Journal of Database Management
Volume 34 • Issue 2

Security of Medical Images Using a Key-Based Encryption Algorithm in the RDWT-RSVD Domain: SeMIE

Monu Singh, National Institute of Technology, Patna, India
Amit Kumar Singh, National Institute of Technology, Patna, India*

ABSTRACT

Today, in the era of big data, an increasingly serious problem is the security of digital media in the healthcare domain. Encryption is a popular technique to resolve the security concern of medical data. In the paper, the authors propose a key-based encryption algorithm – namely, SeMIE, designed by RDWT and RSVD for healthcare applications – which can guarantee the security of the medical images. Initially, the image normalisation procedure along with RDWT-RSVD is followed to generate hash value. Here, image normalisation is used to ensure the high resistance against the geometric modifications. Then, a key expansion process is utilised with the hash value for generating the secure keys. Finally, the encryption process uses Feistel structure along with constant substitution-permutation functions to provide sufficient confusion and diffusion of cipher data. Experimental evaluation indicates that the SeMIE algorithm is secure against several attacks. From the simulation findings, it is inferred that the algorithm exhibits improved security compared to existing methods.

KEYWORDS

Big data, Encryption, healthcare, images, IoT, Security

1. INTRODUCTION

With the proliferation of the internet of things (IoT), the healthcare industry has experienced significant growth in recent years (Bhuiyan et al., 2021). There is no doubt that the use of the IoT in healthcare not only improves operational efðciency for medical professionals and hospitals but also provides service convenience for supporting patients and their relatives. Especially after the COVID-19 pandemic, medical images serve as the information carrier for various purposes, such as medical diagnosis, telesurgery, defense, medical education, teleconsulting, research and business analytics (Singh et al., 2021; Khaldi et al., 2022; Sharma et al., 2021).

However, security of these images is a prerequisite for the application of the IoT in the healthcare industry (Li et al., 2021). Also, cloud-based healthcare is an important solution for the efficient storage,

DOI: 10.4018/JDM.318413 *Corresponding Author

processing and continuous availability of medical data supplied by various sources. However, the protection of this externalised data and services in open environments is a big challenge (Haddad et al., 2020). Therefore, the protection of the medical information for smart healthcare is crucial (Wei et al., 2013). Encryption is a popular technique for protecting medical data from illegitimate access (Kaur & Kumar, 2020). The simplified procedure of an image encryption is depicted in Fig. 1.

Let us assume 'O_i' as original/plain image and 'C_i' as cipher image. The encryption and decryption process is carried out on plain and cipher image respectively as shown in equation (1) and equation (2).

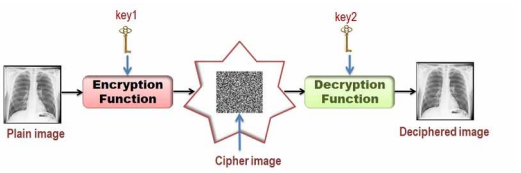
$$C_i = Ef_{key1}\left(O_i\right) \ldots\ldots \quad (1)$$

$$O_i = Df_{key2}\left(C_i\right) \ldots\ldots \quad (2)$$

Where 'Ef_{key1}' & 'Df_{key2}' are encryption and decryption functions along with key. In case of symmetric encryption (Roy et al., 2022), $Key_1 = Key_2$. However, $Key_1 \neq Key_2$ in case of asymmetric encryption.

Over the past few years, researchers have adopted encryption algorithms to provide security for medical images. For example, a chaos-based cipher approach was introduced for medical images (Belazi et al., 2021). This cryptosystem followed permutation-substitution structure. A Logistic Chebyshev map and a Sine-Chebyshev map were utilized to create substitution and diffusion in encrypted images. Their scheme is capable of resisting common attacks, but its encryption time needs to be improved. Another chaos-based cryptosystem for medical images has been proposed (Jain et al., 2021). The secret key used for the encryption/decryption process is twofold since the proposed method is utilizing two different chaotic maps. The original image is passed into a permutation box, where Arnold's Cat Map is used to create confusion in the image. This intermediate data is then processed via diffusion box using two-dimensional logistic-sine-coupling map (2D-LSCM), which assures that a minor change in an input image brings a major change in the output image. The authors have analyzed their scheme against various attacks that range from statistical analysis to contrast analysis, and they established that their scheme is secure, despite the performance of the scheme needing to be analyzed against other attacks like noise and occlusion attacks. Furthermore, the running time of the proposed scheme is longer than state-of-the-art schemes due to the use of multiple chaotic maps. (Masood et al., 2021) introduced an encryption scheme for securing medical images by adapting a Hénon chaotic map to obtain confusion in each block of an image. Diffusion is achieved by utilising Brownian motion (BM) and Chen chaotic system (CCS). The proposed framework provides good encryption results; however, the method could be enhanced to increase security results while reducing computing cost. Another lightweight encryption scheme for enhancing security of medical images was proposed (Hasan et al., 2021). It employed image encryption transformations based on blocks. In addition, the XOR gate

Figure 1. An image encryption process



operation and circular shift operation is applied between the image blocks and selected key to produce a cipher image. This scheme offered less computational cost but with limited encryption capabilities. In reference to (Xue et al., 2021), there is a method for encrypting images based on deoxyribonucleic acid (DNA) chains of varying length. To obtain keys, the proposed technique combines SHA-256 and hamming distances. Here, the plain image is dynamically encoded per the bit stream of a pixel, and then it employs the superior fractional-order hyper-chaotic system (FHCOC) system to achieve the finest DNA dynamic coding, build DNA dynamic chains of various lengths, and perform dynamic deletion and transposition operations on DNA chains. After integrating the DNA chain, the encrypted image is acquired. Their encryption results are good, but the algorithm is more complex. By making use of a similar DNA approach (Li et al., 2021) proposed an encryption technique for digital images. In this scheme, a Two-Dimensional Logistic-adjusted-Sine map (2D-LASM) and a one-dimensional proposed chaotic system were used to generate chaotic sequences. The initial values and system parameters for these maps were determined by applying SHA-256 on plain image. Then, the DNA encoding/decoding rule matrix and the obtained chaotic sequences were utilized in confusion and diffusion stages. The proposed scheme has a larger key space and can withstand chosen plaintext attack. However, the scheme's computational cost is relatively higher than that of several recent methods. An encryption system based on 2D multiple chaotic maps for medical images were suggested by (Yasser et al., 2021). To overcome the limitations of low dimensional chaotic maps, authors have proposed two 2D-chaotic key maps. A two-pass confusion-and-diffusion process is applied on an image after splitting it into two halves. The proposed scheme has good anti-attack capabilities. An edge detection based lightweight encryption technique was presented by (Khashan & AlShaikh, 2020). for medical data. The significant edge-maps are extracted from an image using Prewitt edge detection method. A chaotic map is employed to generate random keys. Then, only identified significant blocks are encrypted using one-time pad method to reduce the time complexity of the proposed scheme. Its performance against statistical attacks needs to be analyzed further, as the histogram of cipher image is non-uniform. (Chai et al., 2019) introduced a technique of encrypting medical images that performs permutation and diffusion operations using the random sequence obtained from the 4D-memristive chaotic map. The SHA-256 value of the image is utilized as the initial parameters of a 4D map, making it immune to known plaintext and chosen plaintext attacks. To obtain a highly random cipher image, authors utilized Latin square for pixel-permutation and bi-directional diffusion. Their scheme performs comparably to state-of-the-art techniques. Based on Hessenberg's transform and chaotic theories, an encryption technique for smart health care systems has been suggested in (Jan et al., 2022). This scheme combines logistic map and sine map to generate the effect of confusion in the given data. After that, diffusion is produced using Hessenberg transform, the proposed scheme has justifiable performance against statistical and differential attacks, and it also has efficient execution time. However, the performance of the suggested scheme has not been assessed against noise attacks. Another lightweight cryptosystem for secure IoT has been introduced by (Usman et al., 2017). This scheme aims to address the issue of security and resource allocation in IoT systems. The architecture of the scheme is a hybrid of Feistel structure and substitution-permutation (SP) network. Initially, this scheme applied a key expansion procedure on the secret key taken from the user to produce five round keys. These round keys are then utilized in the encryption/decryption process. The suggested F-Function and some logical operations are used for encrypting an image. The simulation results indicated that both the computational cost and memory utilization of proposed scheme are efficient. The authors have analyzed the performance of the suggested scheme against statistical and cipher-text only attacks. Its performance needs to be analyzed further against other attacks too. Additionally, this system might be vulnerable to brute-force attack because of its key size. A system for calculating image hash based on image normalization, discrete wavelet transform (DWT) and singular value decomposition (SVD) are introduced by (Singh & Bhatnagar, 2017). Initially, the plain image is pre-processed using normalization process. Then, the image hash is obtained by using DWT and SVD

transform on the pre-processed image. The proposed scheme is secure against scaling and filtering attacks. However, the scheme suffers from the shift variant problem of DWT.

In this study, we propose a key-based encryption algorithm – namely, SeMIE, designed by RDWT-RSVD for healthcare applications – which can guarantee the security of the medical images. Major novelties of this work are as follows:

1) **Benefits of Image Normalization:** The image normalization procedure (Singh & Bhatnagar, 2018) is utilized to transform the image into a standard image, which offers high resistance against the geometric attacks.
2) ***Generation of Hash Value through RDWT-RSVD*:** A combination of RDWT-RSVD transformed is used to generate hash value for better security. RDWT is shift-invariant and holds all the desirable properties of DWT (Singh et al., 2021; Anand & Singh, 2020). Additionally, RSVD is better than SVD with reduced (Anand et al., 2020)
3) ***Better Security Performance*:** Compared with the traditional, the SeMIE algorithm has better security performance at a lower cost, indicating its potential for secure healthcare.

This paper is organized as follows. In Section 2, proposed SeMIE algorithm is described in detail. In Section 3, the simulation is given. Finally, the conclusion is drawn in Section 4.

2. THE SEMIE ALGORITHM

The suggested SeMIE algorithm consists of three main phases: a) key generation process, b) the key expansion procedure, and c) the encryption and decryption procedure. The stepwise procedure of each phase is illustrated in Algorithm 1 to Algorithm 4, respectively. Some commonly used notations in algorithms are listed in Table 1.

2.1 Key Generation Process

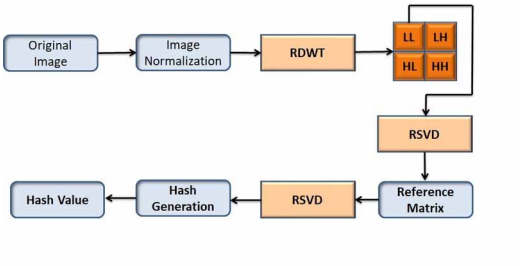
The key is the most critical component in any encryption algorithm. The whole security of the encryption scheme is dependent on this key. The simplified procedure of hash value computation of plain image for the purpose of better security is shown in figure 2. In this process, an image normalization procedure is utilised to transform the image into a standard image, which offers high resistance against the geometric attacks. Here, the image normalisation procedure, along with RDWT-RSVD, is followed to generate hash value. The normalisation procedure for a particular image can be outlined as follows:

Translation Invariance: Initially an input image is transformed to new position using the equation given below:

Table 1. The symbols

Symbol	Function name
$\oplus$	XOR
$\odot$	XNOR
$\dotplus$, $\|\|$	Concatenation

Figure 2. *Hash* **value generation process**



$$\left(X_O, Y_O\right)^T = \left(X_i - t_x, Y_i - t_y\right)^T \ldots\ldots \quad (3)$$

Where

X_O, Y_O = coordinates of output image

X_i, Y_i = coordinates of input image

t_x, t_y = Translation value in x and y direction respectively.

Shearing Invariance (in x-direction): Now shearing is applied on the transformed image in x-direction as shown below:

$$S_x = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$$

Here, S_x *= shearing operator in x-direction*

Shearing Invariance (in y-direction): Again shearing transform in y-direction is applied on the image obtained from step 2.

$$S_y = \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}$$

Here, S_y = shearing operator in y-direction

4) ***Scaling Invariance:*** Finally, a normalized image of specific size is obtained after applying scaling transform in both x and y direction using scaling operator (S_s).

$$S_s = \begin{bmatrix} \gamma & 0 \\ 0 & \lambda \end{bmatrix}$$

The detail of key generation process is discussed in Algorithm 1.

Algorithm 1. Hash Value Generation Process

Input: Plain image $\left(P_i\right)$

Step 1: In pre-processing stage, image normalization procedure is utilized to transform the original image, '$\mathrm{Org}_{\mathrm{img}}$' into normalized image, '$\mathrm{Norm}_{\mathrm{img}}$', which provides better resistance against the geometric attacks.

Step 2: RDWT is performed on $\mathrm{Norm}_{\mathrm{img}}$

$\left[LL, LH, HL, HH\right] \leftarrow RDWT\left(\mathrm{Norm}_{\mathrm{img}}, 'haar'\right)$.

// LL, LH, HL, HH are four sub-bands of image obtained after applying RDWT.

Step 3: Apply RSVD to LL coefficient of $\mathrm{Norm}_{\mathrm{img}}$

$\left[U,S,V\right] \leftarrow RSVD\left(LL\right)$

// U,S,V are Left, diagonal and right singular vectors

Step 4: Reference matrix, 'B' is obtained using first l Colums of U and V.

$B \leftarrow \left[U^1 \ldots U^l, V^1 \ldots V^l\right]$

Step 5: Again, RSVD is applied to transform the reference matrix, 'B'.

$\left[U_1, S_1, V_1\right] \leftarrow RSVD\left(B\right)$

Step 6: Feature vector, 'F_v' is obtained using the combination of U_1, V_1.

$F_v \leftarrow \left[U_1, V_1\right]$

Step 7: Threshold, 'T' is obtained with the help of feature vector.

Step 8: The hash value, 'H' is obtained as mentioned below.

$$H\left(i\right) = \begin{Bmatrix} 1, & F_v\left(i\right) > T \\ 0, & otherwise \end{Bmatrix}$$

Step 9: We take first 64-bit of hash value from 160-bits, which is used as cipher key

tput: 64-bit cipher key

2.2 Key Expansion Module

The simplified procedure of key expansion module is shown in Fig. 3. The major steps for this module are explained in algorithm 2. Initially in this module, a 64-bit key generated by using algorithm 1 is divided into 4-bit segments. Then these 4-bit segments are substituted and grouped with each other to produce 16-bit blocks using equation 4. These 16-bit blocks are taken as input by F-function. The F-function is made up of P and Q tables. The P and Q tables are utilized to perform permutations in 64-bit cipher key as described in fig. 4. Table 2 and 3 shows the transformations performed by P and Q tables.

2.3 Encryption and Decryption Process

The simplified procedure of encryption process is shown in Fig. 5. Initially, the encryption scheme is developed by (Usman et al., 2017). However, our key generation procedure is totally different from the scheme proposed in (Usman et al., 2017). Further, the security analysis of the encryption scheme (Usman et al., 2017) is inadequate. Here, the encryption process can begin after the round

Algorithm 2. Key Expansion Procedure

Input: 64-bit cipher key

Step 1: The 64-bit encryption key (K_c) is divided into 4-bit segments in the initial stage.

Step 2: The F-function works with data that is of 16-bits. Hence, four F-function blocks are utilised. After performing substitution on 4-bit segments of K_c as given in equation 4, 16-bits for every F-function are produced.

$$fKb_i = ||_{j=1}^{4} Kc_{4(j-1)+i} \quad \text{..... (4)}$$

Where i = 1 to 4 for the first four round keys as shown in fig. 3.

Step 3: The very next step is to obtain fKa_i by invoking the F-function on fKb_i as given below:

$$fKa_i = f\left(fKb_i\right) \quad \text{.... (5)}$$

Step 4: The F-function is comprised of P and Q transformation tables which causes confusion and diffusion as shown in fig. 4. Table II and III shows the transformations accomplished by P and Q tables.

Step 5: Four round keys (K_1 , K_2 , K_3 and K_4) are generated through four F-functions. To obtain the fifth key (K_5), an XOR operation is applied on (K_1 , K_2 , K_3 and K_4), as indicated in equation 6.

$$K_5 = \oplus_{i=1}^{4} K_i \quad \text{..... (6)}$$

Output: Five Round Keys (K_1 , K_2 , K_3 , K_4 and K_5), each is of 16choosen -bit.

Table 2. P Table

Kc_i	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$P(Kc_i)$	3	F	E	0	5	4	B	C	D	A	9	6	7	8	2	1

Table 3. Q Table

Kc_i	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$Q(Kc_i)$	9	E	5	6	A	2	3	C	F	0	4	D	7	B	1	8

keys have been generated. This procedure entails certain logical and swapping operations to produce confusion and diffusion effects. It is comprised of five rounds. A separate encryption key is generated for each round using the aforementioned key generation process. The details of image encryption and decryption process are stated in Algorithm 3 and Algorithm 4, respectively. The decryption procedure is the reverse of the encryption process.

Figure 3. Design idea of key expansion module

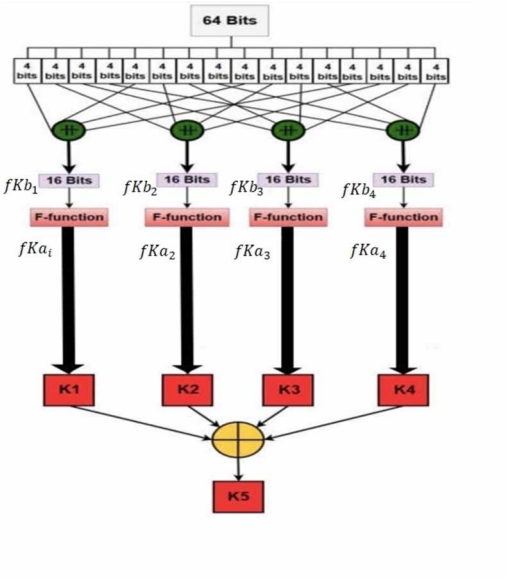
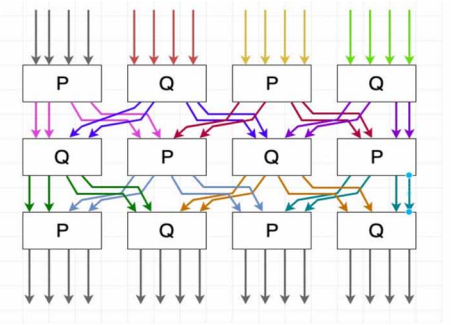


Figure 4. Working of F-function



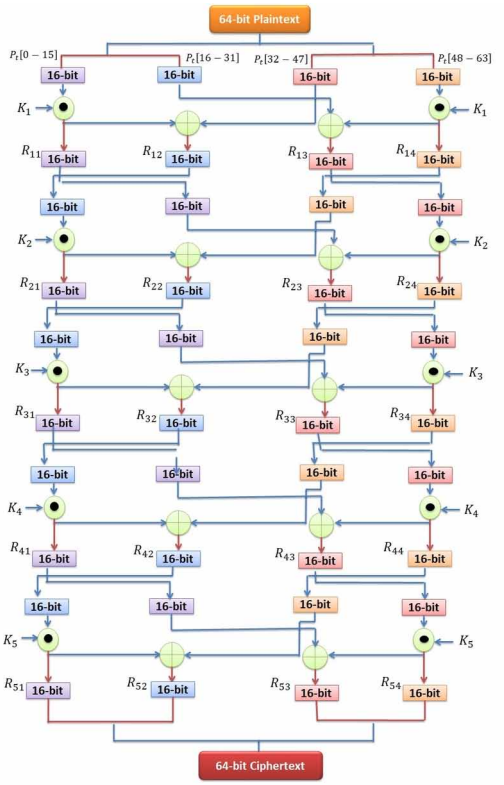
3. EXPERIMENTS AND COMPARISON

In this section, experiments and analyses are conducted to evaluate the effectiveness of the proposed SeMIE algorithm, and we compare it in terms of standard metric with other, similar schemes. Particularly, the performance of the SeMIE algorithm is evaluated by applying several standard tests, including key analysis, statistical analysis, differential analysis and time cost evaluation, on the COVID-19 Radiography dataset of size 256×256 (Data set) . Few of the images used in evaluation are shown in fig. 6. All the experiments were performed using MATLAB 2019a.

3.1 Differential Analysis

Differential analysis is used to measure the strength of the encryption technique by minor changes to the original image and to examine differences (Kamal et al., 2021). NPCR and UACI randomness tests were used to evaluate the differential analysis. It is defined as follows:

Figure 5. Design idea of encryption process



Algorithm 3. Encryption Process

Input: Five Round Keys (K_1 , K_2 , K_3 , K_4 and K_5) and 64-bit Plaintext array (P_t)

Step 1: First of all in round 1, a 64-bit plaintext array is divided into four 16-bit segments i.e. $P_{t[0-15]}$, $P_{t[16-31]}$, $P_{t[32-47]}$ and $P_{t[48-63]}$.

Step 2: The bitwise EX-NOR (XNOR) operation is applied between $P_{t[0-15]}$ and the corresponding rounds key K_i which is generated previously from the key expansion process. The same operation is conducted on $P_{t[48-63]}$ and K_i as well, eventuating in R_{11} and R_{14} respectively.

Step 3: After that, the outcome of $P_{t[0-15]} \odot K_i$ is XORed with $P_{t[32-47]}$ to get R_{12} and the result of $P_{t[48-63]} \odot K_i$ is XORed with $P_{t[16-31]}$ to obtain R_{13} as shown in fig. 5.

Step 4: Finally, a transformation is performed such that R_{11} becomes $P_{t[16-31]}$, R_{12} becomes $P_{t[0-15]}$, R_{13} becomes $P_{t[48-63]}$ and R_{14} becomes $P_{t[32-47]}$ for the next round.

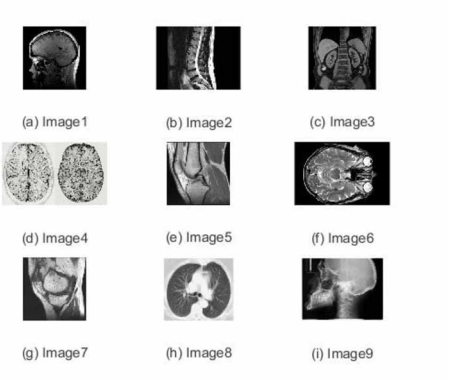
Step 5: The remaining rounds are completed in the same manner. The final round's results are concatenated to produce the ciphertext.

Output: 64-bit Ciphertext

Algorithm 4. Decryption Process

Input: Five Round Keys (K_1, K_2, K_3, K_4 and K_5) and 64-bit ciphertext (C_t)
Step 1: First of all, a 64-bit ciphertext is divided into four 16-bit segments i.e. $C_{t[0-15]}$, $C_{t[16-31]}$, $C_{t[32-47]}$ and $C_{t[48-63]}$.
Step 2: The bitwise EX-NOR (XNOR) operation is applied between $C_{t[0-15]}$ and the corresponding rounds key K_i which is generated previously from the key expansion process. The same operation is conducted on $C_{t[48-63]}$ and K_i as well, eventuating in R_{41} and R_{44} respectively.
Step 3: After that, $C_{t[0-15]}$ is XORed with $C_{t[32-47]}$ to get R_{42} and $C_{t[48-63]}$ is XORed with $C_{t[16-31]}$ to obtain R_{43}.
Step 4: A reverse transformation is performed such that $C_{t[16-31]}$ becomes R_{41}, $C_{t[0-15]}$ becomes R_{42}, $C_{t[48-63]}$ becomes R_{43} and $C_{t[32-47]}$ becomes R_{44} for the next round.
Step 5: The remaining rounds are completed in the same manner. The final round's results are concatenated to produce the plaintext array of 64-bit.
Output: 64-bit Plaintext array

Figure 6. Test images



$$NPCR = \frac{\sum_{i,j} D\left(i,j\right)}{W \times H} \times 100\% \ldots\ldots\ldots \quad (7)$$

Where W & H are width and height of image respectively,

$$D\left(i,j\right) = \begin{cases} 1, C1\left(i,j\right) \neq C2\left(i,j\right) \\ 0, otherwise \end{cases}$$

Where C1 and C2 are ciphered image before and after alteration of pixel.

Table 4. Evaluation of NPCR and UACI

Image	NPCR	UACI
Image1	99.26	41.28
Image2	98.96	42.06
Image3	99.37	37.1
Image4	99.58	34.61
Image5	99.61	32.55
Image6	97.06	39.81
Image 7	99.58	32.66
Image8	99.62	33.6
Image9	99.42	35.27
Image10	99.57	33.53
----	----	----
Image21	99.62	40.19
Mean	**99.30952**	**34.47762**

$$UACI = \frac{\sum_{i,j} E\left(i,j\right) - E'\left(i,j\right)}{255 \times W \times H} \times 100 \ldots\ldots\ldots \quad (8)$$

Where E(i, j) and E'(i, j) are the ciphered images of plain image and modified image respectively. Table 4 lists the average value of NPCR and UACI of the proposed scheme for more than 20 images. The NPCR and UACI values of the proposed scheme are more than 99 and 33, respectively. Hence, our scheme has proven to be robust against differential attacks. Comparison with other schemes is shown in Table 5. Fig. 7 shows the performance of SeMIE in comparison with other state-of-art schemes against differential attacks.

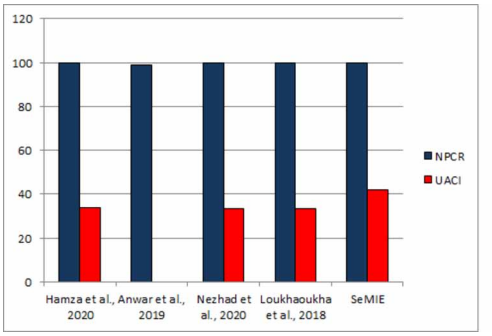
3.2 Statistical Analysis

This analysis is performed to find the statistical resemblance between the ciphered and original image. The histogram and correlation coefficient (CC) are used to evaluate the robust performance against statistical attacks (Kamal et al., 2021).

Table 5. NPCR and UACI comparison

Encryption Algorithm	NPCR	UACI
Hamza et al., 2020	99.61	33.61
Anwar et al., 2019	98.74	-
Nezhad et al., 2020	99.60	33.46
Loukhaoukha et al., 2018	99.62	33.58
SeMIE	**99.67**	**42.06**

Figure 7. Performance of SeMIE and other state-of-the-art schemes against differential attacks

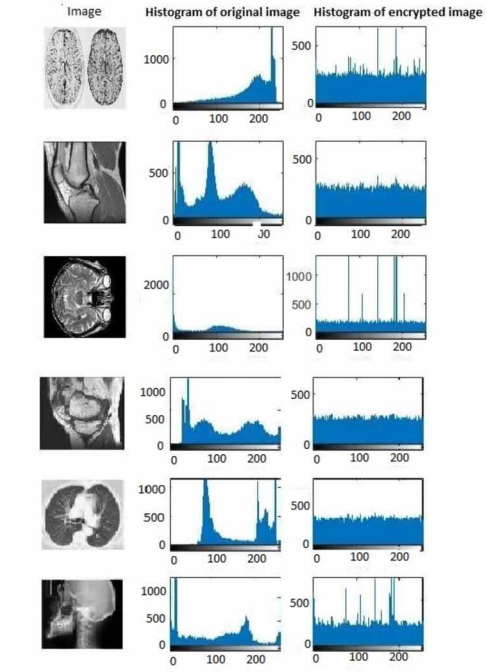


a) ***Histogram:*** A histogram of a cipher image should be almost uniform and differ significantly from the original image histogram. Thus, it provides no information on how to attack on the encrypted image using statistical analysis. Histograms for both plain and cipher images are shown in Fig. 8. As is evident from Fig. 8, the histogram of the encrypted image is uniform. Therefore, our scheme is capable of resisting statistical attacks.

b) Correlation Coefficient (CC)

The correlation coefficient is a significant feature to measure the effectiveness of the encryption technique (Ibrahim et al., 2020). The original image has a high level of redundancy, whereas the

Figure 8. Histogram of original and encrypted image for medical images



encrypted image must have low CC value. The correlation coefficients between pairs of neighbouring pixels in horizontal, vertical, and diagonal directions are defined as:

$$r_{x,y} = \frac{C\left(x,y\right)}{\sqrt{D\left(x\right)}\times\sqrt{D\left(y\right)}} \ldots. \tag{9}$$

Where

$$C\left(x,y\right) = \frac{\sum_{i=1}^{K}\left(x_i - E\left(x\right)\right)\left(y_i - E\left(y\right)\right)}{K}; D\left(x\right) = \frac{1}{k}\sum_{i=1}^{K}\left(x_i - E\left(x\right)\right)^2; D\left(y\right) = \frac{1}{k}\sum_{i=1}^{K}\left(y_i - E\left(y\right)\right)^2$$

Here, x, y = coordinates of an image pixel; C(x, y) = covariance between samples x and y; K = number of pixel pairs (x_i, y_i); D(x) and D(y) = standard deviation of x and y, and E(x) = mean of xi pixel values. We compute horizontal, vertical and diagonal correlation coefficients of original and encrypted images, as shown in Table 6. It can be observed from the table that the CC of encrypted image is very low, which means that redundancy between the adjacent pixel values is greatly reduced. Thus, we can say that our cryptosystem can prevent statistical attack.

3.3 Information Entropy

The entropy is a measurement of the degree of randomness in the encrypted image (Noura et al., 2019). High entropy values indicate the high randomness in the encrypted image. The ideal entropy value of encrypted image is approaching to 8. Entropy is defined as

$$H\left(S\right) = -\sum_{s}\left(\mathrm{P}\left(\mathrm{S_i}\right)\times\log_2\mathrm{P}\left(\mathrm{S_i}\right)\right) \ldots\ldots \tag{10}$$

Where, H (S) = entropy of message source (S) and
$P(S_i)$ = probability of occurrence of S_i

Table 6. Correlation Coefficient of the original and encrypted images

Image	CC of original image			CC of Encrypted image		
	H_O	V_O	D_O	H_E	V_E	D_E
Image1	0.9523	0.945	0.9107	-0.0789	0.0994	-0.0709
Image2	0.9506	0.9842	0.9457	-0.1104	0.0366	-0.025
Image3	0.9535	0.9749	0.9318	-0.0587	0.0603	-0.0606
Image4	0.7444	0.8313	0.6944	0.0112	0.0223	-0.0089
Image5	0.9681	0.9843	0.9623	-0.0026	-0.0093	-0.0314
Image6	0.9448	0.9612	0.9204	-0.052	0.0888	-0.0827
Image7	0.9668	0.9835	0.962	-0.0233	-0.0158	0.0072
Image8	0.9876	0.9925	0.98	-0.0006	-0.016	-0.0001
Image9	0.9859	0.9951	0.9813	-0.0071	0.0141	0.0223

Table 7 shows entropy value of proposed scheme for different images. The entropy value obtained for an encrypted image in our scheme is closer to eight, which means the encrypted image is extremely messy. It ensures that this scheme is robust against cipher-text only attacks. Additionally, the entropy of the proposed scheme is higher as compared to the state-of-the-art scheme, as depicted in Table 8 and in figure 9.

3.4 Perceptual Quality Evaluation

The perceptual quality of the encrypted image is measured by PSNR [32], which indicates the similarity between the encrypted image and the corresponding original image. PSNR is represented as

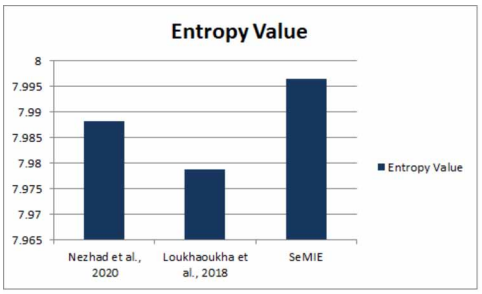
Table 7. Information entropy

Image	Entropy of Original Image	Entropy of Encrypted Image
Image1	5.7123	7.4302
Image2	5.4713	7.3093
Image3	6.5768	7.8727
Image4	6.8308	7.9716
Image5	7.5787	7.9948
Image6	5.6806	7.2518
Image7	7.5072	7.995
Image8	6.9063	7.9964
Image9	7.2084	7.8865

Table 8. Entropy comparison

Encryption Algorithm	Entropy Value
SeMIE	7.9964
Nezhad et al., 2020	7.9882
Loukhaoukha et al., 2018	7.9787

Figure 9. Entropy value of SeMIE and other exisiting schemes



$$PSNR = 10 \times log_{10} \frac{\left(2^n - 1\right)^2}{MSE} \ldots \tag{11}$$

Where n = no. of bits per pixel

$$MSE = \frac{1}{WH} \sum_{x=1}^{x=W} \sum_{y=1}^{y=H} (P\left(x, y\right) - E\left(x, y\right)^2 \ldots\ldots \tag{12}$$

Where (x, y) = pixel coordinates of image; WH = width and height of image; P and E = plain and encrypted images

To evaluate the PSNR performance of the proposed system against noise attack and the corresponding results are depicted below in Table 9. We have calculated the PSNR value between the original and decrypted image. Figure 10 shows the performance of SeMIE against different possible noise attacks.

3.5 Key Sensitivity

Key sensitivity means a minor modification in key results in entirely different results. To perform this analysis, two cipher images are obtained with two secret keys that differ by only one bit. A cryptosystem is considered secure if a minor change in the key results in a completely new cipher

Table 9. Evaluation of quality

Noise Attack	PSNR (in dB)
Salt and pepper noise (0.001)	33.7869
Salt and pepper noise (0.005)	27.0792
Salt and pepper noise (0.01)	24.0979
Salt and pepper noise (0.05)	16.9277
Speckle noise (0.001)	42.2360
Speckle noise (0.005)	35.2968
Speckle noise (0.01)	32.2863
Speckle noise (0.05)	25.4674
Gaussian noise (0.001)	30.6093
Gaussian noise (0.005)	24.1004
Gaussian noise (0.01)	21.2994
Gaussian noise (0.05)	15.0117
Rotation (90)	12.8196
Rotation (180)	11.8738
Rotation (270)	12.8196
Average filter [2 2]	31.2495

Figure 10. Performance of SeMIE against different possible noise attacks

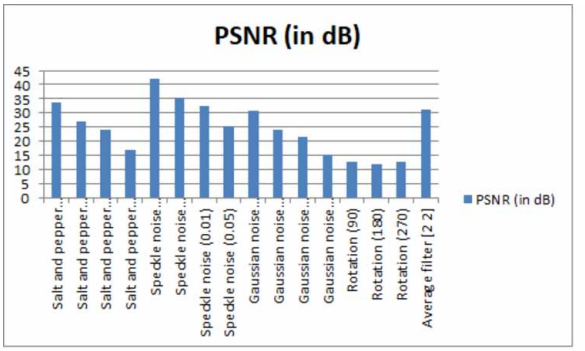
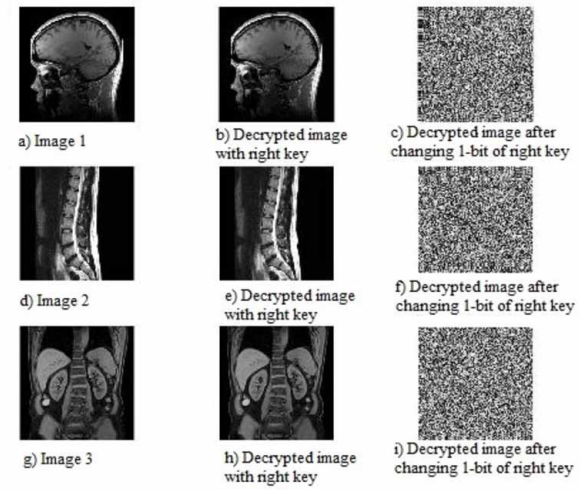


image. From Fig. 11, it is clear that our scheme generates an entirely different cipher image. Thus, we can conclude that our scheme is highly key sensitive.

3.6 Key Space

To strengthen the encryption scheme against brute-force attacks, the key length must be large enough so that the opponent is unable to undertake 2^{n-1} encryptions to find the original key if the key is of n-bit. In this work, we have first calculated 160-bit hash value using the aforementioned process, and the first 64 bits of hash value are used as the cipher key. The key expansion module takes this cipher key as input, executes considerable options on the input key and generates five distinct keys. These keys will be used for encryption and decryption, and they must be strong enough to stay undecipherable during an attack.

Figure 11. Key sensitivity test: Decryption with original and wrong key



3.7 Time Cost Evaluation

This part is to record the encryption and decryption time of different images. The time taken by our scheme to encrypt/decrypt the images shown in Fig. 6 is given in Table 10. The time required by our scheme is slightly higher when compared to other, existing schemes. However, the simulation findings prove that our scheme is robust against geometric, statistical, differential, noise and other common attacks.

4. CONCLUSION

In the paper, we proposed a key-based encryption algorithm – namely, SeMIE, designed by RDWT-RSVD for healthcare applications – which can guarantee the security of the medical images. Initially, the image normalization procedure along with RDWT-RSVD is followed to generate hash value. Here, image normalization is used to ensure the high resistance against the geometric modifications. Then, a key expansion process is utilized with the hash value for generating the secure keys. Finally, the encryption process uses Feistel structure along with constant substitution-permutation functions to provide sufficient confusion and diffusion of cipher data. Experimental evaluation indicates that the SeMIE algorithm is secure against geometric attacks and several other common attacks. From the simulation findings, it is inferred that the algorithm exhibits improved security compared to existing methods. Future work will focus on making this scheme compliant to the more secure and efficient healthcare system.

4.1 Theoretical Contributions

First, we have provided the recent state-art-of the work in the area of medical image security using encryption.

Second, the study extends the limited research on how to achieve a good balance between competing parameters, such as security and complexity.

Third contribution highlights the concept of several standard tests, including differential analysis, statistical analysis, information entropy, perceptual quality evaluation, key analysis, and time cost evaluation, which is necessary for any encryption scheme.

Table 10. Time cost evaluation

Image	Encryption Time (s)	Decryption Time (s)
Image1	11.6237	11.5646
Image2	11.6395	11.0289
Image3	11.3538	12.4687
Image4	11.6142	12.3839
Image5	11.6672	12.5519
Image6	11.9527	13.3413
Image 7	11.8762	12.774
Image8	12.4412	12.3216
Image9	11.701	13.2315

4.2 Practical Contributions

First, we have proposed a key-based encryption algorithm – namely, SeMIE, designed by RDWT-RSVD for healthcare applications – which can guarantee the security of the medical images.

Second, concept of image normalization procedure is utilized to transform the image into a standard image, which offers high resistance against the geometric attacks.

Third, compared with the traditional, our proposed SeMIE algorithm has better security performance at a lower cost, indicating its potential for secure healthcare.

REFERENCES

Anand, A., & Singh, A. K. (2020, September). RDWT-SVD-firefly based dual watermarking technique for medical images (workshop paper). In 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM) (pp. 366-372). IEEE.

Anand, A., Singh, A. K., Lv, Z., & Bhatnagar, G. (2020). Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE MultiMedia, 27(4), 133–143. doi:10.1109/MMUL.2020.2993269

Anwar, S., & Meghana, S. (2019). A pixel permutation based image encryption technique using chaotic map. Multimedia Tools and Applications, 78(19), 27569–27590. doi:10.1007/s11042-019-07852-2

Belazi, A., Talha, M., Kharbech, S., & Xiang, W. (2019). Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 36667–36681. doi:10.1109/ACCESS.2019.2906292

Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities. *IEEE Internet of Things Journal, 8*(13), 10474–10498. 10.1109/JIOT.2021.3062630

Chai, X., Zhang, J., Gan, Z., & Zhang, Y. (2019). Medical image encryption algorithm based on Latin square and memristive chaotic system. *Multimedia Tools and Applications*, *78*(24), 35419–35453. doi:10.1007/s11042-019-08168-x

Rahman, T. (2021). COVID-19 Radiography dataset. Kaggle. https://www.kaggle.com/datasets/tawsifurrahman/covid19-radiography-database

Haddad, S., Coatrieux, G., Moreau-Gaudry, A., & Cozic, M. (2020). Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains. *IEEE Transactions on Information Forensics and Security*, *15*, 2556–2569. doi:10.1109/TIFS.2020.2972159

Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., & Titouna, F. (2020). A privacy-preserving cryptosystem for IoT E-healthcare. *Information Sciences*, *527*, 493–510. doi:10.1016/j.ins.2019.01.070

Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., Islam, M., Alyahya, S., Ahmed, M. M., Kamil, S., & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 47731–47742. doi:10.1109/ACCESS.2021.3061710

Ibrahim, S., Alhumyani, H., Masud, M., Alshamrani, S. S., Cheikhrouhou, O., Muhammad, G., Hossain, M. S., & Abbas, A. M. (2020). Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 160433–160449. doi:10.1109/ACCESS.2020.3020746

Jain, K., Aji, A., & Krishnan, P. (2021). Medical Image Encryption Scheme Using Multiple Chaotic Maps. *Pattern Recognition Letters*, *152*, 356–364. doi:10.1016/j.patrec.2021.10.033

Jan, A., Parah, S. A., & Malik, B. A. (2022). IEFHAC: Image encryption framework based on hessenberg transform and chaotic theory for smart health. *Multimedia Tools and Applications*, *81*(13), 18829–18853. doi:10.1007/s11042-022-12653-1 PMID:35282407

Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 37855–37865. doi:10.1109/ACCESS.2021.3063237

Kaur, M., & Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, *27*(1), 15–43. doi:10.1007/s11831-018-9298-8

Khaldi, A., Kafi, M. R., & Moad, M. S. (2022). Wrapping based curvelet transform approach for ECG watermarking in telemedicine application. *Biomedical Signal Processing and Control*, *75*, 103540. doi:10.1016/j.bspc.2022.103540

Khashan, O. A., & AlShaikh, M. (2020). Edge-based lightweight selective encryption scheme for digital medical images. *Multimedia Tools and Applications*, *79*(35), 26369–26388. doi:10.1007/s11042-020-09264-z

Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., & Srivastava, G. (2021). An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things. *IEEE Journal of Biomedical and Health Informatics*.

Li, S., Zhao, L., & Yang, N. (2021). Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion. *Security and Communication Networks, 2021*, 2021. 10.1155/2021/6624809

Loukhaoukha, K., Refaey, A., Zebbiche, K., & Shami, A. (2018). Efficient and secure cryptosystem for fingerprint images in wavelet domain. *Multimedia Tools and Applications*, *77*(8), 9325–9339. doi:10.1007/s11042-017-4938-9

Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., & Buchanan, W. J. etal. (2021). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wireless Personal Communications*, ●●●, 1–28.

Nezhad, S. Y. D., Safdarian, N., & Zadeh, S. A. H. (2020). New method for fingerprint images encryption using DNA sequence and chaotic tent map. *Optik (Stuttgart)*, *224*, 165661. doi:10.1016/j.ijleo.2020.165661

Noura, H., Chehab, A., Noura, M., Couturier, R., & Mansour, M. M. (2019). Lightweight, dynamic and efficient image encryption scheme. *Multimedia Tools and Applications*, *78*(12), 16527–16561. doi:10.1007/s11042-018-7000-7

Roy, A. K., Nath, K., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Privacy Preserving Multi-Party Key Exchange Protocol for Wireless Mesh Networks. *Sensors (Basel)*, *22*(5), 1958. doi:10.3390/s22051958 PMID:35271104

Sharma, N., Singh, O. P., Anand, A., & Singh, A. K. (2021). Improved method of optimization-based ECG signal watermarking. *Journal of Electronic Imaging*, *31*(4), 041207. doi:10.1117/1.JEI.31.4.041207

Singh, A. K., Anand, A., Lv, Z., Ko, H., & Mohan, A. (2021). A survey on healthcare data: A security perspective. *ACM Transactions on Multimedia Computing Communications and Applications*, *17*(2s), 1–26. doi:10.1145/3422816

Singh, O. P., Kumar, C., Singh, A. K., Singh, M. P., & Ko, H. (2021). Fuzzy-based secure exchange of digital data using watermarking in NSCT-RDWT-SVD domain. *Concurrency and Computation*, e6251. 10.1002/cpe.6251

Singh, S. P., & Bhatnagar, G. (2017, September). A robust image hashing based on discrete wavelet transform. In *2017 IEEE International Conference on Signal and Image Processing Applications (ICSIPA)* (pp. 440-444). IEEE. doi:10.1109/ICSIPA.2017.8120651

Singh, S. P., & Bhatnagar, G. (2018, March). A robust watermarking scheme based on image normalization. In 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA) (pp. 140-144). IEEE. doi:10.1109/CSPA.2018.8368701

Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: a lightweight encryption algorithm for secure internet of things. arXiv:1704.08688.

Wei, J., Lin, B., & Loho-Noya, M. (2013). Development of an E-Healthcare Information Security Risk Assessment Method [JDM]. *Journal of Database Management*, *24*(1), 36–57. doi:10.4018/jdm.2013010103

Xue, X., Jin, H., Zhou, D., & Zhou, C. (2021). Medical image protection algorithm based on deoxyribonucleic acid chain of dynamic length. *Frontiers in Genetics*, *12*, 266. doi:10.3389/fgene.2021.654663

Yasser, I., Khalil, A. T., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2021). A Robust Chaos-Based Technique for Medical Image Encryption. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 244–257. doi:10.1109/ACCESS.2021.3138718

Amit Kumar Singh is currently an Associate Professor with the Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India. Dr. Singh has contributed more 200 papers including more than 40 papers on IEEE/ACM Transactions. He is an Associate Editor of 8 journals including IEEE Trans. Ind. Informat., IEEE Trans. Computat. Social Syst., IEEE J. Biomed. Heal. Informatics, ACM Trans. Multimedia Comput. Commun. Appl., Eng. Appl. Artif. Intell., Elsevier, IEEE Technology Policy and Ethics Newsletter, and Series Editor, The IET International Book Series on Multimedia Information Processing and Security.