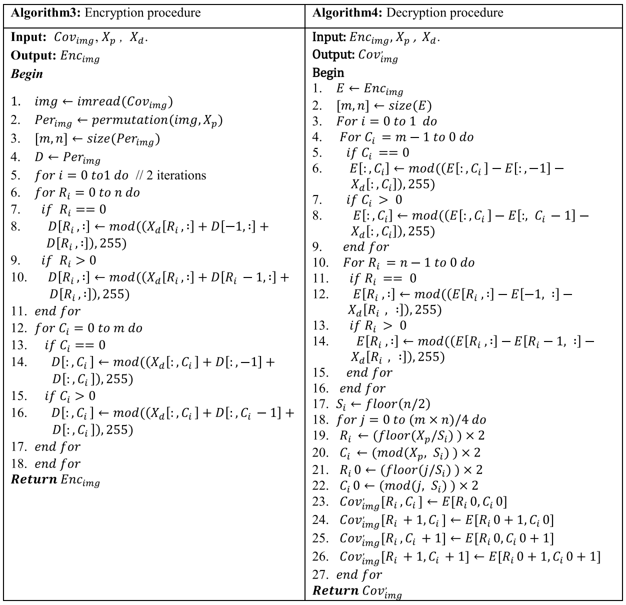
Algorithm1: Key_Initialization

```
Input: $secret\ key, n$
Output: $I_{i+1}, J_{i+1}, K_{i+1}$
Begin
    $key \leftarrow secret\ key(156\ bit)$
    $n = 20$
    $I_1 \leftarrow key[0:31]$
    $J_1 \leftarrow key[32:62]$
    $C_1 \leftarrow key[63:93]$
    $K_1 \leftarrow key[94:124]$
    $C_2 \leftarrow key[125:155]$
    $for\ i = 0\ to\ n-1\ do$
        $I_{i+1} = L(I_i)$
        $J_{i+1} = S(J_i, C_1)$
        $K_{i+1} = S(K_i, C_2)$
    $end\ for$
Return $I_{i+1}, J_{i+1}, K_{i+1}$
```

Algorithm2: Computation of key generation

```
Input: $key\ of\ 156\ bit;\ n = 20;\ Cov_{img}$
Output: $X_p,\ X_d$
Begin
    $[I_0, J_0, K_0, C_1, C_2] \leftarrow initialization(key, 20)$
    $[m, n] \leftarrow size(Cov_{img})$
    $R \leftarrow ceil((m \times n)/4)$
    $R_p \leftarrow floor\left(\frac{m}{2}\right) \times floor(\frac{n}{2})$
    $R_d \leftarrow m \times n$
    $for\ i = 0\ to\ R\ do$
            $r_i = \Big(\big(L(I_i)\ xor\ S(J_i, C_1)\big) + S(K_i, C_2)\Big)\ mod\ 2^32$
        $if\big(i < R_p\big)\ do$
            $X_p \leftarrow [i, r_i]$
        $if (i+1) \times 4 \le R_d\ do$
            Create 4 $r_i$ parts of 8 bit numbers and put it in $X_d$
        $else$
            $Fill\ the\ whole\ X_d\ and\ leave\ left\ 8 - bit$
    $end\ for$
    $sort\ X_p$
    $X_p \leftarrow resize(X_p, [\frac{m}{2}, \frac{n}{2}])$
    $X_d \leftarrow resize(X_d, [m, n])$
Return $X_p,\ X_d$
```

Confusion and Diffusion Procedure The encryption step utilised generated sequence matrix X_p and X_d to encrypt the cover image $\mathrm{Cov}_{\mathrm{img}}$. Encryption is done by 2 times permutation and diffusion processes. Permutation step is done by creating a random number matrix R by combining maps, the size of this matrix is width/2 and height/2 of the $\mathrm{Cov}_{\mathrm{img}}$ since we are taking 2×2 parts of the image to reduce some amount of time in the permutation process, then It is sorted by its value with indexes. This yields X_p matrix with only indexes of random number matrix R, and then the image is scrambled by these indexes. Each time, the $\mathrm{Cov}_{\mathrm{img}}$ is permuted by X_p, and then the permuted image $\mathrm{Per}_{\mathrm{img}}$ is diffused by X_d. Furthermore, every time,m and n rounds of row and column diffusion are performed respectively. The simplified permutation procedure is shown in Fig. 3, and the detailed confusion and diffusion processes are included in Algorithm 3. The decryption process is just the inverse of the encryption process, which utilize the X_p and X_d. First, inverse diffusion is applied on $\mathrm{Enc}_{\mathrm{img}}$ by diffusion key X_d then, inverse confusion is performed to recover the cover image $\mathrm{Cov}'_{\mathrm{img}}$. Algorithm 4 depicts the entire decryption procedure of our approach.



Algorithm3: Encryption procedure

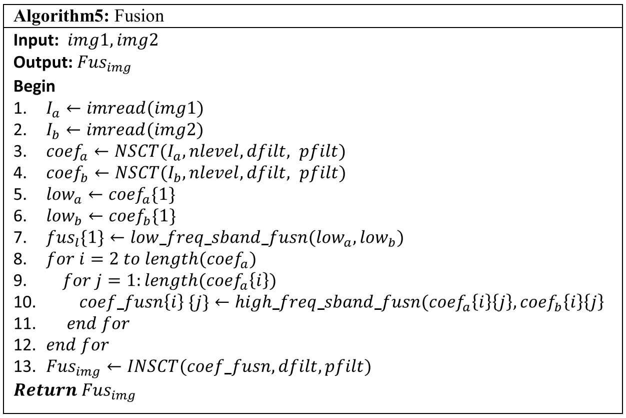
```
Input: $Cov_{img}, X_p,\ X_d.$
Output: $Enc_{img}$
Begin

    $img \leftarrow imread(Cov_{img})$
    $Per_{img} \leftarrow permutation(img, X_p)$
    $[m, n] \leftarrow size(Per_{img})$
    $D \leftarrow Per_{img}$
    $for\ i = 0\ to1\ do$  // 2 iterations
    $for\ R_i = 0\ to\ n\ do$
      $if\ \ R_i == 0$
        $D[R_i, :] \leftarrow mod((X_d[R_i, :] + D[-1, :] +$
        $D[R_i, :]), 255)$
      $if\ \ R_i > 0$
        $D[R_i, :] \leftarrow mod((X_d[R_i, :] + D[R_i - 1, :] +$
        $D[R_i, :]), 255)$
    $end\ for$
    $for\ C_i = 0\ to\ m\ do$
      $if\ C_i == 0$
        $D[:, C_i] \leftarrow mod((X_d[:, C_i] + D[:, -1] +$
        $D[:, C_i]), 255)$
      $if\ C_i > 0$
        $D[:, C_i] \leftarrow mod((X_d[:, C_i] + D[:, C_i - 1] +$
        $D[:, C_i]), 255)$
    $end\ for$
    $end\ for$
Return $Enc_{img}$
```

Algorithm4: Decryption procedure

```
Input: $Enc_{img}, X_p,\ X_d.$
Output: $Cov'_{img}$
Begin
    $E \leftarrow Enc_{img}$
    $[m, n] \leftarrow size(E)$
    $For\ i = 0\ to\ 1\ \ do$
     $For\ C_i\ = m - 1\ to\ 0\ do$
       $if\ C_i\ == 0$
        $E[:, C_i] \leftarrow mod((E[:, C_i] - E[:, -1] -$
        $X_d[:, C_i]), 255)$
       $if\ C_i\ >\ 0$
        $E[:, C_i] \leftarrow mod((E[:, C_i] - E[:,\ C_i - 1] -$
        $X_d[:, C_i]), 255)$
      $end\ for$
      $For\ R_i\ = n - 1\ to\ 0\ do$
       $if\ R_i\ ==\ 0$
        $E[R_i, :] \leftarrow mod((E[R_i, :] - E[-1,\ :] -$
        $X_d[R_i\ ,\ :]), 255)$
       $if\ R_i\ >\ 0$
        $E[R_i, :] \leftarrow mod((E[R_i, :] - E[R_i - 1,\ :] -$
        $X_d[R_i\ ,\ :]), 255)$
      $end\ for$
     $end\ for$
    $S_i \leftarrow floor(n/2)$
    $for\ j = 0\ to\ (m \times n)/4\ do$
     $R_i\ \leftarrow (floor(X_p/S_i)\ ) \times 2$
     $C_i\ \leftarrow (mod(X_p,\ S_i)\ ) \times 2$
     $R_i 0 \leftarrow (floor(j/S_i)\ ) \times 2$
     $C_i 0 \leftarrow (mod(j,\ S_i)\ ) \times 2$
     $Cov'_{img}[R_i, C_i] \leftarrow E[R_i 0, C_i 0]$
     $Cov'_{img}[R_i + 1, C_i] \leftarrow E[R_i 0 + 1, C_i 0]$
     $Cov'_{img}[R_i, C_i + 1] \leftarrow E[R_i 0, C_i 0 + 1]$
     $Cov'_{img}[R_i + 1, C_i + 1] \leftarrow E[R_i 0 + 1, C_i 0 + 1]$
    $end\ for$
Return $Cov'_{img}$
```

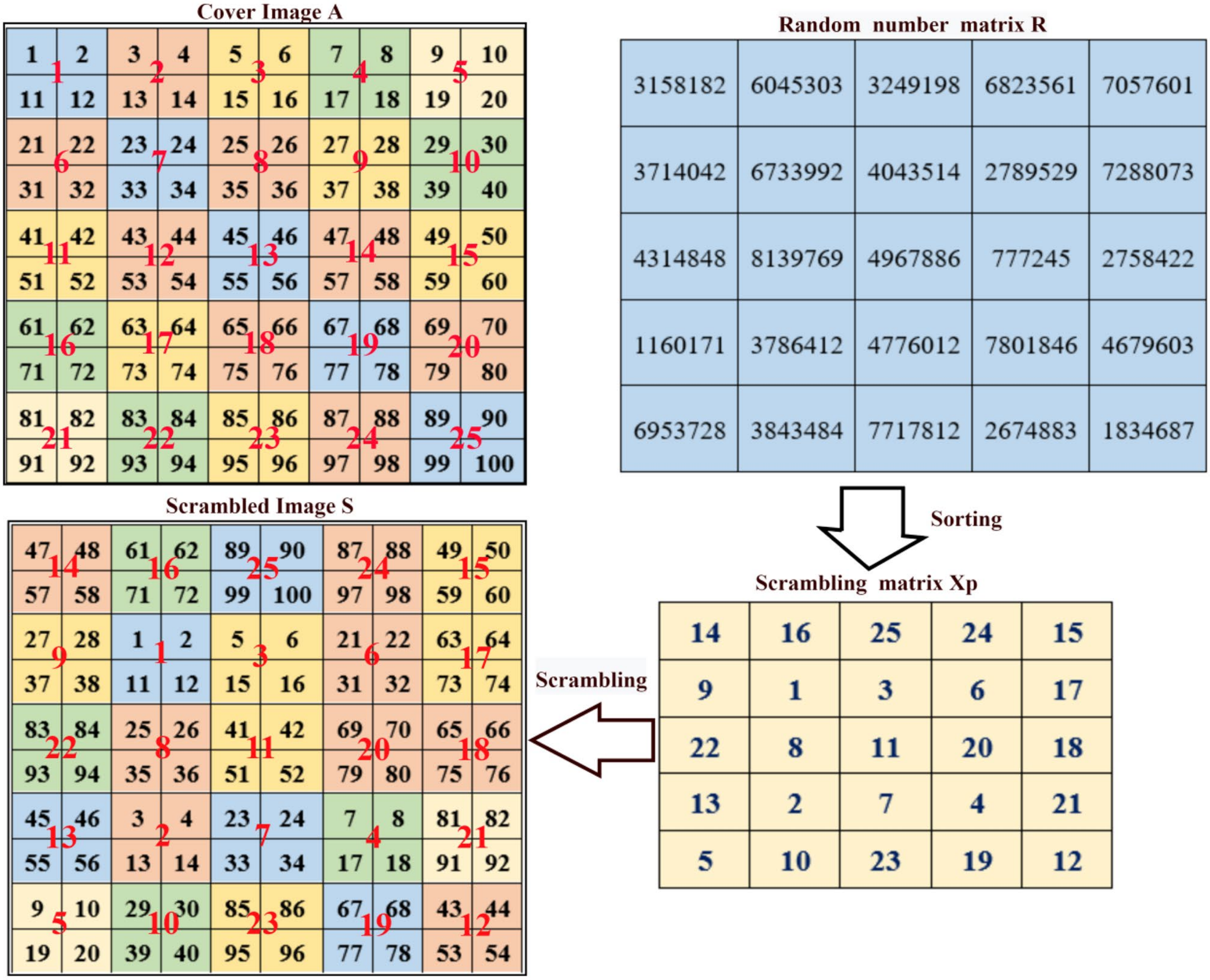
Fusion of Multi-Modal Medical Images

In this section, an NSCT-based fusion approach is performed on multi-modal images, such as CT and MRI images, to obtain a fused mark image, $\mathrm{Fus}_{\mathrm{img}}$. First, NSCT is utilised to transform the CT and MRI images into different resolutions and directions. After that, low- and high-frequency rules are applied to fuse the NSCT coefficients of CT and MRI images, respectively. Lastly, inverse NSCT is performed to generate the fused image. The fused image is used as a watermark. The simplified procedure of multimodal image fusion is described in Algorithm 5.



Algorithm5: Fusion

```
Input: $img1, img2$
Output: $Fus_{img}$
Begin
    $I_a \leftarrow imread(img1)$
    $I_b \leftarrow imread(img2)$
    $coef_a \leftarrow NSCT(I_a, nlevel, dfilt,\ pfilt)$
    $coef_b \leftarrow NSCT(I_b, nlevel, dfilt,\ pfilt)$
    $low_a \leftarrow coef_a\{1\}$
    $low_b \leftarrow coef_b\{1\}$
    $fus_i\{1\} \leftarrow low\_freq\_sband\_fusn(low_a, low_b)$
    $for\ i = 2\ to\ length(coef_a)$
      $for\ j = 1{:}\ length(coef_a\{i\})$
        $coef\_fusn\{i\}\ \{j\} \leftarrow high\_freq\_sband\_fusn(coef_a\{i\}\{j\}, coef_b\{i\}\{j\}$
      $end\ for$
    $end\ for$
    $Fus_{img} \leftarrow INSCT(coef\_fusn, dfilt, pfilt)$
Return $Fus_{img}$
```



Cover Image A

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Random number matrix R

3158182	6045303	3249198	6823561	7057601
3714042	6733992	4043514	2789529	7288073
4314848	8139769	4967886	777245	2758422
1160171	3786412	4776012	7801846	4679603
6953728	3843484	7717812	2674883	1834687

Scrambling matrix Xp

14	16	25	24	15
9	1	3	6	17
22	8	11	20	18
13	2	7	4	21
5	10	23	19	12

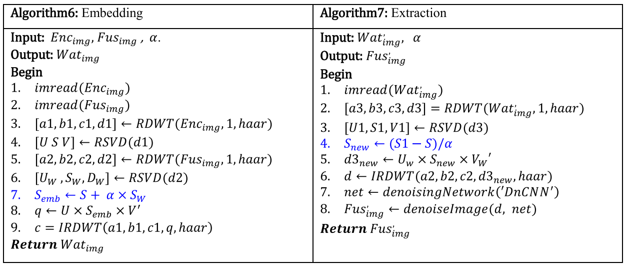
Scrambled Image S

47	48	61	62	89	90	87	88	49	50
57	58	71	72	99	100	97	98	59	60
27	28	1	2	5	6	21	22	63	64
37	38	11	12	15	16	31	32	73	74
83	84	25	26	41	42	69	70	65	66
93	94	35	36	51	52	79	80	75	76
45	46	3	4	23	24	7	8	81	82
55	56	13	14	33	34	17	18	91	92
9	10	29	30	85	86	67	68	43	44
19	20	39	40	95	96	77	78	53	54

Fig. 3 Permutation procedure of plain image

Embedding and Extraction Procedure of Fused Mark

In this section, Enc_{img} and Fus_{img} are transformed using RDWT and RSVD for embedding. Furthermore, the embedding operation is performed by altering the singular value of Fus_{img} with the help of the embedding factor, 'α'. Lastly, the inverse operation of RSVD and RDWT is employed to obtain the encrypted marked image, Wat_{img}. The detailed embedding procedure is explained in Algorithm 6. In addition, to recover fused mark image Fus'_{img} from received encrypted marked image Wat'_{img}, RDWT is utilised to obtain the $a3$, $b3$, $c3$, and $d3$ coefficients of Wat'_{img}. RSVD is employed at the low-frequency coefficient $d3$. Then, singular value S_{new} extraction is applied. Finally, inverse RSVD and RDWT are applied to recover the fused mark image. In addition, DnCNN is used to improve the robustness and degradation of Fus'_{img}. Algorithm 7 represents the detailed decryption process.



```
Algorithm6: Embedding
Input: $Enc_{img}, Fus_{img}$ , $\alpha$.
Output: $Wat_{img}$
Begin
    $imread(Enc_{img})$
    $imread(Fus_{img})$
    $[a1, b1, c1, d1] \leftarrow RDWT(Enc_{img}, 1, haar)$
    $[U\ S\ V] \leftarrow RSVD(d1)$
    $[a2, b2, c2, d2] \leftarrow RDWT(Fus_{img}, 1, haar)$
    $[U_W\ , S_W, D_W] \leftarrow RSVD(d2)$
    $S_{emb} \leftarrow S +\ \alpha \times S_W$
    $q \leftarrow U \times S_{emb} \times V'$
    $c = IRDWT(a1, b1, c1, q, haar)$
Return $Wat_{img}$
```

```
Algorithm7: Extraction
Input: $Wat'_{img}$,  $\alpha$
Output: $Fus'_{img}$
Begin
    $imread(Wat'_{img})$
    $[a3, b3, c3, d3] = RDWT(Wat'_{img}, 1, haar)$
    $[U1, S1, V1] \leftarrow RSVD(d3)$
    $S_{new} \leftarrow (S1 - S)/\alpha$
    $d3_{new} \leftarrow U_w \times S_{new} \times V_W{}'$
    $d \leftarrow IRDWT(a2, b2, c2, d3_{new}, haar)$
    $net \leftarrow denoisingNetwork('DnCNN')$
    $Fus'_{img} \leftarrow denoiseImage(d,\ net)$
Return $Fus'_{img}$
```

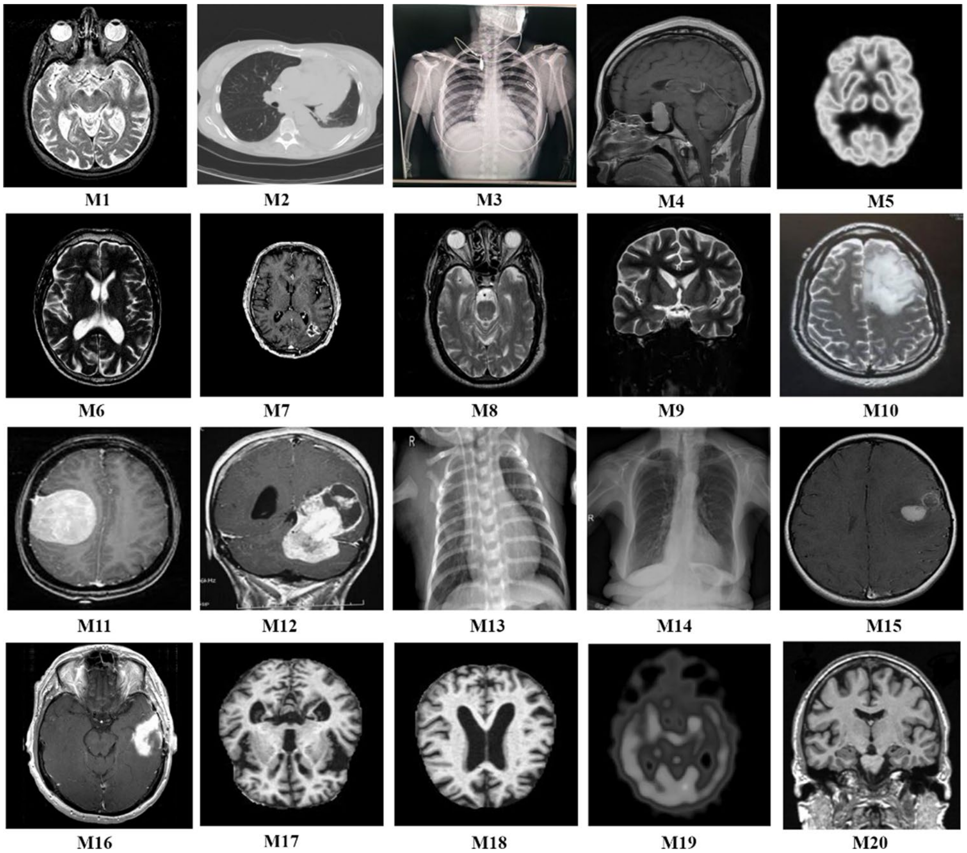


Fig. 4 Sample images used in the experiment

Experiments

In order to confirm the efficiency and resilience against many forms of attacks, we performed different experimental measures. All the experiments were done on MATLAB R2019a with an 8 GB RAM and a 64-bit core i5 processor. We have used different medical images of size 256 × 256 and 512 × 512 from different databases [21, 22]. Figure 4 represented the some of the sample images.

Encryption converts the image information into a meaningless form. From the encrypted image, the attacker cannot infer anything about the plain image. In order to demonstrate the visual perception security of the proposed encryption scheme, different medical images were encrypted and decrypted; the result is shown in Fig. 5. Additionally, to prove the robustness and security of the scheme, various analyses, like statistical, differential, key space, key sensitivity, noise attack, and visual quality, were performed in this section.

Statistical Analysis

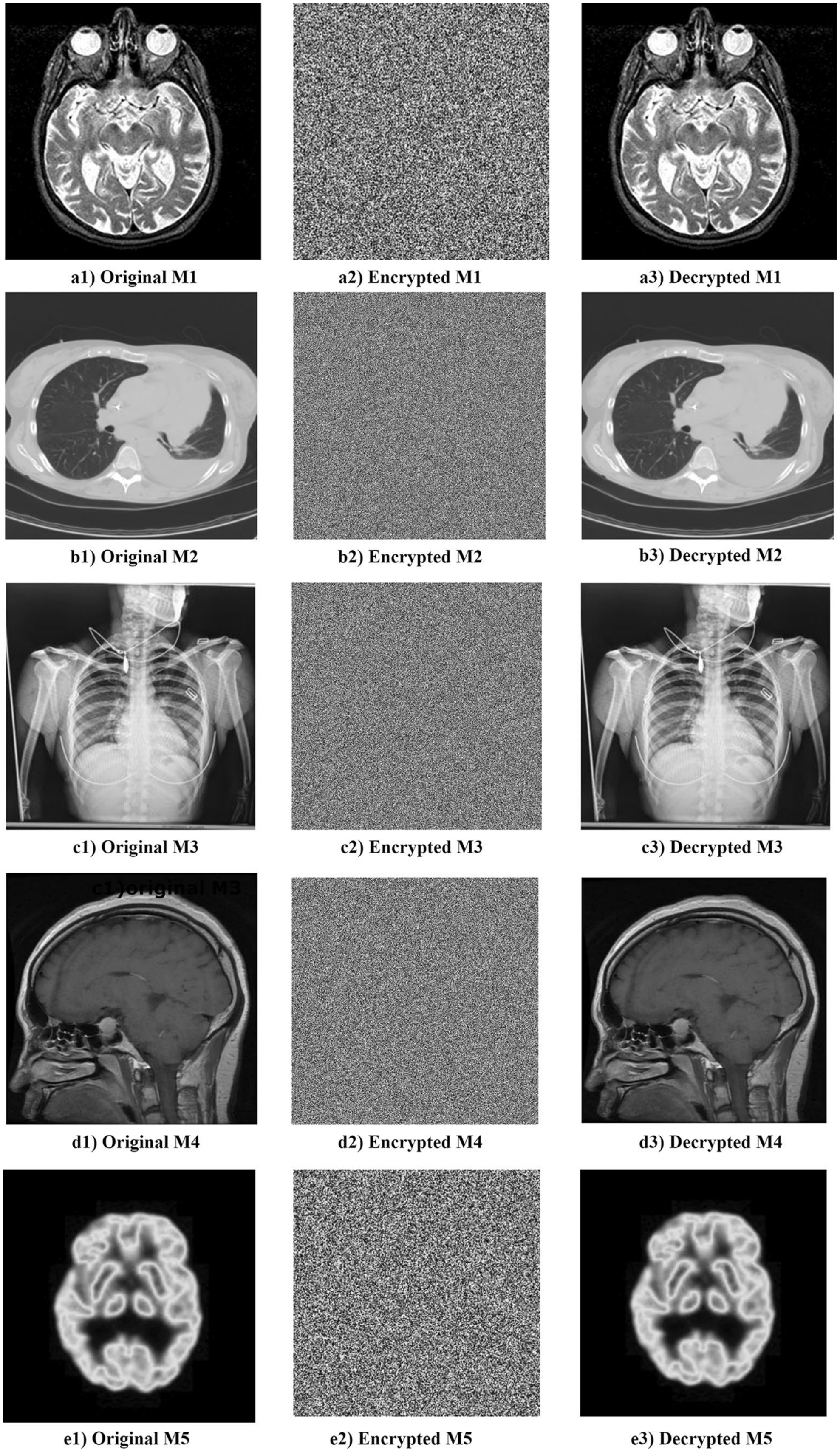
Statistical analysis determines the degree to which the pixels in an image are related. In a plain image, pixels are closely related, but in an encrypted image, there should be no relation [23]. We performed a histogram, correlation coefficient, and entropy analysis to measure the strength of our proposed scheme against statistical attacks.

Histogram Analysis

The histogram of an image represents the number of pixels of each grey level. Ideally, the histogram of the cipher image should be uniform for any encryption technique. The result of the histogram analysis of our encryption scheme is shown in Fig. 6. It is clear that all encrypted images have a uniform histogram and are completely different from the histogram of the corresponding plain images. Hence, the proposed scheme is highly secure against statistical attacks.

Correlation Analysis

The correlation among the adjacent pixels is used to measure the strength of an encryption scheme against statistical attacks [6]. Generally, an encrypted image's pixels are highly uncorrelated. To measure the correlation, correlation-coefficient is calculated in horizontal, vertical, and diagonal directions as



a1) Original M1
a2) Encrypted M1
a3) Decrypted M1

b1) Original M2
b2) Encrypted M2
b3) Decrypted M2

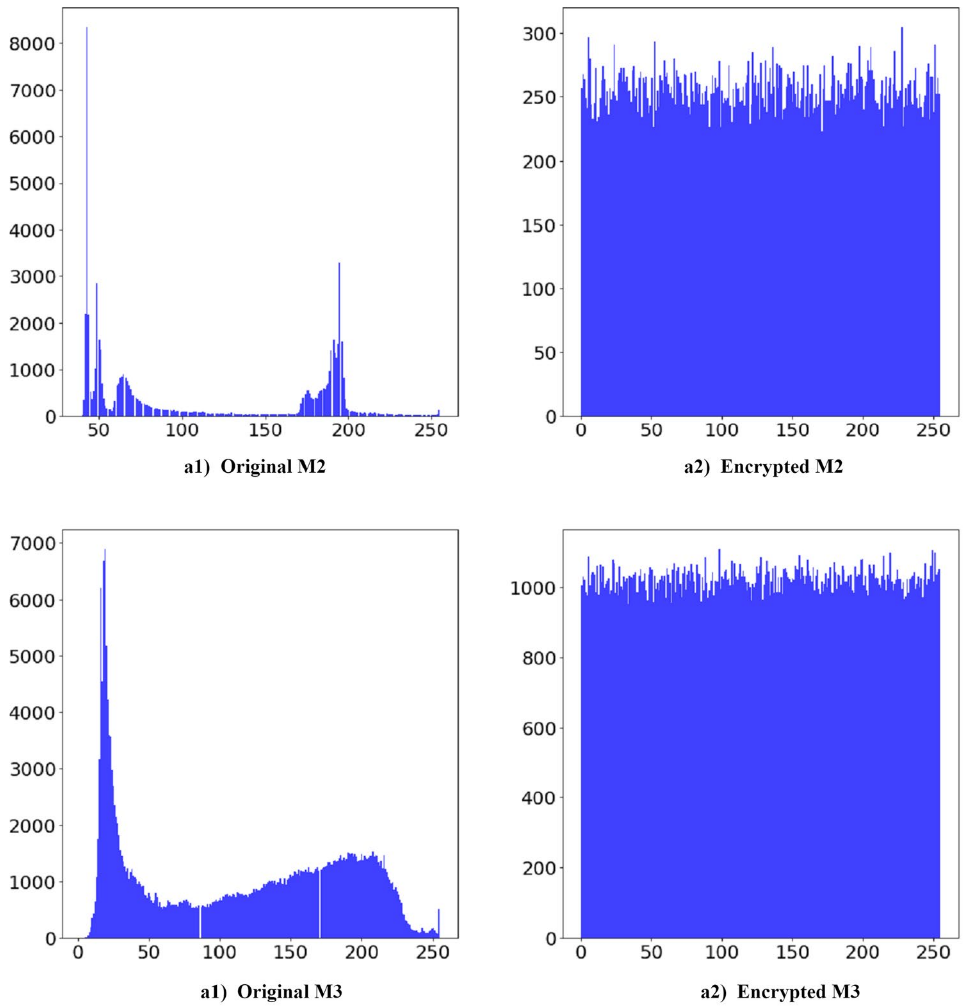
c1) Original M3
c2) Encrypted M3
c3) Decrypted M3

d1) Original M4
d2) Encrypted M4
d3) Decrypted M4

e1) Original M5
e2) Encrypted M5
e3) Decrypted M5

Fig. 5 Original images (**a1**, **b1**, **c1**, **d1**, and **e1**) and their corresponding encrypted (**a2**, **b2**, **c2**, **d2**, and **e2**) and decrypted image (**a3**, **b3**, **c3**, **d3**, and **e3**)

Fig. 6 Histogram evaluation



a1) Original M2

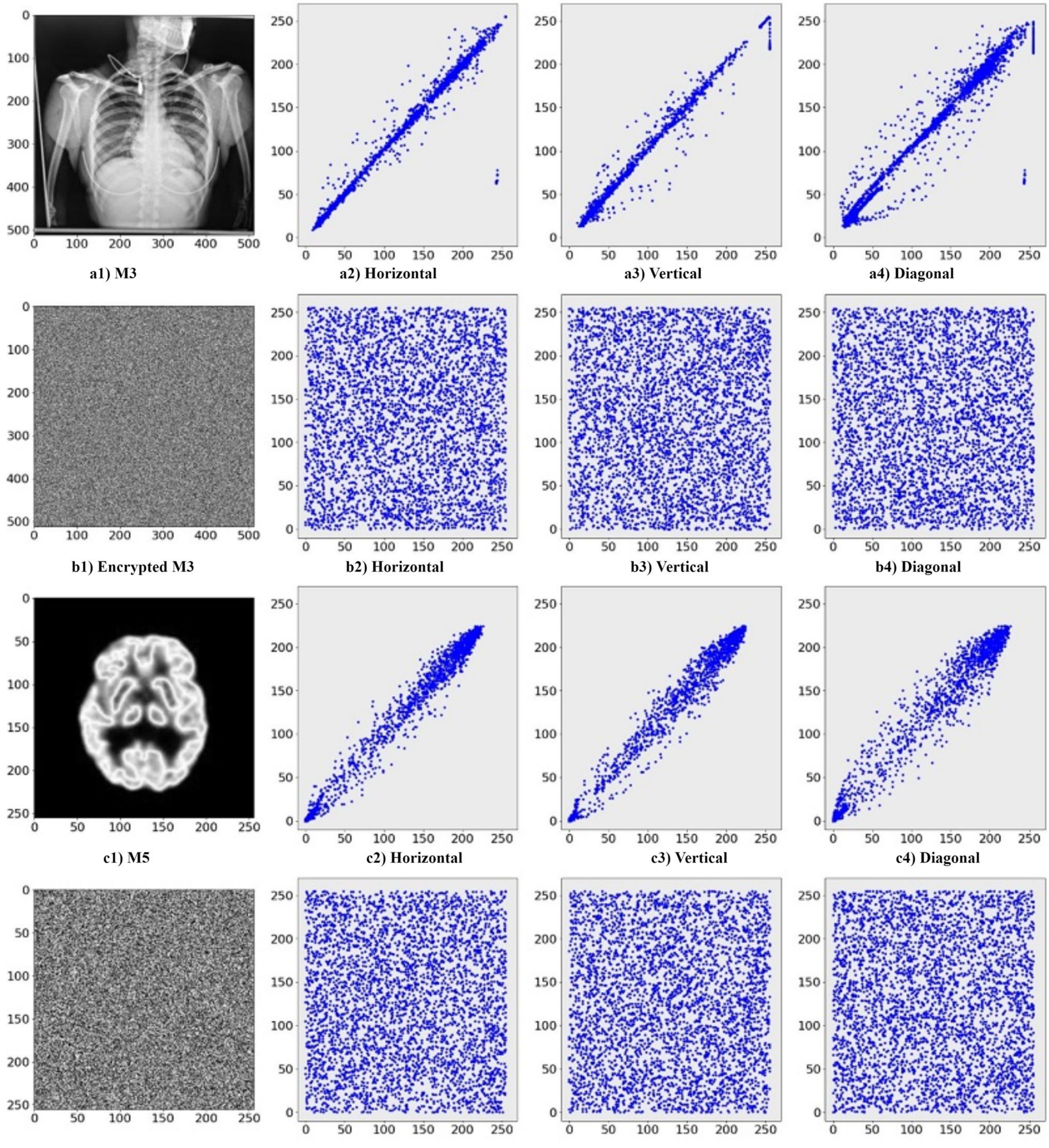
a2) Encrypted M2

a1) Original M3

a2) Encrypted M3

Table 2 Correlation analysis

Method	Image	Plain image			Encrypted image		
		H	V	D	H	V	D
Proposed method	M1	0.9576	0.9577	0.9356	0.0138	−0.0087	−0.0260
	M2	0.9941	0.9776	0.9719	0.0233	−0.0018	−0.0048
	M3	0.9671	0.9783	0.9487	0.0163	0.0068	0.0115
	M4	0.9954	0.9953	0.9826	0.0082	−0.0110	−0.0247
	M5	0.9931	0.9948	0.9882	0.0047	0.0059	0.0189
	M6	0.9093	0.9206	0.8627	−0.0092	0.0470	0.0034
[24]	Chest	0.9936	0.9924	0.9878	−0.0017	−0.0008	0.0133
[25]	46,529,543,479,051,320.dcm	NA	NA	NA	0.0339	−0.0143	−0.0197
[26]	OPENi3	0.9670	0.9715	0.9408	−0.0017	−0.0013	0.0013



a1) M3 a2) Horizontal a3) Vertical a4) Diagonal

b1) Encrypted M3 b2) Horizontal b3) Vertical b4) Diagonal

c1) M5 c2) Horizontal c3) Vertical c4) Diagonal

d1) Encrypted M5 d2) Horizontal d3) Vertical d4) Diagonal

Fig. 7 Correlation coefficient analysis in horizontal, vertical, and diagonal direction of original and encrypted image

Table 3 Entropy analysis

Method	Size of image	Tested image	Entropy	
			Plain	Encrypted
Our encryption scheme	256×256	M1	3.7148	7.9972
	256×256	M2	6.1936	7.9976
	256×256	M5	4.1097	7.9969
	256×256	M6	4.4212	7.9973
	512×512	M3	7.5920	7.9993
	512×512	M4	6.7832	7.9993
Average (50 images of COVID-19 dataset[22])			7.3978	**7.9980**
[24]	256×256	Chest	6.5336	7.9981
[26]	256×256	OPENi3	NA	7.9976
[27]	256×256	Fingerprint	NA	7.9899

$$P_{l,m} = \frac{Q[(l - Q(l))(m - Q(m))]}{\sqrt{R(l)R(m)}} \tag{1}$$

$$Q(l) = \frac{1}{n}\sum_{i=1}^{n} l_i \tag{2}$$

$$R(l) = \frac{1}{n}\sum_{i=1}^{n} (l_i - Q(l))^2 \tag{3}$$

where correlation is calculated between pixel l and m, and n indicates the number of pixel pairs (l, m). The correlation-coefficient value should be near zero, which indicates no correlation. To perform the correlation analysis, we randomly chose 3000 adjacent pixel pairs. Experimental results in Table 2 show that, for the encrypted image, all the values of the correlation-coefficient in all three directions are very close to zero, which means no correlation exists among the pixels of the encrypted image. Furthermore, the correlation performance of the proposed method is compared with that of recent schemes [24–26], indicating the effectiveness of our scheme. Figure 7 represents the correlation coefficients of plain and encrypted images.

Entropy Analysis

The measure of unpredictability in an image is represented by information entropy. A high entropy value shows high unpredictability in image data. Optimal value for grey scale encrypted image is eight [28]. Entropy is presented as

$$H(I) = -\sum_{n=1}^{255}(P(I_n) \times \log_2 P(I_n)) \tag{4}$$

where $P(I_n)$ represent the probability of pixel I_n. The entropy analysis of the proposed encryption scheme is included in Table 3. We found that the entropy of all encrypted images is very close to the optimal value. The maximum, minimum, and average entropy of the proposed scheme are 7.9993, 7.9969, and 7.9979, respectively. We also calculated the average entropy value of 50 images of a COVID-19 data set [22], which was 7.9980. Furthermore, we compare the entropy score with recent state-of-the art [24, 26, 27] which proves that our scheme provides a high level of randomness in encrypted images.

Differential Analysis

Attackers frequently try to identify any meaningful association between the original and the encrypted images by modifying the value of one bit of the original image at a time and encrypting it with the set of keys and methods. If two cypher images have the same pixel values, the information about the plain image is likely to be exposed. Therefore, it is essential that a minor modification, even in a single bit in the plain image, causes the encrypted image to totally change in order to resist differential attacks. NPCR and UACI are two parameters that are used to assess the strength of an encryption scheme against differential attacks [29]. The ideal values for NPCR and UACI for an effective encryption technique are 0.996034 and 0.3346, respectively. NPCR and UACI are calculated as

$$\text{NPCR} = \frac{1}{R \times C}\sum_{p,q} T(p,q) \tag{5}$$

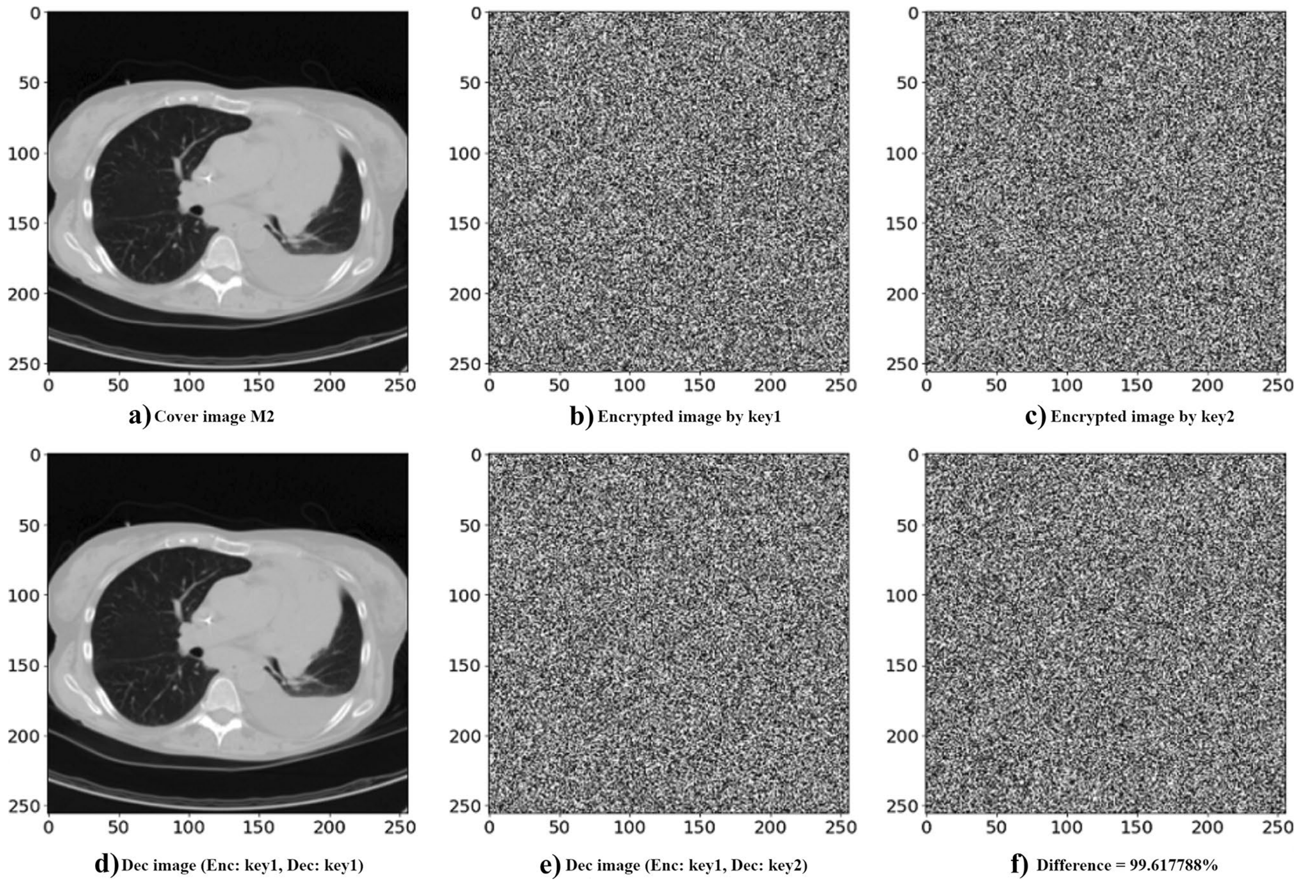
$$\text{UACI} = \frac{1}{R \times C}\sum_{p,q} \frac{|C(p,q) - C'(p,q)|}{255} \tag{6}$$

$$T(p,q) = \begin{cases} 0, if C(p,q) = C'(p,q) \\ 1, if C(p,q) \neq C'(p,q) \end{cases} \tag{7}$$

where, $C(p,q)$ is the encrypted image corresponding to the plain image and the encrypted image is $C'(p, q)$ after 1-bit

Table 4 The NPCR and UACI values of different medical images

Method	Size of image	Tested image	NPCR	UACI
Our encryption scheme	256×256	M1	0.9958	0.3350
	256×256	M2	0.9961	0.3355
	256×256	M5	0.9961	0.3346
	256×256	M6	0.9960	0.3341
	512×512	M3	0.9961	0.3344
	512×512	M4	0.9960	0.3345
Average (50 images of COVID-19 dataset [22])			0.9960	0.3346
[24]	256×256	Chest	0.9961	0.3346
[26]	256×256	OPENi3	0.9955	0.3336
[27]	256×256	Fingerprint	0.9960	0.3355



a) Cover image M2

b) Encrypted image by key1

c) Encrypted image by key2

d) Dec image (Enc: key1, Dec: key1)

e) Dec image (Enc: key1, Dec: key2)

f) Difference = 99.617788%

Fig. 8 Key sensitivity analysis

modification to a plain image. Differential analysis in terms of NPCR and UACI of our encryption scheme are depicted in Table 4. We get the maximum, the minimum, and the average NPCR as 0.9961 and 0.9958, respectively. Furthermore, another 50 images were selected from a COVID-19 dataset [22], and the average NPCR and UACI were computed with values of 0.9960 and 0.3346, respectively.

Table 5 Time cost evaluation

Scheme	Tested image	Size	Computation time (sec)	
			Encryption	Decryption
Our encryption scheme	M1	256×256	0.2692	0.2293
	M2	256×256	0.2391	0.2393
	M5	256×256	0.2054	0.2214
	M6	256×256	0.2445	0.2304
	M3	512×512	0.8906	0.9335
	M4	512×512	0.9155	0.9205
[24]	Chest	256×256	0.2415	0.2288
[26]	OPENi1	256×256	3.9	-
[27]	Fingerprint	256×256	0.459837	0.212294

The results show that all the values of NPCR and UACI are very close to idle values, and the average values of NPCR/UACI are equal to the optimal one. In addition, we also compared the result with recent schemes [24, 26, 27] and found it to be better than those. Therefore, the proposed scheme is suitable to handle differential attacks efficiently.

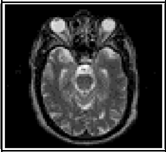
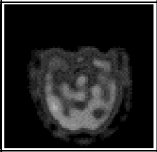
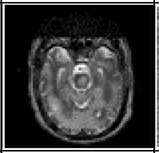
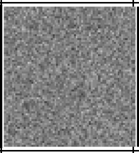
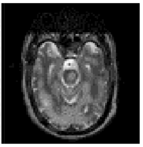
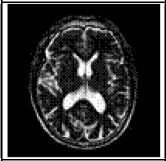
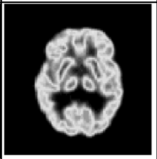
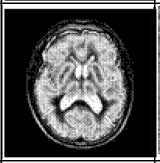
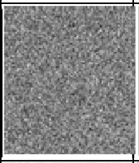
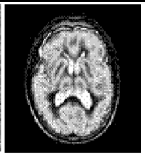
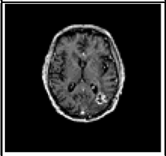
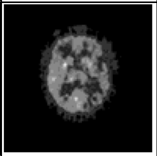
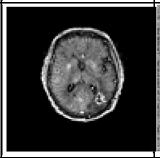
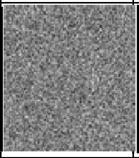
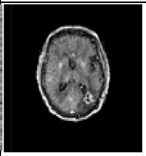
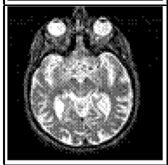
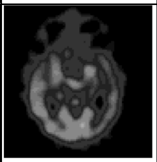
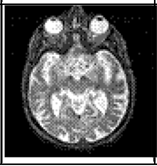
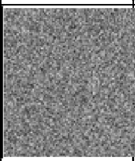
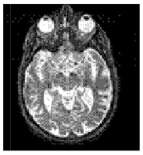
Key Sensitivity Analysis

A strong encryption scheme must be sensitive to its key, which means that a slight change in the encryption key cannot decrypt the encrypted image. To examine the key sensitivity, we encrypted the cover image with the correct key

Table 6 Analysis of proposed scheme on various embedding strength

Embedding Strength	PSNR	SSIM	NC
0.001	49.1845	1.0000	0.9999
0.005	35.2051	1.0000	0.9999
0.01	29.1845	1.0000	0.9999
0.02	23.1639	1.0000	0.9999
0.03	19.6421	1.0000	0.9999

Table 7 Evolution of fussed mark image with respect to same encrypted cover image

Image 1	Image 2	Fused mark image	Encrypted marked image	Recovered fussed image	PSNR	SSIM	NC	Computation time (sec)	
								Embedding time	Extraction time
					33.8763	1.0000	0.9999	0.1846	0.3914
					27.0689	1.0000	0.9999	0.1804	0.3796
					27.2464	1.0000	0.9997	0.1871	0.4016
					28.7768	1.0000	0.9999	0.1774	0.3809

(key1) and, with a one-bit, changed the key (key2). Key1 decrypts the cypher image correctly while decrypting with key2 cannot recover the plain image. Figure 8 shows the result of the key sensitivity analysis. Furthermore, we calculated the difference between the decrypted image with key1 and with key2, which was 99.6177%. We can observe that both the decrypted images are totally different. Therefore, our scheme is very sensitive to its encryption key.

Key Space

To withstand any brute force assaults, the key space of the encryption technique must be greater than or equal to 2^{100} [30]. In the proposed scheme, two chaotic maps, the precision-limited logistic map and the STM were utilised. This requires two different 156-bit random secret keys. Therefore, the key space of our suggested encryption approach is 2^{312}, which is much higher than 2^{100}. Hence, this scheme provides better resistance against brute force assaults.

Time Evaluation

The computational cost is the main feature of any encryption scheme for real-time implementation. Therefore, we have computed the encryption and decryption time of different medical images of sizes 256 × 256 and 512 × 512, which are tabulated in Table 5. Computation time is also compared with recent schemes [24, 26, 27]. Time computation analysis shows that our scheme takes much less time to encrypt and decrypt the images.

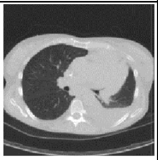
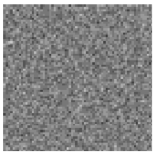
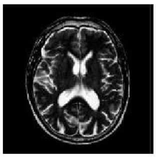
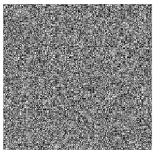
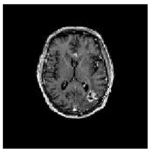
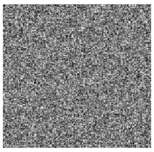
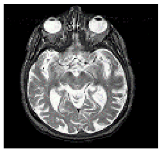
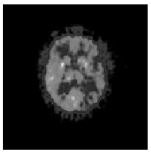
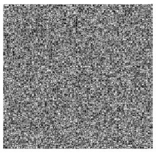
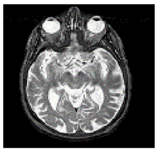
Visual Perception and Robustness Analysis

The normalised coefficient (NC) is used to estimate the robustness of the proposed approach when it is subjected to assaults. The value of NC ranges from 0 to 1, and $NC > 0.7$ is desirable [31]. The PSNR and SSIM are used to measure the visual quality of an image [32]. Table 6 shows how the proposed approach performs with different embedding strengths (α).

'α' ranges from 0.001 to 1. We found that, when $\alpha = 0.001$, the highest value of PSNR is 49.1845. When we increase the value of 'α,' the PSNR performance gradually decreases; however, the SSIM value is ideal to 1 in all cases. Furthermore, the best value of NC is 0.9999 for all the cases.

Table 7 demonstrates the analysis of different fused images in respect to the same cover image. This indicates that, at $\alpha = 0.01$, the highest and lowest PSNR between the encrypted cover image and the encrypted marked image are 33.8764 and 27.0869, respectively, whereas the SSIM value is 1 in all cases. This evaluation proves that perceptual quality is high, even when embedding the mark image.

Table 8 Evolution of fussed image with respect to different encrypted cover image

Cover image	Encrypted cover image	Fussed image	Recovered fused mark image	PSNR	SSIM	NC	Computation time (sec)	
							Embedding time	Extraction time
				28.7966	1.0000	0.9999	0.1682	0.3554
				28.7570	1.0000	0.9999	0.1677	0.3603
				28.7821	1.0000	0.9999	0.1687	0.3563
				28.7354	1.0000	0.9999	0.1747	0.3698
Average value of 100 different cover images form covid19 dataset [22]				29.2699	1.0000	0.9998	0.1708	0.3399

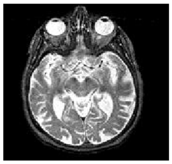
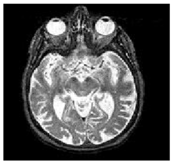
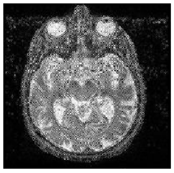
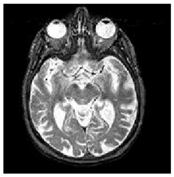
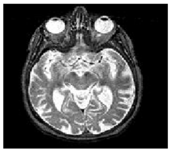
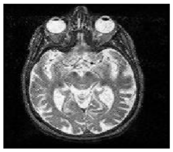
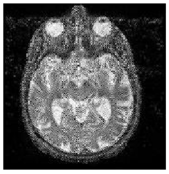
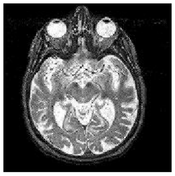
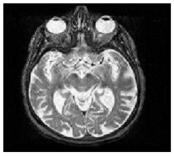
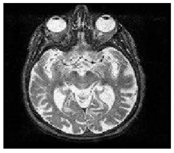
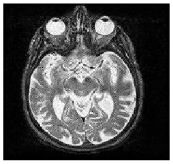
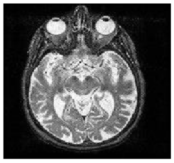
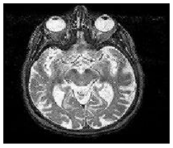
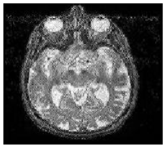
Most importantly, the average NC value between the fused mark image and the recovered fused mark image is 0.9998, and the highest NC value is 0.9999. We also calculated the embedding and extraction time of the fused mark image. The best embedding time and extraction time are 0.1774 and 0.3796 s, respectively, and the average embedding time and extraction time are 0.1823 and 0.3883 s, respectively. The results indicate that the robustness of our scheme is very high against attacks, and it requires much less time to embed and extract the fused mark image.

Furthermore, the analysis of the same fused image with respect to the different cover images is included in Table 8. Here, we get the best PSNR of 28.7966 db, and the SSIM is 1 every time. The best NC value obtained was 0.9999, and the best embedding and extraction times were 0.1677 and 0.3554 s, respectively. In addition to this, we also calculated the average value of PSNR, SSIM, NC, embedding time, and extraction time of 100 different cover images are 29.2699 dB, 1, 0.9998, 0.1708, and 0.3399 s, respectively.

Noise Attack Analysis

The robustness of the proposed scheme against different noise attacks is evaluated, and the result is presented in Table 9. For a salt and pepper attack, if the noise intensity increases from 0.001 to 0.005, the NC value decreases by zero, and if the noise intensity increases from 0.001 to 0.01, the drop in NC value is 0.0006. It is observed that if the intensity of a speckle attack increases (from 0.005 to 0.01), then the NC value decreases slightly (0.008). A similar decrement is also observed for Gaussian noise. However, more degradation is observed for average and median noise attacks. Therefore, the propounded scheme is very robust to various noise attacks.

Table 9 Evaluation of robustness for different noise attack

Attack	Parameter	Recovered fused mark image	NC	Attack	Parameter	Recovered fused mark image	NC
Average	[1 1]		0.9999	Salt & peper	0.001		0.9999
	[2 2]		0.6711		0.005		0.9999
Median	[1 1]		0.9999		0.01		0.9993
	[2 2]		0.7152		0.05		0.9752
Speckle	0.005		0.9998	Gaussian	[0, 0.001]		0.9999
	0.01		0.9990		[0, 0.002]		0.9996
	0.05		0.9711		[0, 0.05]		0.8353

To analyse the effectiveness of our scheme, we compare the result of our scheme with some recent schemes in Table 10 [12, 33, 34]. It can be seen that the NC value of our scheme is better when, Gaussian, and Gaussian low-pass filter with noise strengths of, 0.001 and 0.04, respectively, Furthermore, the proposed scheme performs best for salt and pepper as well as speckle noise. Our suggested technique improves the NC score by 20.14%, and 11.85% when compared to the scheme in [12], and [34] respectively. For all other noise, our scheme provides similar robustness. Hence, our scheme proved improved robustness for several noise attacks.

Table 10 Robustness comparison

Attack	Density	NC score			
		WatMIF	[12]	[33]	[34]
Salt and pepper	0.0001	0.9999	0.9934	0.9987	0.9942
	0.001	0.9999	0.9921	-	0.9712
	0.01	0.9993	0.9908	-	0.8934
Gaussian	[0, 0.001]	0.9999	-	0.9903	-
	[0, 0.05]	0.8353	0.9896	-	-
Speckle	0.001	0.9999	0.9936	-	0.9927
	0.05	0.9711	0.8083	-	-
Histogram equalization		0.8609	0.9125	0.9984	0.8491
Gaussian low-pass filter	Variance 0.04	0.9999	0.9902	-	-
Rotation	1′	0.8284	0.9829	-	0.9023
	45′	0.7842	0.8799	-	0.9209

Conclusion

This paper proposes a multimodal medical image fusion-based watermarking, named WatMIF. The proposed algorithm consists of three major parts: the encryption of cover media, the fusion of multi-modal medical images, and the embedding and extraction of the fused mark. Firstly, we encrypted the host media with a key-based encryption scheme. The encryption scheme is fast without compromising the security of medical images, which is suitable for telehealth scenarios. Secondly, an NSCT-based fusion scheme is employed to fuse the MRI and CT scan images to generate the fused mark image. Finally, the fused watermark is concealed in the encrypted host media using RDWT and RSVD. From the simulation, it is inferred that the WatMIF algorithm exhibits improved robustness compared to existing schemes. The proposed work can be improved with efficient deep learning models in the future.

Acknowledgements This work is supported by research project order no. DLRL/21CR0003/SWCC&ENT/GN/LP dt. 29 August, 2020, DLRL, Hyderabad, India.

Declarations

Ethics Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Consent to Participate Consent was obtained from all individual participants included in the study.

Conflict of Interest The authors declare no competing interests.

References

1. Masood F, Driss M, Boulila W, Ahmad J, Rehman SU, Jan SU, Qayyum A, Buchanan WJ. A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wirel Pers Commun. 2021 pp.1–28.
2. Fan B, Li Z, Gao J. DwiMark: a multiscale robust deep watermarking framework for diffusion-weighted imaging images. Multimedia Syst. 2022;28:295–310.
3. Anand A, Singh AK. Hybrid nature-inspired optimization and encryption-based watermarking for e-healthcare. IEEE Transactions on Computational Social Systems. 2022.
4. Wang B, Shi J, Wang W, Zhao P. Image copyright protection based on blockchain and zero-watermark. IEEE Transactions on Network Science and Engineering. 2022.
5. Kaur M, Singh D, Kumar V. Improved seven-dimensional (i7D) hyperchaotic map-based image encryption technique. Soft Comput. 2022;26:3703–12.
6. Singh KN, Singh AK. Towards integrating image encryption with compression: a survey. ACM Trans Multimedia Comput Commun Appl. 2022;18(3):2022.
7. Amrit P, Singh AK. Survey on watermarking methods in the artificial intelligence domain and beyond. Comput Commun. 2022;188:52–65.
8. Singh OP, Singh AK. A robust information hiding algorithm based on lossless encryption and NSCT-HD-SVD. Mach Vis Appl. 2021;32(101).
9. Wan W, Wang J, Zhang Y, Li J, Yu H, Sun J. A comprehensive survey on robust image watermarking. Neurocomputing. 2022;488:226–47.
10. Anand A, Singh AK, Lv Z, Bhatnagar G. Compression-then-encryption-based secure watermarking technique for smart healthcare system. in IEEE MultiMedia. 2020;27(4):133–143.
11. Zhang K, Zuo W, Chen Y, Meng D, Zhang L. Beyond a Gaussian Denoiser: residual learning of deep CNN for image denoising. IEEE Trans Image Process. 2017;26(7):3142–55.
12. Anand A, Singh AK. Health record security through multiple watermarking on fused medical images. IEEE Transactions on Computational Social Systems. 2021.
13. Bhardwaj R. Hiding patient information in medical images: an encrypted dual image reversible and secure patient data hiding algorithm for e-healthcare. Multimed Tools Appl. 2022;81:1125–52.
14. Vaidya SP. Fingerprint-based robust medical image watermarking in hybrid transform. Visl Comput. 2022 pp. 1–16.
15. Sayah MM, Redouane K, Amine K. A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocess Microsyst. 2022;90: 104490.
16. Ramzan M, Habib M, Khan SA. Secure and efficient privacy protection system for medical records. Sustainable Computing: Informatics and Systems. 2022;35: 100717.
17. Manikandan V, Amirtharajan R. A simple embed over encryption scheme for DICOM images using Bülban Map. Med Biol Eng Comput. 2022;60:701–717.

18. Singh P et al. Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. IEEE Access. 2022.
19. Daoui A, Karmouni H, Sayyouri M, Qjidaa H. Robust image encryption and zero-watermarking scheme using SCA and modified logistic map. Expert Syst Appl. 2022;190: 116193.
20. Li H, Deng L, Gu Z. A robust image encryption algorithm based on a 32-bit chaotic system. IEEE Access. 2020;8:30127–51.
21. https://openi.nlm.nih.gov/gridquery?it=xg,c,m&m=1&n=100. Accessed 25 Mar 2022.
22. https://github.com/ml-workgroup/covid-19-image-repository/tree/master/png. Accessed 25 Mar 2022.
23. Anderson TW. An introduction to multivariate statistical analysis. New York: Wiley; 1958.
24. Lin H, Wang C, Cui L, Sun Y, Xu C, Yu F. Brain-like initial-boosted hyperchaos and application in biomedical image encryption. IEEE Trans Ind Inf. 2022. https://doi.org/10.1109/TII.2022.3155599.
25. Manikandan V, Amirtharajan R. A simple embed over encryption scheme for DICOM images using Bülban Map. Med Biol Eng Comput. 2022;60:701–17.
26. Sarosh P, Parah SA, Bhat GM. An efficient image encryption scheme for healthcare applications. Multimed Tools Appl. 2022;81:7253–70.
27. Teng L, Wang X, Xian Y. Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. Inf Sci. 2022;605:71–85.
28. Adeel A, Ahmad J, Larijani H, Hussain A. A novel real-time, lightweight chaotic-encryption scheme for next-generation audio-visual hearing aids. Cogn Comput. 2020;12.
29. Adeel A, Ahmad J, Hussain A. Real-time lightweight chaotic encryption for 5g iot enabled lip-reading driven secure hearing-aid. 2018. arXiv preprint arXiv:1809.04966.
30. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos. 2006;16(08):2129–51.
31. Anand A, Singh AK. An improved DWT-SVD domain watermarking for medical information security. Comput Commun. 2020;152:72–80.
32. Singh OP, Singh AK. Data hiding in encryption–compression domain. Complex Intell Syst. 2021.
33. Khare P, Srivastava VK. A Secured and robust medical image watermarking approach for protecting integrity of medical images. Trans Emerging Tel Tech. 2021;32: e3918.
34. Anand A, Singh AK. Dual watermarking for security of COVID-19 patient record. IEEE Transactions on Dependable and Secure Computing. 2022. https://doi.org/10.1109/TDSC.2022.3144657.

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