



Edge-based lightweight selective encryption scheme for digital medical images

Osama A. Khashan¹  • Muath AlShaikh¹

Received: 26 August 2019 / Revised: 28 April 2020 / Accepted: 24 June 2020 /

Published online: 14 July 2020

© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Securing digital medical images is increasingly becoming a major concern due to the rapid growth of the amount of medical images transferred over a network and stored on the web servers. However, the enormous size of multimedia and the huge volume of exchanging medical images have motivated the development of low computational complexity methods. This paper presents a lightweight selective encryption scheme to encrypt the edge maps of medical images. The edge map is firstly extracted by an edge detection method. Then, a chaotic map is used to generate a large key space. We propose a one-time pad algorithm to respectively encrypt the significant detected image blocks. The experimental results have proven that the proposed encryption scheme provides an acceptable percentage of encrypted image data. It can also effectively perform image encryption and decryption in a lightweight manner, which makes the scheme a good candidate for real time applications. Moreover, the security analysis demonstrates that our scheme has a robust resistance against various security attacks.

Keywords Selective encryption · Medical image security · Edge detection · One-time pad · Chaotic map

1 Introduction

Digital medical images nowadays are playing an increasingly important role in the medical diagnosing and treating diseases. Vast amount of medical images is produced using multiple imaging technologies, called modalities, including X-Ray, CT, MRI, etc., which are sent via public or private networks for the medical diagnosis, monitoring, or various analyses ([32,

✉ Osama A. Khashan
o.khashan@seu.edu.sa

Muath AlShaikh
m.alshaikh@seu.edu.sa

¹ College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia

46]). Unfortunately, these medical images may involve confidential information concerning patients, where exchanging these sensitive images over a network is vulnerable to numerous security threats and privacy violations. Faced with these growing threats, securing medical images is an important concern [25, 35].

Several technologies have been introduced to address the security threats and to protect all kinds of images, including medical images, such as data hiding, watermarking and encryption. Among these techniques, encryption is the effective solution to preserve the security of medical images by transforming them into unrecognized noise-like ones [19]. Traditional encryption algorithms, such as AES, DES, Blowfish, etc. are originally designed for textual data. Using traditional ciphers for image encryption, image data are transformed into a one-dimensional binary bit stream, which extract plain image data bit by bit and then encrypt the resulting bit stream [21]. Although the security level provided by traditional encryption ciphers is high, however, these methods have been found that they are not suitable for digital images. This is due to the intrinsic features of images, such as large data volumes, high redundancy and strong correlation between pixels. This would consequently require a huge computational cost for image encryption and decryption that prevent them from being used efficiently in real-time applications [16].

The impact of chaos theories has attracted researchers' attention to develop lightweight encryption schemes for digital images. A chaotic system is a mathematical model with complex, unpredictable, and nonlinear behavior can effectively satisfy the requirements of an image encryption. Chaotic methods are very subtle to the preliminary conditions and have a deterministic performance but changeable output. The sensitivity of the system to the initial conditions incomes that slight modifications in the initial factors will yield extremely different performance. Therefore, because of this arbitrariness, orderliness and the sensitivity to the initial conditions, it is very valuable to practice the chaos in the encryption techniques [47].

A general chaos-based image encryption method employs a synchronous confusion and diffusion phases. The confusion phase scrambles image pixels to reduce its correlation, while the diffusion phase masks the pixel values with other random values [38]. Accordingly, various research works have been carried out using chaotic cryptography for digital images with many improvements to the general confusion-diffusion architecture. Some approaches propose a high-dimensional chaotic image encryption [39]. Other approaches use hyper-chaos system combined with DNA encoding [2, 13], or use a combined chaotic encryption-compression methods [28].

Although chaos-based encryption can efficiently deal with the intractable problem of fast and highly secure image encryption, the computation complexity and the high processing time needed to carry out full image encryption is still a challenge for real-time implementations [24].

To overcome the complexity issue of full image encryption up to a considerable extent, partial or selective encryption was proposed. The objective of this approach is to minimize the encryption ratio and thereby reducing the encryption time. It trades off security for computational complexity to satisfy the requirements of high-speed real-time secure communication for limited-power devices [17]. However, one of the major issues related to this approach is the selection of the most important information in an image for encryption. Some selective encryption schemes in the literature, perform manual or static selection of encrypted data and encryption parameters. Other schemes exploit the statistical properties of an image to encrypt the most significant bits, pixels or blocks [18]. Recent approaches consider the regions in an image with semantic information for the encryption, while ignoring other smooth regions without encryption [5, 42, 47].

On the other hand, several chaotic-based image cryptosystems have been proven in the literature to exhibit various security weaknesses that crypt-analyzed successfully [7, 24, 48]. This is due to the inability of the implemented chaotic maps to provide complex dynamical behaviors, which render the cryptosystem vulnerable to different kinds of attacks [30]. Furthermore, medical images contain important visual information about disease or afflictions to the human body different from other visual data. Besides, specific features that are different from natural images, as reported in [9].

To address these issues, this work proposes a selective encryption scheme to encrypt the edge maps of medical images. The major contributions of this work are summarized as follows:

1. We propose an edge-based lightweight selective encryption scheme using a combination of edge detection, One Time Pad (OTP), and Chaotic Map approaches to protect medical images with high efficiency and robustness.
2. The proposed scheme is able to reduce the computational time of encryption process by only encrypting the significant detected image blocks using the OTP algorithm. Moreover, the scheme provides high key sensitivity with a sufficiently large key space generated by a chaotic map to increase the security of encrypted medical images and to resist a certain degree of attacks, while keeping image quality at a relatively high level.
3. We provide security and performance analyses of our scheme. The results and comparisons show that the proposed scheme has high security level, less computation complexity, and better robustness against attacks, which make the scheme suitable for real-time encryption applications as well as resource-constrained devices.

The remainder of this paper is organized as follows. Section 2 provides a review for the related work. The proposed scheme is presented in Section 3. Section 4 discusses the experimental results. Finally, the conclusion of the paper is given in Section 5.

2 Related work

Many approaches have been proposed in the literature using selective image encryption for both spatial and frequency domains. In frequency domain, selective encryption is applied on selected frequency coefficients of image data based on predefined criteria. While in the spatial domain, selective encryption is applied on bit-level or pixel-level using confusion and diffusion to change their actual values [21].

Several works have exploited the Discrete Wavelet Transform (DWT) [1, 15] to encrypt LL band coefficients or selected coefficients from other bands using chaotic maps. Other proposed methods [23, 31] used Discrete Cosine Transform (DCT) to select significant coefficients for subsequent encryption operations. Literatures ([36]; [34]) proposed schemes that represent a number of bit-planes in an image for encryption using chaotic maps. Another proposed scheme by [14] which was based on the correlation coefficient of image blocks with high values, which are XORed and shuffled using a chaotic map to achieve the goal of encryption.

Recently, many researchers tend to develop selective encryption schemes based on semantic image features, which would give attackers useful details about the original data. These feature encryption schemes first perform feature detection, such as objects, edges, region of interests (ROI), contours, etc. using detection algorithms then implement encryption. Edges in

an image carries more significant features than other smoothness parts. Edge detection is an image processing method to recognize the significant boundaries or contour features in an image where significant changes occur in color, intensity or texture [18]. Several edge detection methods are available, e.g. Prewitt, Sobel, Canny, etc., each employs different techniques to generate an edge map in a digital image.

An edge based encryption scheme was presented by [47] by applying CNN edge detection for further segmentation. In the scheme, the significant blocks are performed using reversible hidden transform followed by multiple-order discrete fractional cosine transform which are encrypted using a two-dimensional chaotic map. A further edge based selective encryption scheme for medical images was presented by [5]. The scheme was structured from three parts including bit-plane decomposition, generator of chaotic, random sequence, and permutation method that change both positions of the bits and values of pixels. The authors [49] introduced a scheme to partially encrypt obtained an edge map of medical images using an algorithm structured from multiple processes using XOR operation, random bit sequence generation for edge map encryption, and bit-plane shuffling process. The authors [27] proposed a novel lightweight privacy preserving technique based on deep learning model for object detection. The author re-design an existing protocol of the mathematical functions with CORDIC algorithm. After providing a set of training and testing of SecRCNN, they can extract the features, region proposal and classifying the images. Although the approach is reliable and preserve the privacy of the image, it requires a high computational complexity for training and testing.

One Time Pad (OTP) is a mathematical approach that is used in the encryption domain. The main idea of the OTP is to encrypt each plaintext in a unique key. OTP is an optimal cipher, since it is very solid to discover a connection between two cipher images. Theoretically, OTP encryption approach cannot be cracked since deriving the used key for encryption is a very complicated task and depends on the volume of the plaintext [3].

However, some of these selective encryption schemes suffer from drawbacks, such as the inability to achieve high randomness for encrypted image parts, further they did not provide security analysis for their proposed methods. Moreover, very few of these schemes have provided a time-complexity analysis or proved the performance efficiency of their proposed algorithms. Where the inappropriate combination between selection and encryption of significant image data may lead to a computational cost similar to that of full encryption. On the other hand, as a key space is a crucial characteristic for any encryption, some schemes use a short key space for encrypting the selected image data. This consequently means the plain image can be easily recovered via a brute force attack in a reasonable period of time. Based on the aforementioned issues, this work consists of the primarily motivations to adequately resolve the issues in the proposed scheme.

3 Proposed scheme

The proposed scheme mainly consists of three major steps. In the first step, the medical image is decomposed into non-overlapping blocks of pixels of specified size. Then, a low cost edge detection algorithm is used to recognize the significant image blocks,

with a certain threshold value. In the second step, a chaotic map is used to generate a matrix of random keys equal to the obtained significant blocks in an image. In the last step, the identified significant blocks are encrypted in sequence using a one-time pad algorithm. Each significant block is encrypted using a unique encryption key, where the non-significant blocks are left without encryption. The block diagram of our proposed scheme is illustrated in Fig. 1.

3.1 Edge detection

In the proposed scheme, we apply the Prewitt edge detection method [33] for detecting significant edge maps in medical images using a certain threshold value. Prewitt detector has a simple implementation, inexpensive computational cost, and accurate in estimating the edge positions in digital images [18].

Prewitt operator is a discrete differentiation operator that is constructed on the gradient or decisive the first-direction imitative of the original image pixel. The routine of Prewitt stretches the orientation and magnitude of the edge in the image. The steps of Prewitt method are abridged as follows:

The two 3×3 convolution kernels Q_x and Q_y convolved with the original image (i) (Eq. 1). Q_x and Q_y are horizontally and vertically decomposed images at each point. Q_x and Q_y are computed by the following machinist:

$$Q_x = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} * i \quad Q_y = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} * i \quad (1)$$

$$i(f'_x(x, y)) = f(x+1, y-1) - f(x-1, y-1) + f(x+1, y) - f(x-1, y) + f(x+1, y+1) - f(x-1, y+1)$$

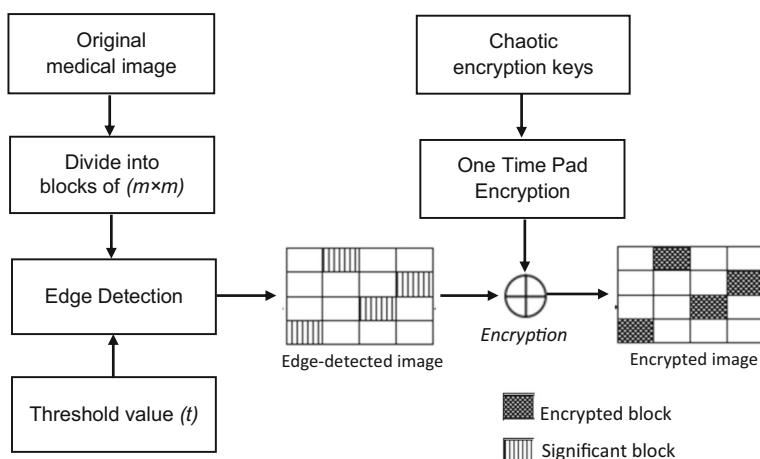


Fig. 1 Block diagram for edge-based medical image encryption

$$i(f'_y(x, y)) = f(x-1, y+1) - f(x-1, y-1) + f(x, y+1) - f(x, y-1) \\ + f(x+1, y+1) - f(x+1, y-1)$$

$$Q[f(x, y)] = \sqrt{f'^2_x(x, y) + f'^2_y(x, y)}$$

Typically, an approximate magnitude is figured by using Eq. 2:

$$|Q| = |Q_x| + |Q_y| \quad (2)$$

Moreover, the angle of orientation (θ) of edge is specified by the following Eq. 3:

$$\theta = \tan^{-1} \left(\frac{Q_x}{Q_y} \right) \quad (3)$$

Figure 2 illustrates the output of (Q) and the original medical image (i) acquired by a Prewitt edge detection method.

Following are the steps being followed for edge detection mechanism in the proposed scheme:

1. The original medical image is initially divided into non-overlapping blocks of size $m \times m$, where (M) is the total number of blocks in the image (i).
2. Count the total number of pixels (P) in each detected block (B_{ij}) and then calculate its corresponding significant degree (S) using $S_{ij} = P_{ij} / M$, where B_{ij} is the coordinate location of the block in the detected image.
3. Set the threshold value (t), ($0 \leq t \leq 1$). For each block B_{ij} , when $S_{ij} \geq t$, it indicates that the corresponding block is significant, whereas, on the contrary, the block is insignificant (i.e., $S_{ij} < t$).
4. A binary index array of size $1 \times M$ is used to indicate the index of blocks in the image. The element '1' reflects the corresponding block is significant, whereas '0' reflects a non-significant block.

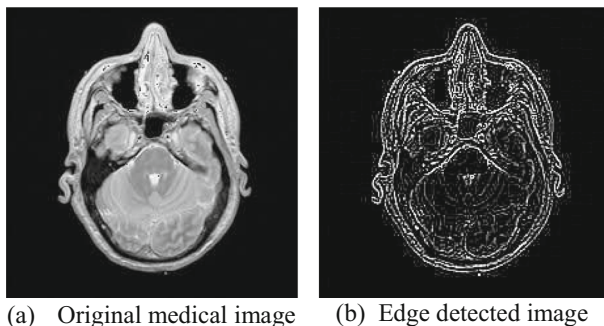


Fig. 2 Edge map output using Prewitt detector

- Finally, all significant blocks are encrypted in sequence, which are then used to replace the original blocks in the same corresponding positions and thus obtaining the encrypted medical image (C).

3.2 Key generation

The key space of any chaos-based cryptosystem must be large enough to resist various attacks. In this approach, we stratify the chaotic map in order to generate the key space (Eqs. 4 and 5), whereas the key size is equal to the obtained blocks.

$$Ks_1 = \alpha, \quad \alpha \in \mathbb{R}, \alpha \neq 0 \quad (4)$$

$$Ks_q = \sum_{q=2}^{q \leq \vec{\pi}} \left[\left(\left| \lambda^{-Ks_{q-1}} \right| / \left| \lambda^{-\left(q(Ks_{q-1}) \right)} \right| \right) \right] \quad (5)$$

$$\{2, \dots, n\} \leftarrow q \in \mathbb{R}, n \leq \vec{\pi}$$

$$\forall Ks_{q \pm 1} \neq Ks_q$$

Where Ks_1 is the initial key, Ks_q is the key space, α is a constant, λ is a security factor, π_1, \dots, π_n is the original obtained pixels.

Previous steps (Eqs. 4 and 5) provide a key with same obtained blocks size in term of security stricture λ . Our chaotic map provides a unique and non-duplicated key for each pixel in the obtained blocks. In addition, there is a strong correlation between key values, since the current key depends on the previous key and all keys are associated with the primary (initial) key (Ks_1). Any slight change in the first key (Ks_1) will occur an extremely effective for the whole key maps and its behaviors, which is really stretching indicators to detect any tamper happened during the key generation.

3.3 Encryption technique

After key generation, we encrypt the plaintext based on one time pad principle “6”. We use modular arithmetic in order to realize and achieve OTP conditions. Moreover, we generate a secret key during the encryption process, this key is used during the decryption phase in order to increase the security level and to prove the authentic of the key space during the decryption Pr_{kq} is generated in this step 7.

$$en_k = \sum_{q=1}^{q \leq \vec{\pi}} (Ks_q(\lambda) + \pi_k) \bmod \varphi \quad (6)$$

Where en_k is the encrypted blocks image of the index k , φ is a modulo base $\varphi \in \mathbb{Z}$, $0 \leq \gamma < \varphi$.

$$Pr_{kq} = \left[\sum_{q=1}^{\overrightarrow{\pi}} (Ks_q + \pi_k) / \varphi \right] \quad (7)$$

The main condition in an OTP method is to encrypt each plaintext with a unique key. Our equation is using the generated key which is based on chaotic map, consequently, each pixel in a block will encrypt with an exclusive key. Moreover, we use a modular base of 255 where the encryption results motionless in the image range.

3.4 Decryption technique

In the decryption process, the authorized user can decrypt the cipher images and retrieve the original image, which requires the key space and the security key. Besides, the decryption process is based on the reversible OTP equations of our approach.

We decrypt the data based on one time pad and the key generated in the encryption process as present in Eq. 8. We use the key space (Ks_q) and the security key (Pr_k), which are generated through the encryption phase. de_k denotes the decrypted blocks of the index k .

$$de_k = \left[\sum_{i=1}^{\overrightarrow{de}} (en_k - Ks_q * \lambda) + Pr_k * \varphi \right] \bmod \varphi \quad (8)$$

4 Experimental results

In this section, our experimental results are presented to validate the important features of the provided approach. These features comprise of robustness to noise and compressive sensing with high peak-to-signal-noise ratio (PSNR) of decrypted result. We have implemented our approach on a set of 8 bit/pixel gray scale images of size 225×225 and using a block of size 3×3 . We have also implemented the approach with a security parameter $\lambda = 12$.

4.1 Edge-based encryption results

Figure 3 shows the edge based encryption output for the used test images. In fact, the number of detected blocks in an image is directly related to the used threshold value (t). Decreasing t value will increase the number of detected blocks for encryption, whereas the number of detected blocks approaches zero when t is reaching one. In this scheme, we found that when $t = 0.12$, most of significant pixels in all the images we used can be detected with an acceptable percentage of encrypted image data and low encryption time. Therefore, we chose the default value $t = 0.12$ in all our conducted experiments. Table 1 shows the correlation between changing the t value and the percentage of detected pixels for encrypting the Head image of size 225×225 and using a block of size 3×3 .

The experimental results portray that our partially encrypted images do not disclose any momentous information about the original image. The results also indicate that the percentage

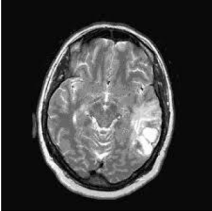
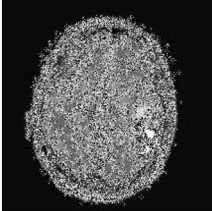
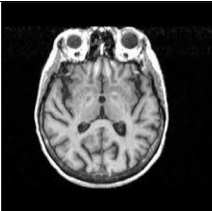
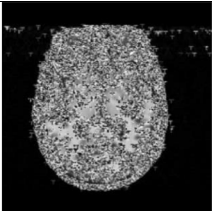
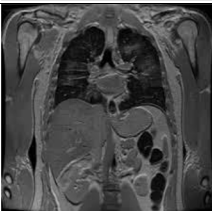
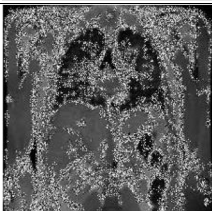

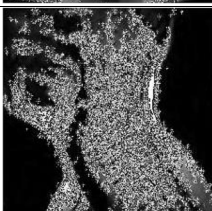

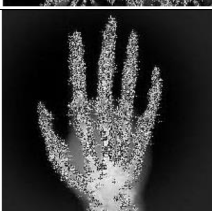

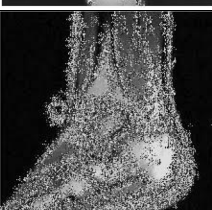
| Image name | (a) Original image | | (b) Encrypted image | |
|------------|---|--|---|--|
| Brain |  | |  | |
| Head |  | |  | |
| Chest |  | |  | |
| Neck |  | |  | |
| Hand |  | |  | |
| Leg |  | |  | |

Fig. 3 Edge-based encryption results (a) Original plain images, (b) Partially encrypted images

of the encrypted area did not exceed 47% of the size of the original test images. Thus, the selective encryption approach can provide a low computational complexity because the encryption operation is realized on the smallest and most significant volume of data.

Table 1 Percentage of detected pixels when changing the value of (t) for encrypting the Head image of size 225×225 using a blok of size 3×3

| Threshold value (t) | Percentage of detected pixels |
|-------------------------|-------------------------------|
| 0.05 | 41.57% |
| 0.10 | 35.53% |
| 0.15 | 30.59% |
| 0.20 | 24.78% |
| 0.30 | 13.02% |

4.2 Transparency and robustness to attacks

Transparency measures the degradation of the retrieved image quality after applying the encryption and decryption processes. The optimal approach should provide a less degradation results. In order to improve the robustness factor in our approach, we applied different geometric and non-geometric attacks. The cipher images are attacked using Stirmark Benchmark [37]. At the receiver side, the user can decrypt the attacked encrypted image using the proposed approach. In order to prove the robustness of our approach, we have applied different kinds of attacks to the encrypted image. These attacks are geometrical transformation attacks such as Affine of factor 3, JPEG compression ratio of 60% degree, adding filtration of factor 7, adding noise with 60 degree and rotation the image with 45 degree as described in Table 2, then we decrypted the attacked encrypted image. The quality of the decrypted images is measured using Peak Signal to Noise Ratio (PSNR) [10], Normalize Cross Correlations (NCC) [11] and SSIM [41].

Figure 4 presents the attacked encrypted image under several kinds of geometric and non-geometric attacks, in addition to the corresponding values of PSNR, SIM and NCC. PSNR, SSIM and NCC measure the quality of retrieved images, and show how much the effect of the approach on the degradation of the quality of the retrieved images. Higher PSNR means lower distortion and better image quality.

Typically, the image quality is acceptable if the PSNR is larger than 34 dB. When the PSNR is greater than or equal to 40 dB, it indicates that the two images are virtually indistinguishable by human observers. For SSIM and NCC, a closer value to 1 means high similarity between compared images, while a value closer to 0 meaning they are completely different [22].

According to our results, in case of no attacks, we achieved PSNR around 50 in most images, while SSIM and NCC, the values were very close to 1. In case of the attacks, the mean value of PSNR is equal to 39.84 dB, while the values of SSIM and NCC are greater than 0.82 in the least cases.

We have compared the PSNR, SSIM, and NCC average results of our scheme with other related encryption schemes reported in [4, 8, 20, 29, 36]. Table 3 shows the PSNR, SSIM and

Table 2 The applied attacks

| Attack type | Factor |
|---------------------|------------|
| Affine | 3 |
| Compression (JPEG) | 60% |
| Filtration (Median) | 7 |
| Noise | 60 |
| Rotation | 45 degrees |

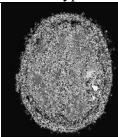
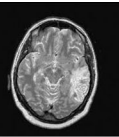
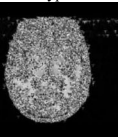
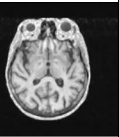
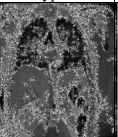

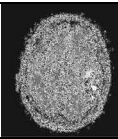
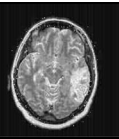
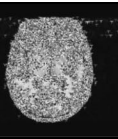

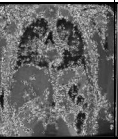
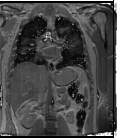
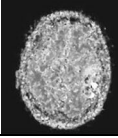
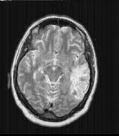
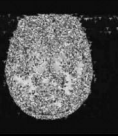

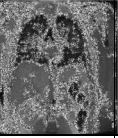

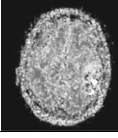
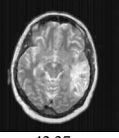
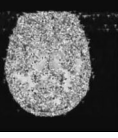
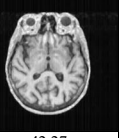
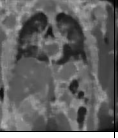

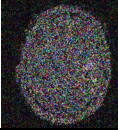
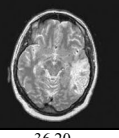
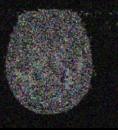
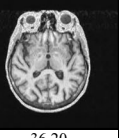
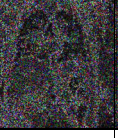
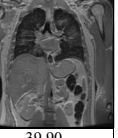
| Attack type | Attacked Encrypted | Decrypted | Attacked Encrypted | Decrypted | Attacked Encrypted | Decrypted |
|-------------|--|--|--|--|--|---|
| No attack |  |  |  |  |  |  |
| PSNR | | 58.35 | | 57.89 | | 48.50 |
| SSIM | | 0.993 | | 0.997 | | 0.974 |
| NCC | | 0.982 | | 0.998 | | 0.959 |
| Affine |  |  |  |  |  |  |
| PSNR | | 43.28 | | 45.26 | | 37.29 |
| SSIM | | 0.895 | | 0.914 | | 0.875 |
| NCC | | 0.961 | | 0.957 | | 0.937 |
| JPEG |  |  |  |  |  |  |
| PSNR | | 34.62 | | 39.29 | | 42.29 |
| SSIM | | 0.773 | | 0.845 | | 0.947 |
| NCC | | 0.950 | | 0.965 | | 0.943 |
| Median |  |  |  |  |  |  |
| PSNR | | 42.27 | | 42.27 | | 42.27 |
| SSIM | | 0.929 | | 0.913 | | 0.957 |
| NCC | | 0.962 | | 0.965 | | 0.943 |
| Noise |  |  |  |  |  |  |
| PSNR | | 36.20 | | 36.20 | | 39.90 |
| SSIM | | 0.873 | | 0.902 | | 0.896 |
| NCC | | 0.965 | | 0.987 | | 0.959 |

Fig. 4 The attacked encrypted images, and the decrypted images under several attacks with the corresponding values of PSNR, SSIM and NCC

NCC comparison results. The results demonstrate that the PSNR is higher than other schemes, which thus indicates a lower degradation and the reconstructed images are similar to the original ones. On the other hand, the high SSIM and NCC values of our scheme indicate that the original and the cipher images are approximately the same. It is also evident through the results that the proposed approach provides a high retrieved image quality without attacks (Transparency), and the approach is robust against several kinds of attacks.

4.3 Security and cryptanalysis

For any lightweight cryptographic approach, the cryptanalysis should be performed to prove the security aspect. Cryptanalysis aids to distinguish the correlation between the original image, key and encrypted image. It, moreover, targets to provide some details about the key

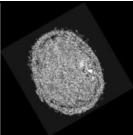
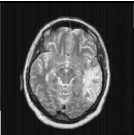
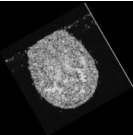
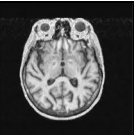
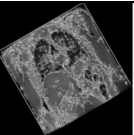
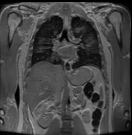
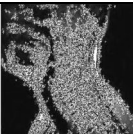

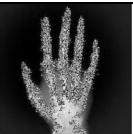

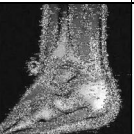

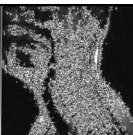

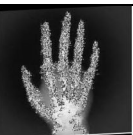

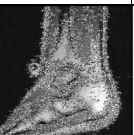

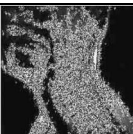



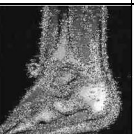

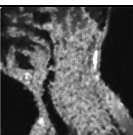

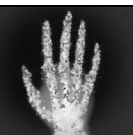

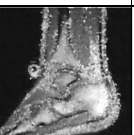





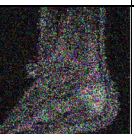

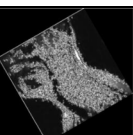

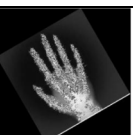

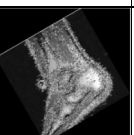

| | | | | | | |
|-----------|---|---|---|---|---|--|
| Rotation |  |  |  |  |  |  |
| PSNR | | 46.21 | | 35.75 | | 36.84 |
| SSIM | | 0.926 | | 0.959 | | 0.847 |
| NCC | | 0.956 | | 0.878 | | 0.946 |
| No attack |  |  |  |  |  |  |
| PSNR | | 54.02 | | 59.11 | | 53.28 |
| SSIM | | 0.945 | | 0.993 | | 0.995 |
| NCC | | 0.982 | | 0.986 | | 0.997 |
| Affine |  |  |  |  |  |  |
| PSNR | | 33.13 | | 39.36 | | 44.62 |
| SSIM | | 0.850 | | 0.954 | | 0.854 |
| NCC | | 0.936 | | 0.955 | | 0.950 |
| JPEG |  |  |  |  |  |  |
| PSNR | | 32.31 | | 32.27 | | 32.27 |
| SSIM | | 0.840 | | 0.895 | | 0.915 |
| NCC | | 0.908 | | 0.908 | | 0.931 |
| Median |  |  |  |  |  |  |
| PSNR | | 42.27 | | 39.27 | | 32.27 |
| SSIM | | 0.934 | | 0.909 | | 0.935 |
| NCC | | 0.959 | | 0.959 | | 0.962 |
| Noise |  |  |  |  |  |  |
| PSNR | | 36.44 | | 36.42 | | 36.07 |
| SSIM | | 0.897 | | 0.814 | | 0.818 |
| NCC | | 0.925 | | 0.864 | | 0.926 |
| Rotation |  |  |  |  |  |  |
| PSNR | | 39.59 | | 35.92 | | 36.28 |
| SSIM | | 0.892 | | 0.806 | | 0.871 |
| NCC | | 0.965 | | 0.821 | | 0.882 |

Fig. 4 continued.

Table 3 Comparison of PSNR, SSIM and NCC results between proposed and existing schemes

| Scheme | PSNR (dB) | SSIM | NCC |
|----------|-----------|--------|--------|
| Proposed | 49.843 | 0.961 | 0.959 |
| [29] | 22.425 | NA | NA |
| [4] | 11.231 | 0.0375 | 0.0296 |
| [20] | 11.169 | 0.0303 | 0.0301 |
| [36] | 9.083 | NA | NA |
| [8] | 31,025 | 0.987 | NA |

or encrypted image or both. A security assessment of an image encryption approach is one of the most significant matters, which must be patterned carefully. An encryption algorithm should resist against differential and statistical attacks.

4.3.1 Key space analysis

The critical aspect in any cryptographic approach determines the strength of an image encryption key space. The brute force attack is not possible if a cryptosystem has a superior key space. Fundamentally, all chaotic techniques are subtle to preliminary conditions which ensure developed security for an image encryption approach.

Firstly, we need to prove the chaotic sequence generation equations that were proposed. We intend to verify that the generated sequence is indeed a chaotic one. There are a lot of tests available in the literature to help this evident, such as calculating the Lyapunov exponents [44], plotting a histogram [43], random binary matrix rank test, Lempel-Ziv complexity test, etc. In the response, Lyapunov exponents with some statistical tests are performed.

We calculated Lyapunov exponents with Matlab. In case of Lambda is 0.99, the maximal Lyapunov exponent MLE is 0.0205. While, if Lambda is 0.2, MLE is 0.0161. The results of the generated key distribution are presented in Fig. 5. We can note that according to Lyapunov exponent statistical analysis, our equations provide a chaotic sequence.

In any chaotic approach, if the key space has exceeded 2100, the approach is considered secure [26]. Meanwhile, the secret key constraints in our proposed scheme in each repetition

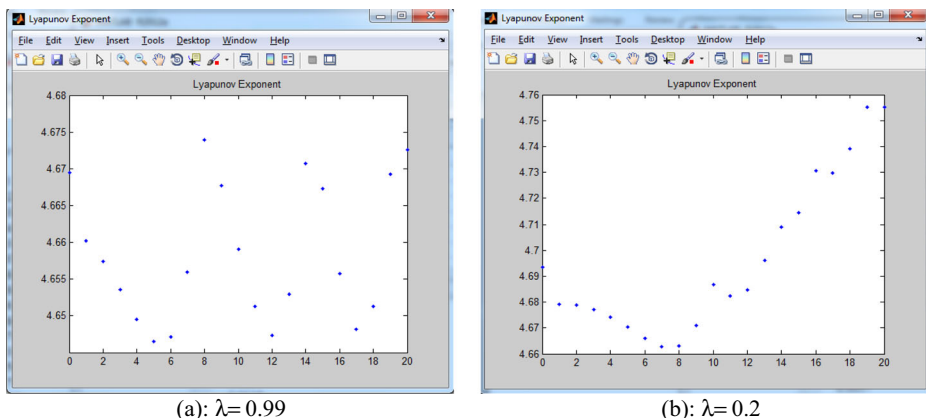
**Fig. 5** Lyapunov exponent in case of (a): $\lambda = 0.99$, and (b): $\lambda = 0.2$

Table 4 NPCR and UACI results

| Image | NPCR % | UACI % |
|-------|--------|--------|
| Brain | 99.19 | 32.62 |
| Head | 99.28 | 32.66 |
| Chest | 99.06 | 32.59 |
| Neck | 99.15 | 32.55 |
| Hand | 99.24 | 32.71 |
| Leg | 99.10 | 32.65 |

(λ) and in case of blocks of size 3×3 are about 160,000. Even for a single iteration and a fixed size, the key space is sufficiently satisfactory to battle all kinds of brute force attack.

4.3.2 Differential attack analysis

The utmost common attack on block ciphers is a differential cryptanalysis, which is presented in details in the work of [45]. After that, an important research has been approved to demonstrate their link and to improve explanations to thwart them [6]. The research presented by [12] is considered as the most influential and characteristic approach for attaining a security guaranteed with deference to this attack.

Differential cryptanalysis is a technique that examines the outcome of certain differences in plain couples on the differences of the resultant cipher couples. These differences are used to give possibilities to the potential keys and to discover the most feasible key. Normally, the approach works on several couples of the plain with the same particular difference using only the resultant cipher couples.

In our approach, we firstly study the entire cryptosystem using the differential cryptanalysis. Further, we consider a process that generates the key with different values of Lambda (λ). Then, we encrypt the image using these values. Following that, we apply a fixed XORed value to the pair of the plain and ciphered images.

Suppose the images are im_1 and im_2 , respectively, while the difference between the plain images is Δim . Further, these two images are measured by using XOR operation. $\Delta im = im_1 \oplus im_2$. Then, we converted these images into cipher images based on our approach, where the difference between these two cipher images en_1 and en_2 is represented as Δen . $\Delta en = en_1 \oplus en_2$. The couple (Δim , Δen) present the differential characteristics. Moreover, the difference between the pair of the plain images is projected to be a greater value as likened to average probability.

However, in order to evaluate the effect of a minor modification of the plain image on its cipher image and to analyze the differential attack, the number of pixel change rate (NPCR) and the unified averaged changing intensity (UACI) [45] are computed.

Table 4 shows the NPCR and UACI results for our cryptographic approach. As can be seen from the results, the NPCR between original and cipher images is greater than 99%, which

Table 5 Comparison of NPCR and UACI results between proposed and existing schemes

| Scheme | NPCR % | UACI % |
|-----------|--------|--------|
| Proposed | 99.017 | 32.630 |
| [36] | 98.972 | 32.183 |
| (ur [34]) | 99.612 | 29.077 |
| [8] | 99.504 | 33.122 |

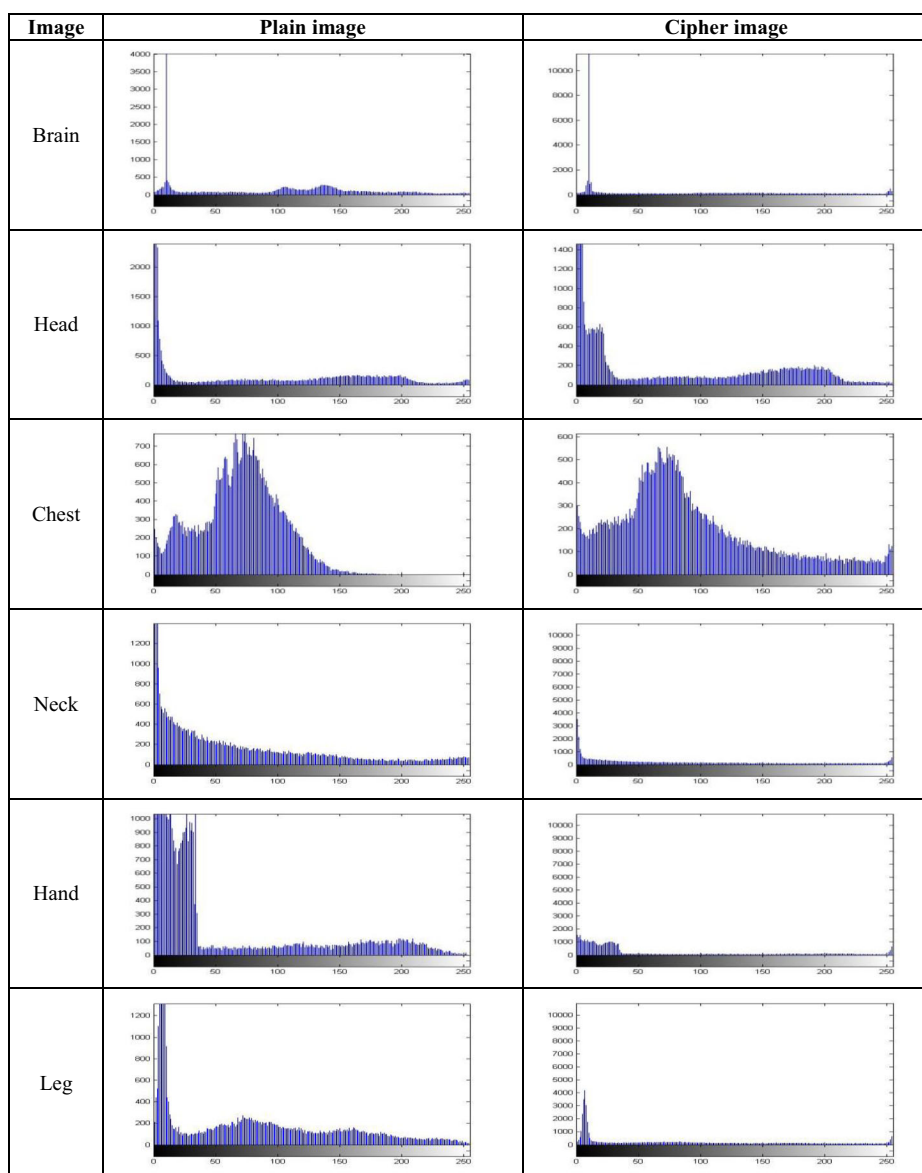


Fig. 6 Plain and Cipher images Histogram

Table 6 Correlation Coefficient values of the encrypted images

| Image | Correlation Coefficient |
|-------|-------------------------|
| Brain | - 0.5203 |
| Head | - 0.6463 |
| Chest | - 0.0763 |
| Neck | - 0.3476 |
| Hand | - 0.1812 |
| Leg | - 0.3741 |

indicates that the pixels positions have been randomly changed. The closer NPCR value to 100%, the more sensitive the cryptosystem is to the changing of the plain image. On the other hand, we obtained UACI results greater than 32%, which means that the intensity values of pixels for the encrypted images have been changed from their values in original images.

A comparison has been made with the results of the earlier works reported in ([36]; [8, 34]). Table 5 shows the mean of NPCR and UACI results of our scheme compared to those of related schemes. In an ideal cryptosystem, the NPCR and UACI values should be large enough and greater than 99% and 33%, respectively [45]. The mean values of NPCR and UACI for our scheme are equal to 99.017%, and 32.63, respectively, and slightly higher than the ones of other schemes. This ensures that the proposed encryption scheme can resist differential attack effectively.

4.4 Statistical attack analysis

Normally, the attacker tries to find any related information to the plain image by applying statistical attacks on the cipher image. Thus, the image encryption approach must be hardy to all types of these kinds of statistical attacks. To demonstrate the security in contradiction of statistical attacks, we are presenting histogram analysis and correlation analysis.

4.4.1 Histogram analysis

In order to improve the security aspect for any encryption approach, the histogram of the cipher image should be different from the original (plain) image. Moreover, the histogram of the cipher image should not reveal any information about the plaintext image. Results of histogram analysis for our encryption are shown in Fig. 6.

Although our approach is a partial encryption scheme and around 47% of a plain image is encrypted, it is clear from the plots in Fig. 6 that the histogram of the cipher images approximates the Gaussian distribution. These results indicate that the encrypted histogram hide the frequency distribution of plain image.

4.4.2 Correlation analysis

Correlation among adjacent pixels is an inherent aspect of a plain image. Normally, weak correlation standards are obligatory. From Table 6, which presents the correlation coefficient values of the encrypted images, we note that the encrypted images have a smaller amount of correlation.

Table 7 The selective encryption and decryption time for test medical images

| Image | Encrypted data (%) | Detection time (sec) | Total selective encryption time (sec) | Total selective decryption time (sec) |
|-------|--------------------|----------------------|---------------------------------------|---------------------------------------|
| Brain | 38.5 | 0.02374 | 0.06861 | 0.04256 |
| Head | 30.6 | 0.02106 | 0.06253 | 0.04076 |
| Chest | 48.2 | 0.02914 | 0.08116 | 0.05671 |
| Neck | 46.8 | 0.02783 | 0.07845 | 0.05259 |
| Hand | 17.8 | 0.01307 | 0.04079 | 0.02767 |
| Leg | 41.3 | 0.02586 | 0.07002 | 0.04799 |

Table 8 Comparison of selective encryption time between proposed and some existing schemes

| Schemes | Encryption time (sec) |
|----------|-----------------------|
| Proposed | 0.0669 |
| [18] | 0.1314 |
| [34] | 2.1700 |
| [40] | 2.8077 |
| [36] | 0.4943 |
| [8] | 0.202 |

4.5 Computational time analysis

Several experiments were performed to measure the execution time for edge-based encryption and decryption processes. The experiments were conducted on Intel Core i5-2430M CPU (2.4 GHz), and 4 GB of RAM, and Windows 7 (32-bit version), using Matlab R2017 programming language. Table 7 shows the computational selective encryption and decryption time of various test images. Total selective encryption time involves the time required to detect the edges of an image, the time required to generate the key space, and the time required to transform the plain blocks into ciphertext blocks. The average elapsed time for the edge detection process was about 0.02326 s. Selective decryption is the reverse process and its time involves the time of retrieving the encrypted blocks followed by decryption using the same key space.

In Table 8, the average selective encryption time of the proposed scheme is compared with the selective encryption time of those reported in ([18]; [8, 34, 36, 40]) for images of size 225×225 . It is observed that the average encryption time of our proposed scheme is significantly less compared to the schemes depicted in Table 8. This is due to that the image encryption in our scheme is performed in pixel level, while some other schemes encrypt image in bit level. Hence, the encryption time only corresponds to the detected significant pixels in an image and irrelevant to the number of bits representing the pixel. Besides, the computation complexity and time consumption of encryption algorithm, chaotic and encryption variables for encrypting one pixel is significantly lower than some other methods which perform encryption in rounds and require much computation time. Our approach is a single round encryption scheme that leads to high encryption speed with less computations.

5 Conclusion

In this paper, we introduced a selective encryption scheme that encrypts digital medical images partially. The scheme is based on edge detection which is used to determine the edge map from an image. Then, the original image is divided into non-overlapping blocks of pixels, where the blocks that include the optimal position of pixels, based on a threshold value, will be considered for encryption process. The proposed scheme presents a large key space where different keys are used for detected blocks, which are generated using a chaotic map. To perform encryption, a one-time pad algorithm is used to encrypt the significant image blocks. Several experiments were carried out on multiple test images to prove the robustness and efficiency of the proposed encryption scheme. The security analysis and performance evaluation show that the proposed approach can achieve high security level and less computation complexity, which make the scheme feasible for image encryption in real time applications.

As a future work, the proposed technique will be implemented and evaluated in realistic real-time medical and IoT scenarios. A further research will be carried out to improve the security and performance of the proposed technique using intelligent cryptography.

References

1. Abdmouleh, MK, Khalfallah, A, and Bouhlef, MS (2017). A novel selective encryption dwt-based algorithm for medical images. In *2017 14th International Conference on Computer Graphics, Imaging and Visualization*, pages 79–84. IEEE
2. Akkasaligar PT, Biradar S (2020) Selective medical image encryption using dna cryptography. *Information Security Journal: A Global Perspective* 29(2):91–101
3. AlShaikh M, Laouamer L, Nana L, Pascu AC (2017) Efficient and robust encryption and watermarking technique based on a new chaotic map approach. *Multimed Tools Appl* 76(6):8937–8950
4. Bhatnagar G, Wu QJ (2012) Selective image encryption based on pixels of interest and singular value decomposition. *Digital signal processing* 22(4):648–663
5. Cao W, Zhou Y, Chen CP, Xia L (2017) Medical image encryption using edge maps. *Signal Process* 132:96–109
6. Chabaud F, Vaudenay S (1994) Links between differential and linear cryptanalysis. In: *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, pp 356–365
7. Chen L, Wang S (2015) Differential cryptanalysis of a medical image cryptosystem with multiple rounds. *Comput Biol Med* 65:69–75
8. Darwish SM (2019) A modified image selective encryption-compression technique based on 3d chaotic maps and arithmetic coding. *Multimed Tools Appl* 78(14):19229–19252
9. Hua Z, Zhou Y, Huang H (2019) Cosine-transform-based chaotic system for image encryption. *Inf Sci* 480: 403–419
10. Huynh-Thu Q, Ghanbari M (2008) Scope of validity of psnr in image/video quality assessment. *Electron Lett* 44(13):800–801
11. Jain B, Taylor A (2003) Cross-correlation tomography: measuring dark energy evolution with weak lensing. *Phys Rev Lett* 91(14):141302
12. Juels A, Weis SA (2005) Authenticating pervasive devices with human protocols. In: *Annual international cryptology conference*. Springer, pp 293–308
13. Kar M, Kumar A, Nandi D, Mandal M (2020) Image encryption using dna coding and hyperchaotic system. *IETE Tech Rev* 37(1):12–23
14. Khan JS, Ahmad J (2019) Chaos based efficient selective image encryption. *Multimed Syst Sign Process* 30(2):943–961
15. Khan MA, Ahmad J, Javaid Q, Saqib NA (2017) An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. *J Mod Opt* 64(5):531–540
16. Khashan OA, Khafajah NM (2018) Secure stored images using transparent crypto filter driver. *IJ Network Security* 20(6):1053–1060
17. Khashan OA, Zin AM (2013) An efficient adaptive of transparent spatial digital image encryption. *Procedia technology* 11:288–297
18. Khashan OA, Zin AM, Sundararajan EA (2014) Performance study of selective encryption in comparison to full encryption for still visual images. *Journal of Zhejiang University SCIENCE C* 15(6):435–444
19. Khashan OA, Zin AM, Sundararajan EA (2015) Imgfs: a transparent cryptography for stored images using a filesystem in userspace. *Frontiers of Information Technology & Electronic Engineering* 16(1):28–42
20. Krishnamoorthi R, Murali P (2017) A selective image encryption based on square-wave shifting with orthogonal polynomials transformation suitable for mobile devices. *Multimed Tools Appl* 76(1):1217–1246
21. Kulsoom A, Xiao D, Abbas SA et al (2016) An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and dna complementary rules. *Multimed Tools Appl* 75(1):1–23
22. Laouamer L, AlShaikh M, Nana L, Pascu AC (2015) Robust watermarking scheme and tamper detection based on threshold versus intensity. *Journal of Innovation in Digital Ecosystems* 2(1–2):1–12
23. Leng L, Li M, Kim C, Bi X (2017) Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. *Multimed Tools Appl* 76(1):333–354
24. Li C, Lin D, Feng B, Lu J, Hao F (2018) Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *IEEE Access* 6:75834–75842
25. Liao X, Yin J, Guo S, Li X, Sangaiah AK (2018) Medical jpeg image steganography based on preserving inter-block dependencies. *Comput Electr Eng* 67:320–329

26. Liu H, Wang X, Kadir A (2012) Image encryption using dna complementary rule and chaotic maps. *Appl Soft Comput* 12(5):1457–1466
27. Liu, Y, Ma, Z, Liu, X, Ma, S, and Ren, K (2019). Privacy-preserving object detection for medical images with faster r-cnn. *IEEE Trans Inf Forensics Secur*, 1
28. Mou, J, Yang, F, Chu, R, and Cao, Y (2019). Image compression and encryption algorithm based on hyper-chaotic map. *Mobile Networks and Applications*, pages 1–13
29. Moumen A, Bouye M, Sissaoui H (2015) New secure partial encryption method for medical images using graph coloring problem. *Nonlinear Dynamics* 82(3):1475–1482
30. Noura M, Noura H, Chehab A, Mansour MM, Sleem L, Couturier R (2018) A dynamic approach for a lightweight and secure cipher for medical images. *Multimed Tools Appl* 77(23):31397–31426
31. Pavithra, V and Chandrasekaran, J. (2020). Developing security solutions for telemedicine applications: medical image encryption and watermarking. In *Smart Medical Data Sensing and IoT Systems Design in Healthcare*, pages 76–96. IGI Global
32. Prabhu P, Manjunath K (2019) Secured transmission of medical images in radiology using aes technique. In: *Computer Aided Intervention and Diagnostics in Clinical and Medical Images*. Springer, pp 103–112
33. Prewitt JM (1970) Object enhancement and extraction. *Picture processing and Psychopictorics* 10(1):15–19
34. Rehman A u, Liao X, Kulsom A, Abbas SA (2015) Selective encryption for gray images based on chaos and dna complementary rules. *Multimed Tools Appl* 74(13):4655–4677
35. Riad K, Hamza R, Yan H (2019) Sensitive and energetic iot access control for managing cloud electronic health records. *IEEE Access* 7:86384–86393
36. Som S, Mitra A, Palit S, Chaudhuri B (2019) A selective bitplane image encryption scheme using chaotic maps. *Multimed Tools Appl* 78(8):10373–10400
37. Steinebach M, Petitcolas FA, Raynal F, Dittmann J, Fontaine C, Seibel S, Fates N, Ferri LC (2001) Stirmark benchmark: audio watermarking attacks. In: *Proceedings international conference on information technology: coding and computing*. IEEE, pp 49–54
38. Tang Z, Yang Y, Xu S, Yu C, Zhang X (2019) Image encryption with double spiral scans and chaotic maps. *Security and Communication Networks* 2019:1–15
39. Tong X, Zhang M, Wang Z (2015) A new image encryption algorithm based on the high-dimensional chaotic map. *The Imaging Science Journal* 63(5):263–272
40. Ullah I, Iqbal W, Masood A (2013) Selective region based images encryption. In: *2013 2nd National conference on information assurance (NCIA)*, pages 125–128. IEEE
41. Wang L-T, Hoover NE, Porter EH, Zasio JJ (1987) Ssim: a software leveled compiled-code simulator. In: *Proceedings of the 24th ACM/IEEE Design Automation Conference*, pages 2–8. ACM
42. Wen W, Zhang Y, Fang Z, Chen J-X (2015) Infrared targetbased selective encryption by chaotic maps. *Opt Commun* 341:131–139
43. Wilks DS (2011) *Statistical methods in the atmospheric sciences*, volume 100. Academic press
44. Wolf A, Swift JB, Swinney HL, Vastano JA (1985) Determining lyapunov exponents from a time series. *Physica D: Nonlinear Phenomena* 16(3):285–317
45. Wu Y, Noonan JP, Agaian S et al (2011) Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)* 1(2):31–38
46. Wu L, Xu Z, He D, Wang X (2018) New certi_cateless aggregate signature scheme for healthcare multimedia social network on cloud environment. *Security and Communication Networks* 2018:1–13
47. Zhang Y, Xiao D, Wen W, Tian Y (2013) Edge-based lightweight image encryption using chaos-based reversible hidden transform and multipleorder discrete fractional cosine transform. *Opt Laser Technol* 54:1–6
48. Zhang L-B, Zhu Z-L, Yang B-Q, Liu W-Y, Zhu H-F, Zou M-Y (2015) Cryptanalysis and improvement of an e_cient and secure medical image protection scheme. *Math Probl Eng* 2015
49. Zhou Y, Panetta K, Agaian S (2009) A lossless encryption method for medical images using edge maps. In: *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 3707–3710. IEEE



Osama A. Khashan was born in Jordan, in 1983. He received the B.S. degree in computer science from Irbid National University, Jordan, in 2005, the M.S. degree in information technology from Utara University Malaysia, in 2008, and the Ph.D. degree in computer science from the National University of Malaysia, Malaysia, in 2014. He is currently working as an Assistant Professor with the College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia. His research works focus on information and network security, cryptology, watermarking, image processing, and performance analysis.



Muath AlShaikh has been a Ph.D. holder in Computer Science since 2016, University of Bretagne Occidentale, France. He received his Master degree in computer science in 2010 from Utara University in Malaysia and his B.Sc in computer science in 2006 from AlBalqa University, Jordan. He is affiliated to Lab-STICC / UMR CNRS 6283, SFIIS team of the University of Bretagne Occidentale, France. He has been an Assistant Professor with Computer Science Department, Saudi Electronic University, KSA. His research interests include Homomorphic, Cyber security, Watermarking, Cryptology, Information Security and Image processing and Computer vision.