# A dynamic approach for a lightweight and secure cipher for medical images

Mohamad Noura, Hassan Noura, Ali Chehab, Mohammad Mansour, Lama Sleem, Raphael Couturier

**Noname manuscript No.**
(will be inserted by the editor)

,

# A Dynamic Approach for a Lightweight and Secure Cipher for Medical Images

Mohammad Noura, Hassan Noura, Ali Chehab, Mohammad M. Mansour, Lama Sleem, Raphaël Couturier

the date of receipt and acceptance should be inserted later

**Abstract** Protecting the contents of medical records is of paramount importance when it comes to preserving patients' privacy. Most existing cryptographic-based solutions rely on traditional encryption algorithms having a multi-round structure, which introduces processing latency and requires increased resources. Medical images possess special characteristics compared to other types of images. The main goal of this paper is to leverage these characteristics to design and implement an efficient and secure encryption algorithm for such images. The proposed solution defines three variants of encryption algorithms: **(a) full, (b) middle-full, and (c) selective**. The full approach encrypts all sub-matrices of an image, while the middle-full variant is a middle solution between the selective and full algorithms and its goal is to just hide the type of the medical image. Selective encryption identifies a set of sub-matrices of an image according to a statistical average test, known as region of interest (ROI). In the three approaches, a high security level is ensured since each image is encrypted independently of the previous and next images. Also, all primitives of the proposed cipher, such as permutation and substitution, depend on a dynamic key. Furthermore, the encryption scheme is efficient since the proposed round function is lightweight and applied for only one round. This reduces the latency and the required resources as compared to traditional cryptographic schemes. The proposed approach is flexible as it can be applied in either selective, middle-full, or full mode. Also, the size of a sub-matrix is variable and can be changed according to the available memory size. Several security and performance tests are conducted to evaluate the effectiveness of the proposed solution. The results validate the robustness of the proposed scheme against almost all considered types of attacks and show an improvement in terms of latency and resources compared to current image-encryption schemes. Also, the results confirm the robustness of the proposed algorithm in protecting the contents of medical images.

**Keywords** Selective or partial encryption algorithm; Full encryption algorithm; Permutation and substitution primitives; Cryptographic analysis.

## 1 Introduction

Digital medical images are critical diagnostic tools. They are generated using a number of technologies and are mainly used for treating and predicting diseases. These technologies include X-ray radiography, ultrasound, magnetic resonance imaging (MRI), etc. There exists a number of applications which require storing and transmitting medical images across public channels such as the Internet and hence, making them vulnerable to security threats such as privacy, confidentiality, authentication, and integrity. Hospitals are hesitant to allow access to such sensitive data via their networks, and as such, there is a great need to secure such networks and enable them with the various security services, which mainly rely on cryptographic algorithms, to resist the various types of attacks (1; 2). The main security services include Data Confidentiality (DC), privacy, Data integrity (DI) and Source Authentication (SA). Encrypting an image protects its private contents from being accessed by an unauthorized party. This ensures DC and privacy during transmission or storage, which can solve the problems of passive attacks. Moreover, DI service is used to ensure that the received data has not been modified during transmission and SA permits to verify

[1]-FEMTO-ST Institute, Univ. Bourgogne Franche-Comté (UBFC), France
· [2]-American University of Beirut, Electrical and Computer Engineering, Beirut, Lebanon

the source of the image (3; 4). The traditional encryption schemes are based on symmetric key cryptography, which is efficient in terms of computational resources and latency when compared to asymmetric key cryptography (AKC). A symmetric cipher can be block or stream based; a block cipher divides the data into separate blocks of fixed size such as the Data Encryption Standard (DES) (5), the Advanced Encryption Standard (AES) (6) (128-bit length), the International Data Encryption Algorithm (IDEA) (7), etc.

### 1.1 Problem Definition

Recently, a set of medical image authentication schemes were presented in (8)-(13). While, in this paper, we focus to design an efficient and secure medical cipher image solution. In fact, The conventional encryption schemes that encrypt the whole plain image and not appropriate when executed on constrained devices and in the case of real-time medical applications over wireless medical networks and in mobile medical services. Recently, a selective image encryption approach was presented to overcome the existing issues of conventional encryption, whereby the insignificant parts are not encrypted, or encrypted using a light encryption method. Selective encryption reduces the computational complexity to the minimum possible level while preserving a sufficient security level. The selective approach is debatable since the most existing schemes are designed based on image compression algorithms, and thus they are codec-specific, while the rest are applied at the pixel level (14), (15)-(23). Recent research works presented a new kind of compression algorithms that are specific for encrypting image and video, and can ensure good performance such as (24)-(27). Therefore, we focus on this class since it provides more flexibility, being codec-independent.

In fact, the selective image encryption approach meets the requirements of real-time applications and tiny devices because a significant reduction of processing time for encryption and decryption is achieved. Different pixel selection techniques have been suggested in the literature such as edge maps (28), region of interest (ROI) (18), entropy-based techniques (29), and average of sub-matrices (30; 23).

Nonetheless, a number of approaches, based on conventional encryption schemes such as AES, has been proposed to protect medical records in the DICOM system (31) and in many other research papers (32)-(34). **However, traditional cryptographic algorithms are defined mainly to protect textual data**. Thus, they are not designed for encrypting multimedia contents and do not account for the intrinsic characteristics of multimedia such as (i) large data size, (ii) bulk data capacity, (iii) high redundancy and (iv) strong correlation between adjacent pixels. Therefore, a revision of the current encryption schemes should be done to propose new ones taking into account the application requirements.

Another paradigm that was investigated by researchers in the last decade is the "Chaos" field, which consists of a non-linear dynamic system that looks like random (35). Due to its extreme sensitivity to initial conditions, chaos was integrated extensively into the design of medical image encryption algorithms (28)-(30). Unfortunately, chaos-based encryption is not always secure; some of these approaches have security weaknesses and many of them have been crypt-analyzed successfully as in (41)-(47) due to the instability arising from the periodicity of mapping (48) and the finite computing precision that renders the system vulnerable to different kinds of attacks (49; 50). Additionally, the majority of chaotic encryption algorithms is based on non-integer operations, which introduces high resource requirements and computational complexity and consequently overhead in terms of efficiency and latency, especially that a floating-point system is much more expensive than an integer one. Accordingly, we recommend to revise the chaotic cryptographic algorithms and to discretize chaotic maps (integer) to replace the real ones (original form). This is mandatory to reduce the required resources and latency overhead and to simplify the hardware implementation and cost. Recently, an image encryption algorithm for medical images was presented in (30) but unfortunately, it suffers from the limitations of the chaotic paradigm.

It is worth mentioning that focusing on updating chaotic cryptographic algorithms and discretizing chaotic maps is justified since all traditional cryptographic algorithms are based on integer operations such as AES, which can be implemented using bytes or words of size 16 or 32 bits.

### 1.2 Contribution

In this paper, an efficient encryption scheme suitable for full and selective medical image encryption applications is proposed. It exhibits low processing latency and reduced resource requirements. Depending on the application, the scheme can be used for encrypting (i) the full plain image or (ii) part of the plain image

containing sensitive information. We propose to detect the sensitive regions (ROI) and the non-sensitive regions (ROB) in an image using a statistical approach based on the average of each sub-matrix, which should be greater or equal to a threshold that we obtain according to simulation results. Towards reducing the latency and the required resources, we propose a cipher scheme with a dynamic key that changes for each input image. The proposed scheme presents 4 variants for medical image encryption as shown below:

1. **Selective Encryption-1 (SE1):** this technique employs only a permutation of the sub-matrices of ROI. This variant requires the minimum computational complexity compared to the other variants. It is the best choice for real-time applications, and systems with constrained devices. However, this variant preserves the type of medical data;
2. **Selective Encryption-2 (SE2):** in addition to the permutation technique of SE1, SE2 consists also of a masking operation to the sub-matrices of ROI. As such, it provides a higher security level than SE1 because of the masking process, which is associated with a low overhead in terms of latency and resources;
3. **Middle-Full (MF):** this technique consists of masking the sub-matrices of ROI and permuting all the sub-matrices of a plain image (ROI and ROB). This variant is designed to hide the type of a medical image that is preserved using the previous selective variants, SE1 and SE2;
4. **Full approach:** this variant consists of masking and permuting all the sub-matrices of a plain image. It requires more overhead compared to the middle and selective variants and it is used to obscure all useful information for the encrypted medical image.

The common property among these variants is that they are all iterated for just one round and have a key-dependent structure. Moreover, the round function is based on a permutation table (P-box) and a substitution table (S-box) that are both dependent on a dynamic key and an initial matrix $IM$, which is introduced to enhance the statistical randomness of the proposed masking function. The dynamic key generation algorithm produces a key, which depends on a secret key and an Initial Vector (IV) and that should be changed for each input image to guard against cryptanalytic attacks. Additionally, the different steps of the cipher are variable and depend on this dynamic key in contrast to the existing solutions that employ a static cipher structure and require several rounds. The proposed technique reduces the number of rounds to just one since variable cipher primitives are applied to each input image and the desired randomness degree is attained. Consequently, this reduces the execution time while maintaining a high security level. Simulation results verify the high performance and the robustness against existing attacks. Note that the proposed scheme is easily applicable to other kinds of images that require selective and full encryption. The novelty of the proposed approach is that it is based on a dynamic approach, where the substitution and diffusion operations are variable and can be changed for each new input image. In addition, the proposed cipher only requires one round and its round function is very lightweight compared to the existing solutions such as 3DES and AES.

### 1.3 Organization

The paper is organized as follows: Section 2 describes the statistical approach for the selection of the ROI. Section 3 gives a detailed look on the key derivation used in this model. Then, detailed description of the proposed image encryption scheme is presented in Section 4. Next, we explain in details the various cipher operations of the proposed scheme in 5. In Sections 6 and 7, we test a number of parameters to prove that the cipher has the requirements to prevent cryptanalytic attacks. In Section 8, we discuss the immunity of the proposed cipher variants against cryptanalysis and we study their corresponding execution times. Finally, the paper is concluded in Section 9.

## 2 Selective Encryption based on Sub-matrices

The proposed image encryption scheme targets digital medical images and can also be applied to other kinds of digital images. Medical images possess special features making them of special interest; they usually consist of two regions:

- the Region of Interest (ROI), which contains the sensitive information;
- the Region of Background (ROB), which contains the non-sensitive information.

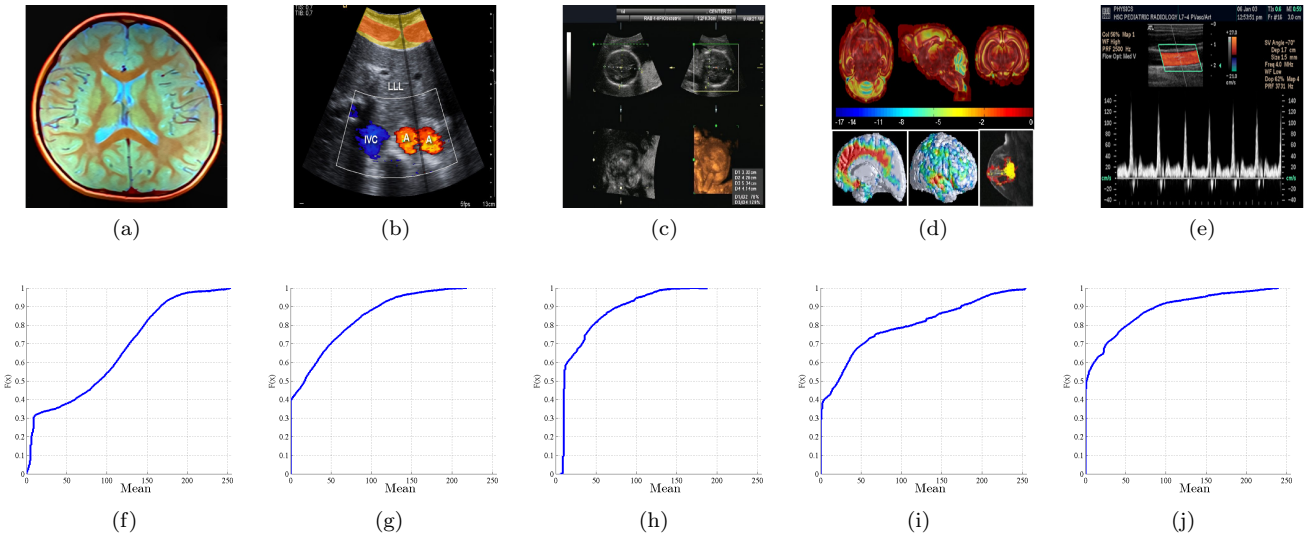



Fig. 1: Original images studied (a)-(e) and their corresponding ECDF of the sub-matrices average (f)-(j).

An input medical image, in matrix form, has a size is $r \times c \times p$, where $r$ is the number of rows, $c$ is the number of columns and $p$ is the number of planes (in gray scale $p$=1). The number of blocks in the image is padded, if necessary, to obtain a multiple of $h^2$ complete sub-matrices; each sub-matrix consists of $(h \times h)$ bytes. In the rest of the paper, $h$ will be set to 8 and an optimum value may be selected depending on the application and the available memory space. The total number of sub-matrices is $\alpha$, where $\alpha = \lceil \frac{r \times c \times p}{h^2} \rceil$. In order to locate the Region of Interest, we adopt a thresholding segmentation method based on the average and the standard deviation, as explained in (30). Indeed, in this paper, for each sub-matrix, the average only is required and it is computed and compared against a threshold to detect its corresponding region.

Different kinds of medical images such as X-ray and Ultra-sound are analyzed in order to quantify the threshold by analyzing the Empirical Cumulative Distribution Function (ECDF) of the average of sub-matrices.

According to experimental (simulation) results, we found that almost all the ROI sub-matrices have an average greater than the threshold $\tau = 10$, as shown in Fig. 1 based on the ECDF of the average of sub-matrices. All sub-matrices of ROI have a mean that falls in the interval $[\tau, 255]$.

The average of each sub-matrix is calculated and compared against this threshold to determine whether or not to consider it as significant. If the average of a specific sub-matrix is greater than the threshold, then, it is flagged as part of ROI and it will be encrypted. ROB sub-matrices are not encrypted since they can affect seriously the latency and influence the resources. Note that the encrypted parts from ROI are combined with the unchanged parts from ROB before being stored or sent over the channel.
The decryption scheme applies the same classification in order to locate the encrypted ROI sub-matrices that should have a higher value close to the average (128) since encrypted sub-matrices exhibit the uniformity propriety. On the other hand, Table 1 presents the notation and symbols used in this paper.

## 3 Key Derivation

In order to achieve low complexity and simple implementation on constrained devices, we consider one Secret Key shared between the transmitter and receiver. To protect the key, it can be renewed by using Elliptic Curve Diffie Hellman (ECDH) and transmitted to the receiver in an encrypted form or via a feedback channel. In order to make the algorithm even more secure, the key is renewed after a periodic interval depending on the application.

Table 1: Table of Notations

| Notation | Definition |
|---|---|
| $L$ | Number of rows |
| $C$ | Number of columns |
| $P$ | Number of planes (in gray scale $p$=1) |
| $SK$ | Secret Key |
| $DK$ | Dynamic Key |
| $IV$ | Initialization Vector |
| $S_k$ | Substitution Key |
| $P_k$ | Permutation Key |
| $IM$ | Initial Matrix |
| $i$ | Index of Sub-matrix from [1, $l$] |
| $IM_i$ | Dynamic Initial matrix with index i |
| $h$ | Size of a block (sub-matrix) |
| $\psi$ | Dynamic Counter |
| $l$ | Number of sub-matrices (equal to $\alpha$ for the full approach and $\beta$ for the selective ) |
| $\alpha$ | Number of sub-matrices in one image |
| $\beta$ | Number of ROI sub-matrices in one image |
| $rs$ | Number of rounds to produce a good S-box |
| $rp$ | Number of rounds to produce a good P-box |

### 3.1 Dynamic Key Generation, $D_k$

The secret key is xor-ed with an initialization vector $IV$ (128 bits), which is then hashed using SHA-512 to form the dynamic key of size 64 bytes. Note that the initial vector is changed for every image hence the dynamic feature of the key is maintained. Next, the dynamic key is divided into 4 sub-keys as such:

- The Permutation Key, $P_k$, is used to generate a dynamic permutation table, P-box, which is used to permute the selected sub-matrices according to the cipher variant. For example, it is used to permute ROI sub-matrices for SE1 or SE2. The 128 bits of $P_k$ are taken from $D_k$ and this sub-key can be used with any stream cipher to produce the required binary key stream to control the proposed Modified Group Operation Permutation algorithm (MGRP). Then, MGRP is iterated for $Rp$ times to obtain the P-box, which has a length of $\beta$ and its values are within [1, $l$].
- The Substitution Key, $S_K$, is used to generate a dynamic substitution table, S-box. Another set of 128 bits are extracted from $D_k$ and can be used with the same stream cipher to produce the required binary key stream for $rs$ iterations of MGRP. Note that the produced S-box has a length of 256 and its values vary between [0, 255].
- Initial Matrix, $IM$: The third set of 128 bits of $D_k$ will be passed to the same stream cipher to produce a key stream sequence with $h^2$ byte length. This sequence will be reshaped to form an initial matrix $IM$ with size $h \times h$, which will be used to construct the different $IM_i$ that vary for every sub-matrix, $i = 1, 2, \ldots, \beta$.
- Counter $\psi$: The fourth group of 128 bits is used to obtain another matrix $\psi$ that is also used in the construction of $IM$.

The above sub-keys are unique for every image and are all derived from one dynamic key that changes for every input image. Below is an explanation of these components. The initial matrix, $IM$, will be used as a starting point to generate all the required $IM_i$ where $i$ is a variable between [1, $l$]. As such, we use a different $IM$ for every sub-matrix to add randomness to the system and hence to lower the success probability of cryptanalytic attacks. $IM$ is first xor-ed with the first value of the initial vector $\psi$. Then, the result will undergo a substitution process using a dynamic key $S_k$. The result is used as the first $IM$. The process continues similarly while incrementing the dynamic counter $\psi$. After each iteration, a right shift operation is applied to the S-box. For example, for the first operation, when $\psi = 1$, no shift operation is done to the S-box, while for $\psi = 2$, one right shift is performed as indicated in Figure 3. The importance of this operation is that all the required $IM_i$ can be obtained in parallel for the encryption process. Accordingly, the execution time will be reduced because of the parallelism property inherent in this algorithm. Not only do we achieve a high level of security, but also a lower execution time as compared to existing multi-round cipher algorithms.

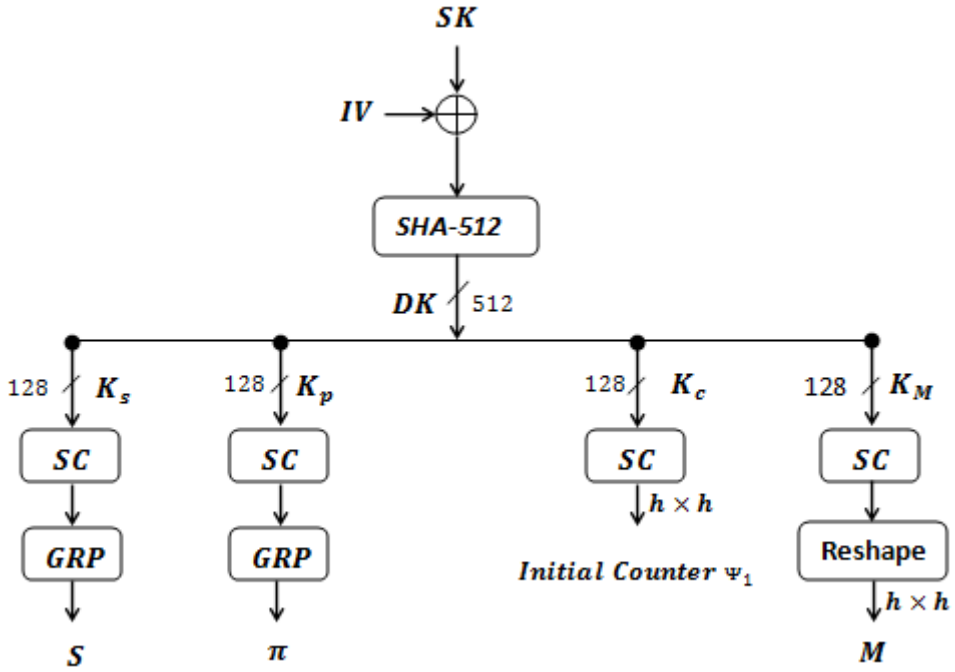



Fig. 2: Proposed dynamic key generation technique and the corresponding dynamic sub-keys

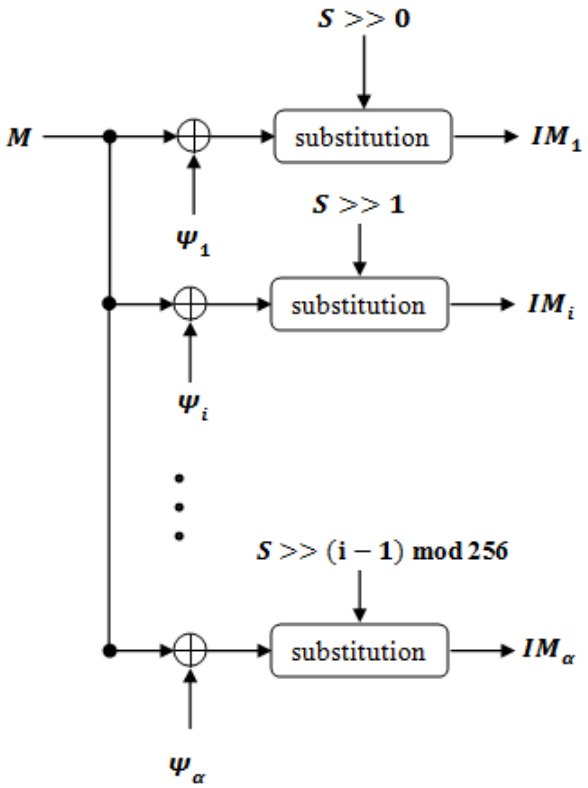



Fig. 3: The proposed technique to generate the required pseudo-random masking sub-matrices.

## 4 The Proposed Cipher Algorithm

In this section, the proposed cipher algorithm is described. We start by introducing the selective approach and then, we provide details about the permutation and masking processes. Finally, we describe briefly the decryption process.

### 4.1 Encryption Process

In Fig. 4, the encryption scheme is illustrated. First, the input $\alpha$ sub-matrices are subjected to the threshold test. If the average of each sub-matrix exceeds the $\tau$ parameter, then this sub-matrix will be considered as a part of ROI, otherwise, it is considered as part of ROB.

The selective cipher option has two variants, the first one, $SE1$, applies only a permutation among the selected sub-matrices, without the masking operation. While, the second variant, $SE2$, employs additionally the masking operation, which makes the system resilient against cryptanalytic attacks. Accordingly, each selected sub-matrix will be xor-ed with its corresponding $IM_i$. The result will be also xor-ed with the corresponding dynamic permutation sub-matrix for this selected sub-matrix. Next, another substitution is performed to increase randomness. This whole masking process is done for every sub-matrix. Then, a permutation between the sub-matrices will be performed based on a new P-box that is obtained by flipping the P-box array from right to left. This operation further randomizes the relationship between the selected sub-matrices. Finally, all sub-matrices are concatenated (ROI and ROB) to form the final encrypted image.

The second option, Middle-Full, has the principal objective of hiding any information related to the type of the medical image. A global permutation operation is done on all sub-matrices as compared to the previous operation, $SE2$, which applies it to the $\beta$ sub-matrices. Global permutation is done on both ROI and ROB regions. Hence, it will be very hard for an attacker to recognize the type of the image. These steps, in the selective or middle approaches, ensure a sufficient level of security for images, and hence provide an efficient approach for medical image encryption.

It is important to note that the execution time of such a scheme is low since only the important regions of the image are encrypted. Also, the use of a dynamic key, a single round, and a low number of operations is sufficient to achieve the required security level.
This approach may be extended by additional chaining; more randomness could be added to the scheme but parallelism will not be feasible. In this work, we achieved satisfactory results without chaining, however, it can be adopted by users who require additional protection for their images. The following equation represents the extended model:

$$C_{ip} = S(X_{ip} \oplus S(X_i \oplus IM_i)), \;\; i = \{1, 2, 3, ..., \alpha\} \tag{1}$$

where

- $S$ represents a dynamic S-box.
- $X_{ip}$ represents the corresponding permutation of $X_i$.
- $IM_i$ represents the corresponding initial matrix to be xor-ed with the sub-matrix $X_i$.

### 4.2 Decryption Process

Decryption is similar to the encryption process but in a reverse manner. The receiver performs the same encryption steps but in a backward approach, and using the inverses of S-box and P-box. In case of global permutation, we first perform an inverse global permutation. Decryption is complete when all the sub-matrices are decrypted and then grouped to re-construct the original image. Decryption could be represented by:

$$C_{ip} = S^{-1}(Y_{ip} \oplus S^{-1}(Y_i \oplus IM_i)), \;\; i = \{1, 2, 3, ..., \alpha\} \tag{2}$$

where

- $S^{-1}$ represents the inverse of the dynamic S-box.
- $Y_i$ represents the received encrypted sub-matrix from ROI.
- $Y_{ip}$ represents the corresponding inverse permutation of $Y_i$ at index $i$.
- $IM_i$ represents the corresponding initial matrix for the sub-matrix $Y_i$.

In the proposed approach, the channel error will not propagate since every sub-matrix is encrypted independently of the other sub-matrices.

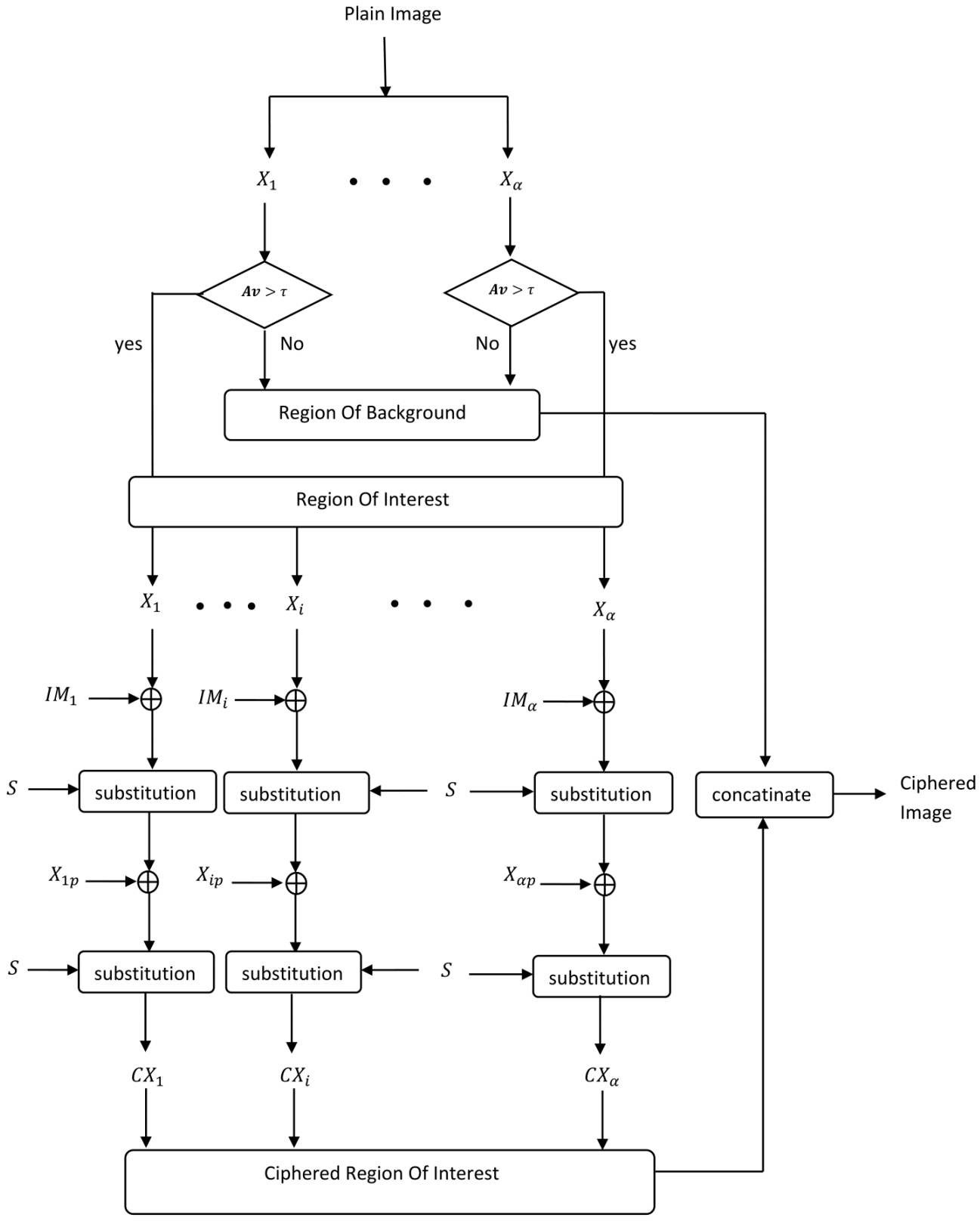
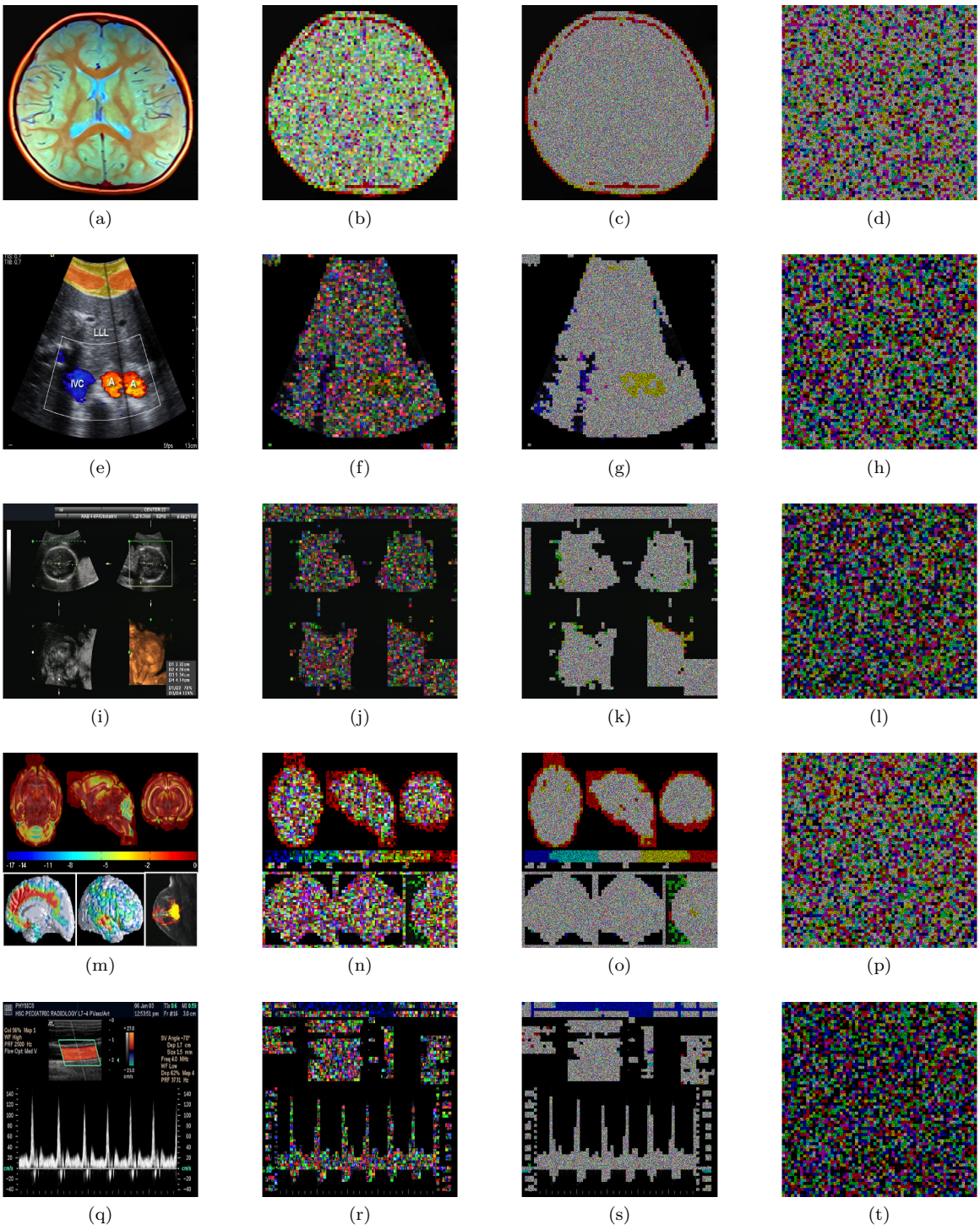



Fig. 4: Proposed Selective Encryption-2 (SE2) Scheme.




(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

(q) (r) (s) (t)

Fig. 5: (a) Original Brain MRI image, (b) encrypted image after permutation, (c) encrypted image after masking, (d) encrypted image after global permutation.
(e) Original Aorta image, (f) encrypted image after permutation, (g) encrypted image after masking, (h) encrypted image after global permutation.
(i) Original Head-3D , (j) encrypted image after permutation, (k) encrypted image after masking, (l) encrypted image after global permutation.
(m) Original image 06, (n) encrypted image after permutation, (o) encrypted image after masking, (p) encrypted image after global permutation.
(q) Original Spectral Doppler, (r) encrypted image after permutation, (s) encrypted image after masking, (t) encrypted image after global permutation.

**Algorithm 1** GRP permutation algorithm

```
1: procedure GRP(R_src, CR, l)
2:     j ← 0
3:                                  ▷ If the control register bit is zero, place its corresponding index at left
4:     for i ← 0 to l − 1 do
5:         if CR[i] == 0 then
6:             R_dest[j++] ← R_src[i]
7:         end if
8:     end for
9:                                  ▷ After that, if the control register bit is one, place its corresponding index at right
10:    for i ← 0 to l − 1 do
11:        if CR[i] == 1 then
12:            R_dest[j++] ← R_src[i]
13:        end if
14:    end for
15:                                 ▷ R_dest is the output substitution vector
16:    Return R_dest
17: end procedure
```

**Algorithm 2** Proposed substitution algorithm

```
1: procedure PERM(DK, l, rt)
2:                                  ▷ l is the length of input vector
3:     R_src ← 0 to l − 1
4:
5:     for w ← 1 to rp do
6:         CR_w ← CR[(w − 1) × l : (w) × l − 1]
7:         R_src = GRP(R_src, CR_w)
8:         CR_w ← ¬CR_w
9:         R_src = GRP(R_src, CR_w)
10:    end for
11:                                 ▷ Last R_src can be a dynamic Pbox or S − box.
12:    Return R_src
13: end procedure
```

## 5 Construction of Cipher Primitives

The proposed techniques to generate dynamic key-dependent S-boxes and P-boxes are presented next. This is done by using a modified version of the group operation of permutation (51). key-dependent permutation and substitution tables are generated and used in the encryption process, while their corresponding inverse tables are used in the decryption process.

### 5.1 Construction of Dynamic Permutation and Substitution Tables

After the dynamic key generation, permutation and substitution tables are built and the keys are used to produce a corresponding key-stream sequence as described in Section 3. The generation of the dynamic permutation and substitution primitives is done using a key-dependent permutation algorithm based on the GRP permutation algorithm (51). GRP is chosen as a basic element since it is simple, flexible and efficient in terms of software and hardware implementations. The GRP permutation algorithm is described in Algorithm 1. Note that $R\_src$ is the input vector, $CR$ is the configuration vector (control register) and $R\_dest$ is the output. $R\_src$, $CR$ and $R\_dest$ all have the same length, which is equal to $l$ for constructing the permutation table and 256 for the construction of the substitution table.

The basic idea of the $GRP$ is to divide the index into two groups according to the pseudo-random bit sequence ($CR$). If the bit in $CR$ is 0, this index is moved to the first group, otherwise, the element is moved to the second group as seen in Fig. 6.

However, the original $GRP$ algorithm performs poorly for just one iteration due to the low number of unique output vectors and the high number of fixed points as shown in Fig. 7. As such, and to enhance the $GRP$ algorithm, we iterate for multiple rounds, whereby for each round, a different control $CR_i$, $i = 1, 2, \ldots, rs$ is used. Also, for each round, $CR_i$ and $\overline{CR_i}$ are used respectively, for the two iterations of the GRP algorithm. The enhanced algorithm is described in Table 2.

Fig. 6 shows an example of the **proposed** GRP algorithm implementation for 8 elements.

To produce a substitution table (S-box) or permutation table (P−box), an initial vector $R\_src$ is used, where $R\_src[j] = j$ and $j = 0, 1, \ldots, l$ ($l = 256$ for substitution table and equals to $\alpha$ or $\beta$ for the permutation table according to the cipher option). Then, the process of permutation is applied for $rt$ times. The output vector $R\_dest$, after each permutation iteration, becomes the input vector $R\_src$ for the next one. The cryptographic performance of the output $R\_dest$ is quantified for each iteration. This transformation is applied for multiple rounds $irs = 1, 2, \ldots, rs = 10$. Therefore, dynamic permutation and substitution tables can be produced by applying the proposed permutation algorithm for $\geq 5$ rounds (different $CR$ for each iteration). Since the process of the substitution layer generation is based on the use of permutation, the produced S-boxes will feature a high probability of unique dynamic S-boxes (PoU) ($\approx 0.8 \times 2^q!$ as seen in Fig. 7 for $q = 3$) compared to using fixed CR. Even though the dynamically generated P-boxes and S-boxes (output vector $R\_dest$) exhibit good cryptographic characteristics, yet, these are still lower than the maximum achieved by static S-boxes that are used in the modern block cipher (AES).

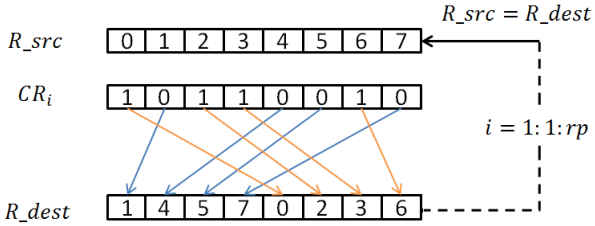



Fig. 6: Example of constructing a permuted vector ($P - box$) based on the GRP algorithm with $q = 3$ and for a specific $CR$.

Consequently, a good randomness degree, a large number of different unique S-boxes are generated with a lower probability of fixed points (close to $\frac{1}{2^q}$ on average) and an acceptable CC ($O(2^q)$) can be achieved using the proposed permutation algorithm. An example of producing dynamic S-box for $q = 8$ and its corresponding inverse $(\text{S-box})^{-1}$ are shown in Fig. 8.

### 5.2 Cryptographic Performance of Dynamic Substitution

A robust and efficient key-dependent construction technique of substitution tables (S-boxes) should ensure several cryptographic criteria such as bijectivity, Linear Probability boolean Function ($LPF$), Differential Probability Approximation Function ($DPF$), Strict Avalanche Criterion (SAC), and output Bits Independence Criterion (BIC). In the following, these criteria are described briefly and the results of the proposed construction technique are presented in order to prove that the proposed technique ensures good cryptographic performance in a dynamic manner.

- **Bijectivity**: This criteria validates that an inverse S-box exist, and hence, the substitution transformation can be reversed in the decryption algorithm. A simple technique to verify the bijectivity is to compute the different number of elements needed for the S-box using the unique function. If the number of unique elements equals to $2^q$ for Galois field $q$, then this S-box is bijective, otherwise it is not. In the proposed model, a bijective permutation technique based on GRP algorithm is employed and consequently the proposed S-box is bijective.
- **Linear Probability approximation Function** $LPF$: A lower $LPF$ value indicates higher immunity against linear attacks since there would be no linear relationship between bits of the plain text and the substituted ones (52). The average variation of the $LPF$ values *versus* the number of iterations is shown in Fig. 9-(a). The results indicate clearly that the required number of iterations to reach a stable low $LPF$ value, close to $2^{-4.79}$, is 5. Also, in Fig. 9-(e) the variation of $LPF$ for 10,000 random $S_K$ is presented and the maximum, minimum and average values of LPF are $2^{-3.8}$, $2^{-5.7}$ and $2^{-4.8}$, respectively. In fact, the majority of the produced substitution tables have low and acceptable $LPF$ values. This, combined with the dynamic nature of the S-boxes, ensures sufficient resistance against linear attacks.

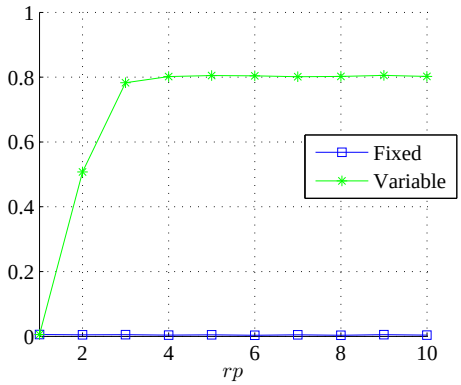
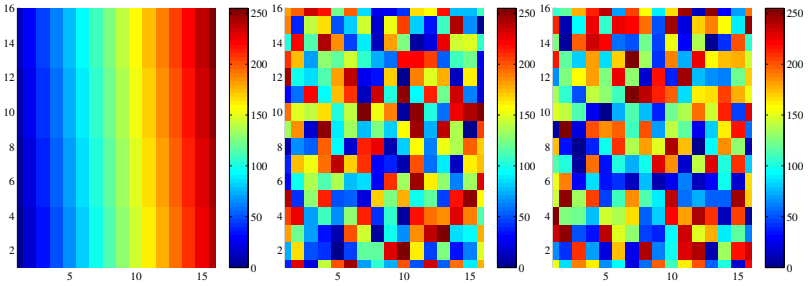



Fig. 7: Varition of the average of $PoU$ for $2^{15}$ random $CR$ versus $rp$ (here $rp = rs$) using fixed and variable CR



(a) $V$ in matrix form (b) P-box (c) P-box$^{-}$1

Fig. 8: Original input matrix of $R\_src$ (a), generated P-box by using a random dynamic key (b) and its corresponding inverse one (c) for $l = 256$

– **Differential Probability approximation Function** $DPF$: This criterion shows the effect of a slight change in plain-text pairs on the corresponding substituted pairs. Typically, a low value of $DPF$ indicates high resistance against differential attacks (53). In Fig. 9-(b), the average variation of $DPF$ versus the number of iterations to reach a low stable value of $DPF$, close to $2^{-4.5}$, is also 5. Additionally, in Fig. 9-(f), the maximum, minimum and average $DPF$ values for 1,000 dynamic keys are shown and they are equal to $2^{-4}$, $2^{-4.69}$, and $2^{-4.41}$, respectively.
These results confirm that the generated S-boxes ensure good cryptographic performance against differential attacks.
– **Strict Avalanche Criterion,** $SAC$: This criterion is to show that a one-bit change in any element of an S-box produces a different substituted element by at least 50%. The variation of the probability of SAC with regards to different number of iterations is shown in Fig. 9-(c). The results indicate that 5 iterations are necessary to be closer to the SAC ideal value of 0.5. Also, in Fig. 9-(g), the variation of $SAC$ for 1000 produced random S-boxes with the proposed technique are shown and the results indicate that the SAC value is always close to 0.5.
These results validate that the proposed technique is compliant with the SAC criterion.
– **Bit Independence Criterion,** $BIC$: This states that two output bits $j$ and $k$ must change independently when a single input $i$ is changed for all $i, j$ and $k$. The probability variation for different number of iterations is illustrated in Fig. 9-(d). It is clear that the probability values of $BIC$ become close to the optimal value 0.5 when $rs = 5$. In Fig. 9-(h) the variation of $BIC$ for all produced S-boxes is close to 0.5. This validates the $BIC$ criterion. Therefore, according to these results, $rs$ and $rp$ are chosen to be equal to 5.

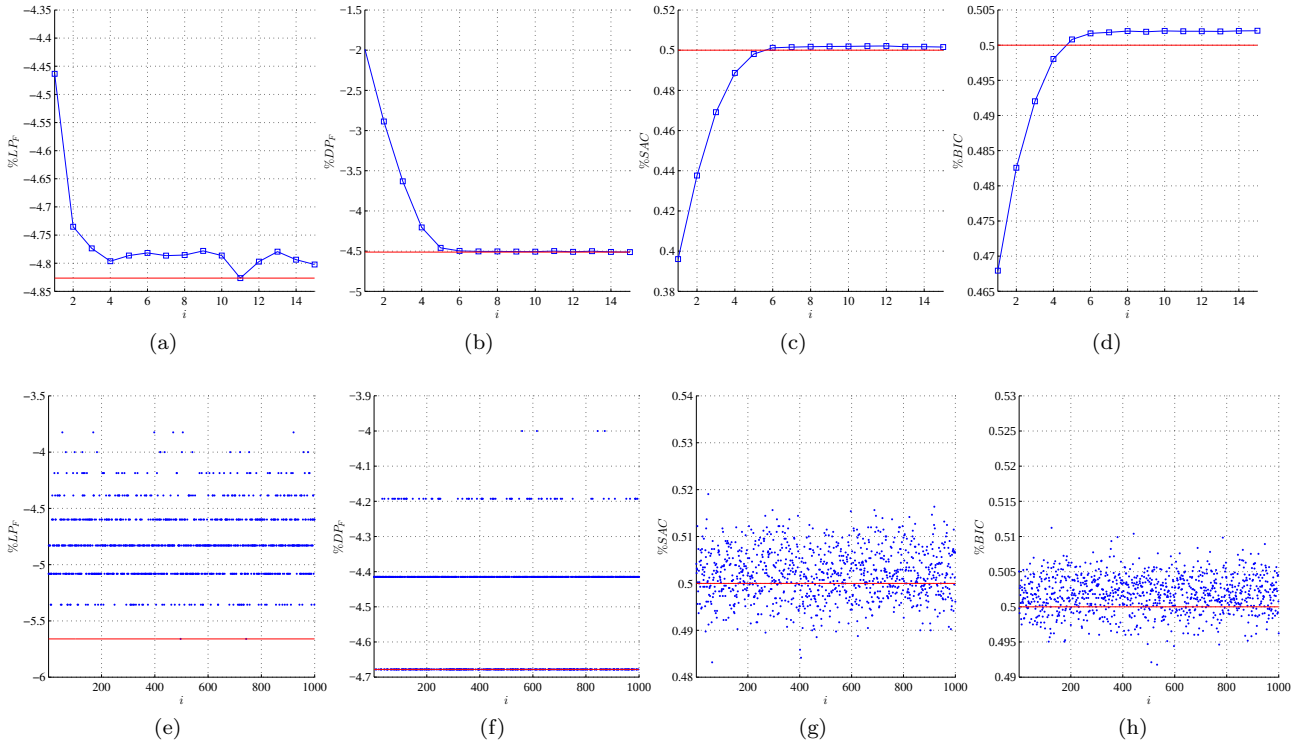



Fig. 9: Variation of the average $LPF$ (a), $DPF$ (b), SAC (c), and BIC (d) versus $rs$ for the proposed S-box. Variation of the average $LPF$ (a), $DPF$ (b), SAC (c), and BIC (d) against 1,000 dynamic keys for $rs = 5$.

## 6 Encryption/Decryption Efficiency Analysis

In this section, we assess the performance of the proposed flexible cipher variants. We consider a number of ordinary and medical images of different structures. Then, selective and full encryption are applied to these images using the proposed variants. In the second selective encryption variant, SE2, ROI is encrypted using the same algorithm as full encryption and we present various tests to prove the robustness of the proposed cipher for selective as well as for full encryption in the next section.

For selective encryption, we consider square blocks of size $8 \times 8$ and $\tau$=10. We compute a set of Effective Cumulative Probability Density Functions, to identify a specific threshold. Also, in this section, we present ROI and ROB in the encrypted image. The mean for the ROI encrypted region is close to 128, which is the required criteria for the feasibility of decryption. The recovery of the original plain images was verified since the same regions of the selectively encrypted images are also selected for decryption. In figure 10, it is obvious that the five images presented in our tests have a clear average, which makes the decryption possible.

Moreover, the ECDF for the same five images are presented in Figure 1 indicating that the ECDF is preserved and the encryption starts from the point that we have no zero-value pixels (black pixels), which are considered as the background. ECDF defines the threshold relative to the average of every sub-matrix in the image. The size of matrix used is $8 \times 8$. We select three images from Figure 5 for selective and full encryption and the results are presented in Figure 11. Comparing the full approach with the selective one, it is clear that the result of global permutation, done after the masking process, is the closest to full encryption, which indicates that the level of security is preserved, yet, with less computational overhead. The recovered images are identical to those presented.

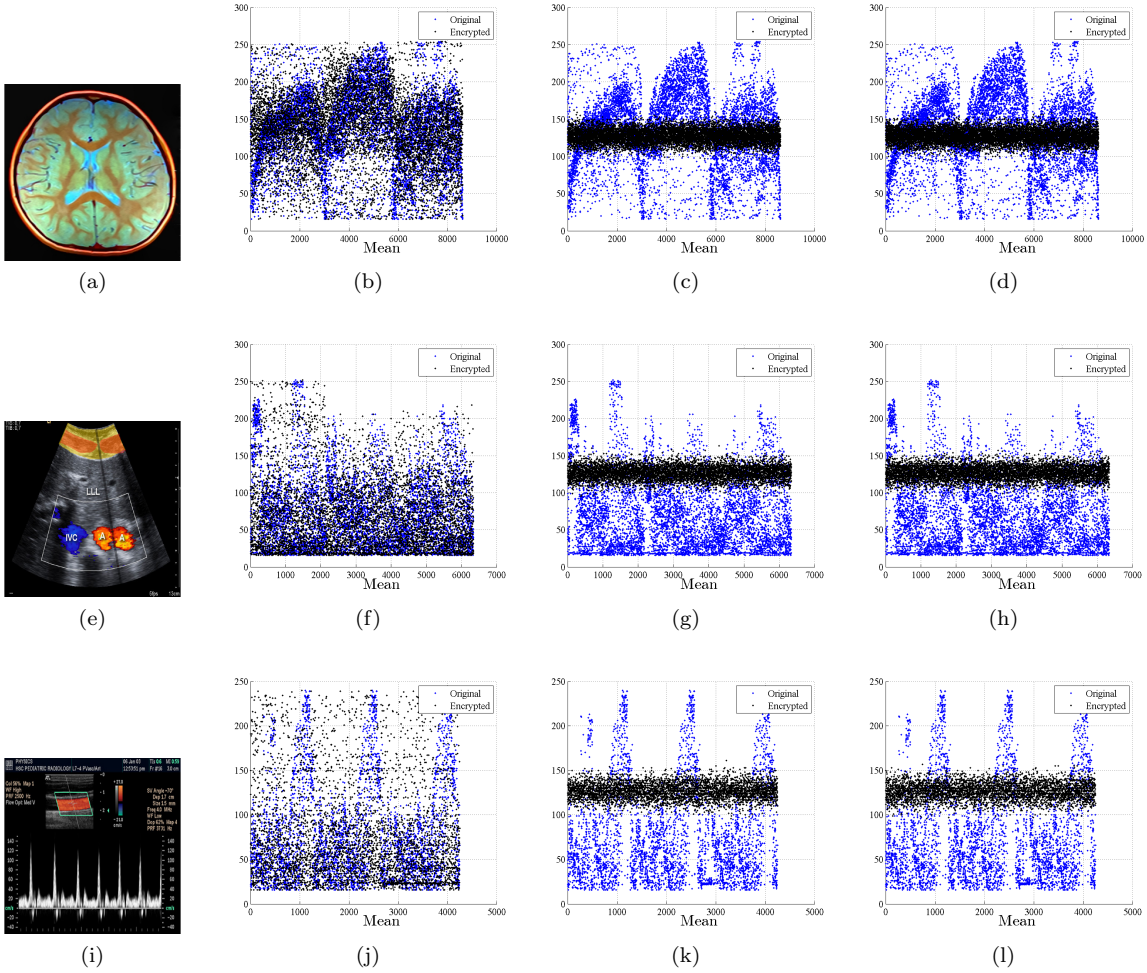


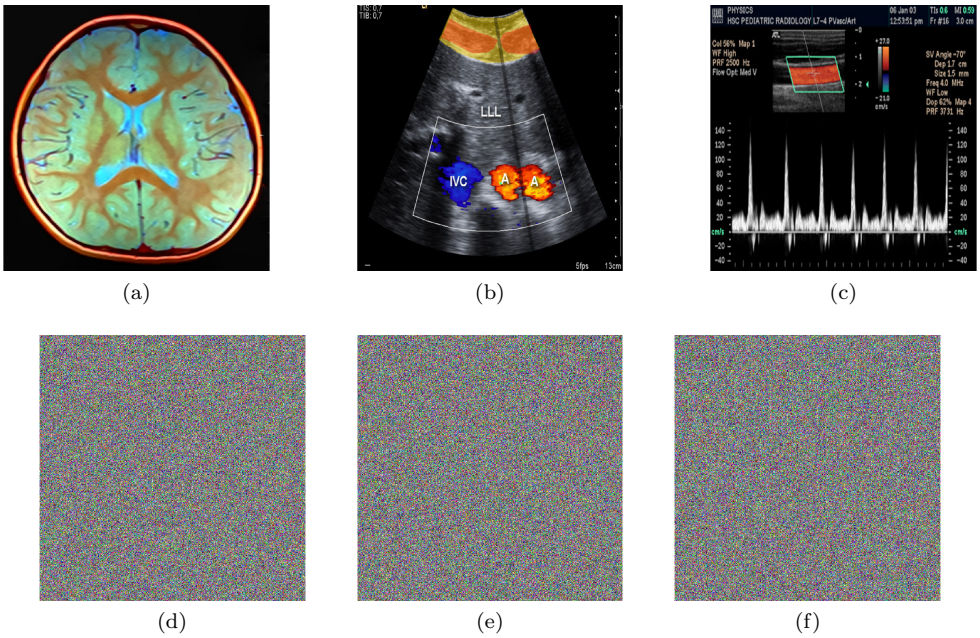

Fig. 10: Distribution of ROI and ROB; ROI is represented by the black points and ROB is represented by the blue points. First column represents the original images; Second column represents the distribution of pixels after permutation; The third column represents the distribution after masking; The fourth line represents the distribution after global permutation.

## 7 Statistical and Security Analysis

In this section, we assess the cryptographic robustness against different kinds of attacks such as statistical, chosen/known plain text attacks in both approaches, full and selective. Accordingly, several statistical metrics are presented to prove that the cipher images ensure a high randomness degree in addition to key sensitivity, which is an essential criterion since our approach is based on a dynamic key. On the other hand, the required latency is reduced since the core function of the cipher, the round function, is iterated only once. In the following, we prove that one round is sufficient to reach the desired performance. More importantly, the structure of the proposed cipher scheme can be implemented in parallel, which further reduces the associated latency.

### 7.1 Uniformity of Probability Density Function

To resist statistical attacks, the encrypted image should have certain random properties. The most important one is the Probability Density Function (PDF) of the encrypted image, which should be uniform; that is, each symbol has an occurrence probability close to $\frac{1}{n}$, where $n$ is the number of symbols. The PDF of the four original plain-images and their corresponding cipher images are shown in Fig. 12. It can be seen




(a) (b) (c)

(d) (e) (f)

Fig. 11: Original images Brain MRI (a), Aorta (b), and Spectral Doppler (d) with their corresponding encrypted results using full encryption approach (d)-(f).

that the PDF of the encrypted images using the proposed scheme is close to a uniform distribution with a value close to 0.039 that is $\frac{1}{256}$. Note that, since the permutation doesn't affect the distribution of pixels, we can see that, after masking, the PDF of encrypted ROI tends to be uniform. Additionally, the PDF of encrypted images after full encryption is also similar to the second variant of the selective encryption algorithm. To validate this result at the sub-matrix level, an entropy test is performed and described next.

Table 2: Simulation Results with $h = 8$

| | **min** | **mean** | **max** | **std** |
|---|---|---|---|---|
| Dif | 49.8877 | 49.9997 | 50.1071 | 0.0340 |
| Entropy of original sub-matrix | 2.1823 | 4.2014 | 5.7813 | 0.7991 |
| Entropy of encrypted sub-matrix | 5.4200 | 5.7666 | 6.0000 | 0.0766 |
| KS | 49.8828 | 49.9982 | 50.1067 | 0.0349 |
| NPCR | 99.5747 | 99.6097 | 99.6468 | 0.0118 |
| UACI | 33.2960 | 33.4646 | 33.6079 | 0.0460 |

Table 3: Simulation Results with $h = 16$

| | **min** | **mean** | **max** | **std** |
|---|---|---|---|---|
| Dif | 49.8955 | 49.9989 | 50.1330 | 0.0343 |
| Entropy (original sub-matrix) | 2.7235 | 4.9910 | 6.8398 | 0.9624 |
| Entropy (encrypted sub-matrix) | 6.9631 | 7.1730 | 7.3445 | 0.0523 |
| KS | 0.0308 | 0.0359 | 0.0436 | 0.0017 |
| NPCR between original and cipher images | 49.8581 | 50.0004 | 50.1029 | 0.0342 |
| UACI between original and cipher images | 99.5724 | 99.6093 | 99.6460 | 0.0125 |

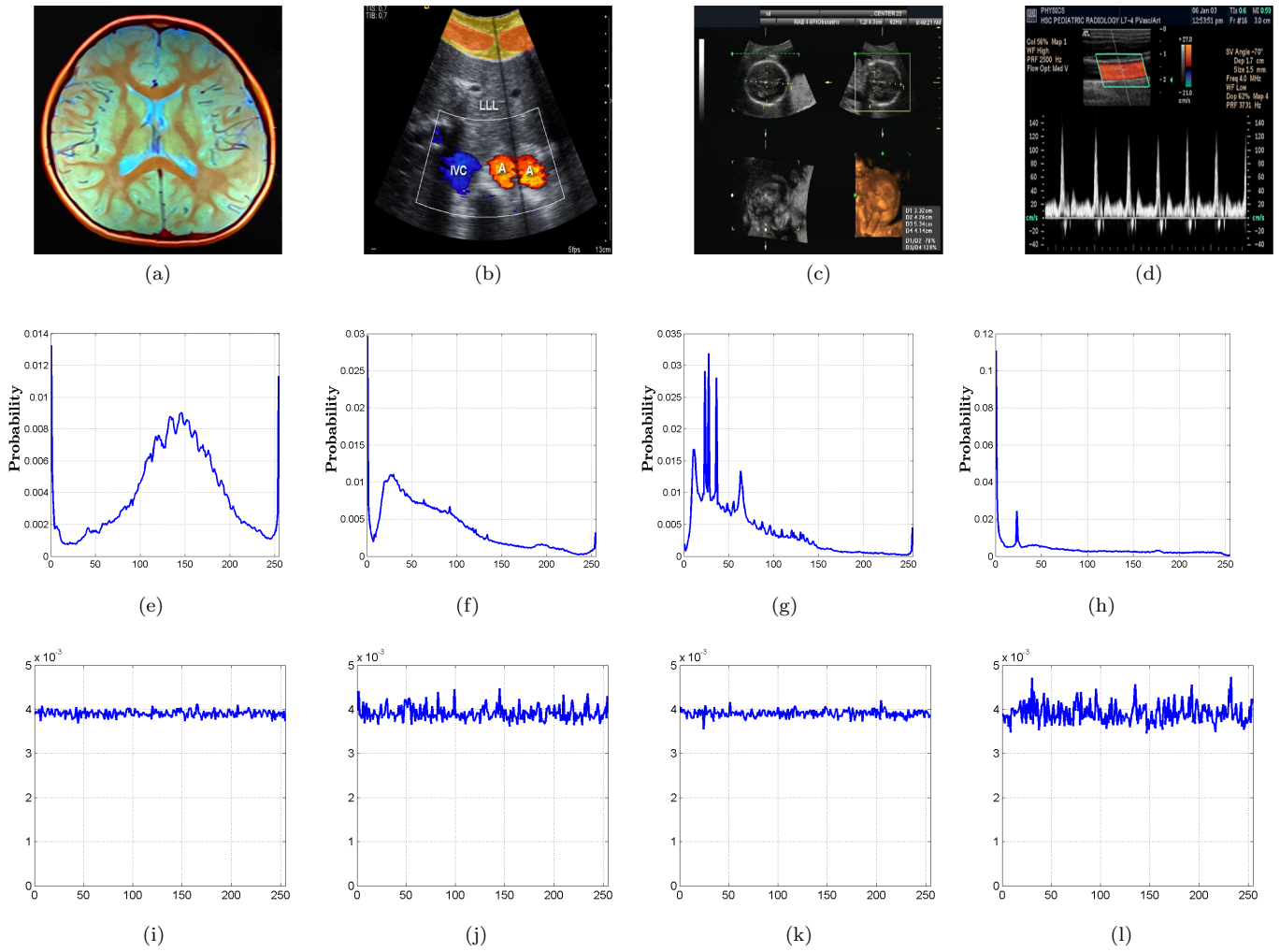



Fig. 12: Original medical images (a)-(d) and their corresponding PDF (c)-(h). PDF of the corresponding encrypted images after full encryption (i)-(l).

### 7.2 Entropy Analysis

The entropy information of an image $M$ is a parameter that measures the level of uncertainty in a random variable, and is defined using the following equation:

$$H(m) = -\sum_{i=1}^{h^2} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{3}$$

Where $p(m_i)$ represents the occurrence probability of the symbol $m_i$, and $h^2$ is the size of the square matrix $(h \times h)$; the entropy is expressed in bits. A truly random entropy source is equal to 7 when $h = 16$ for a uniform distribution. We are calculating entropy at the sub-matrix level. A value close to $\log(h^2)$ is the desired value.

$$H(m) = -\sum_{i=1}^{n} \frac{1}{(h \times h)} \log_2 \frac{1}{(h \times h)} = \log_2(h^2)$$

Looking at Figure 13, we can clearly see that for $h^2 = 16 \times 16$, $H$ is between 7 and 7.3 for the encrypted image. Also, we can see in the Figure the difference between the entropy of the original plain image and the encrypted one. We can conclude that our system is safe against statistical attacks.

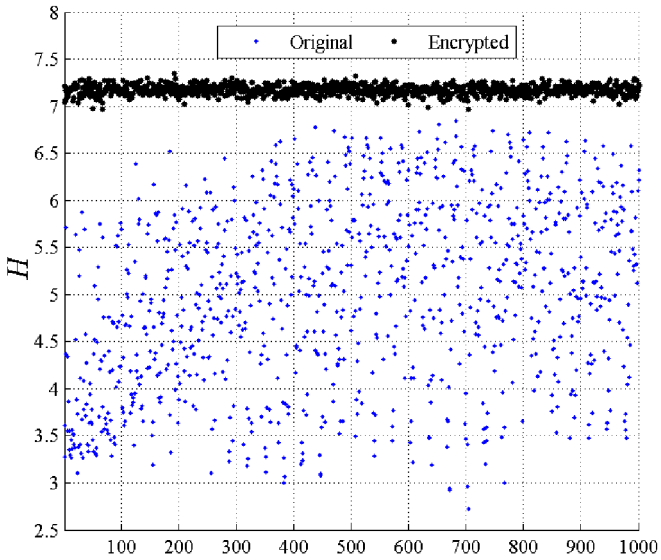



Fig. 13: Entropy test for the cipher sub-matrices with $h = 16$ for the full approach.

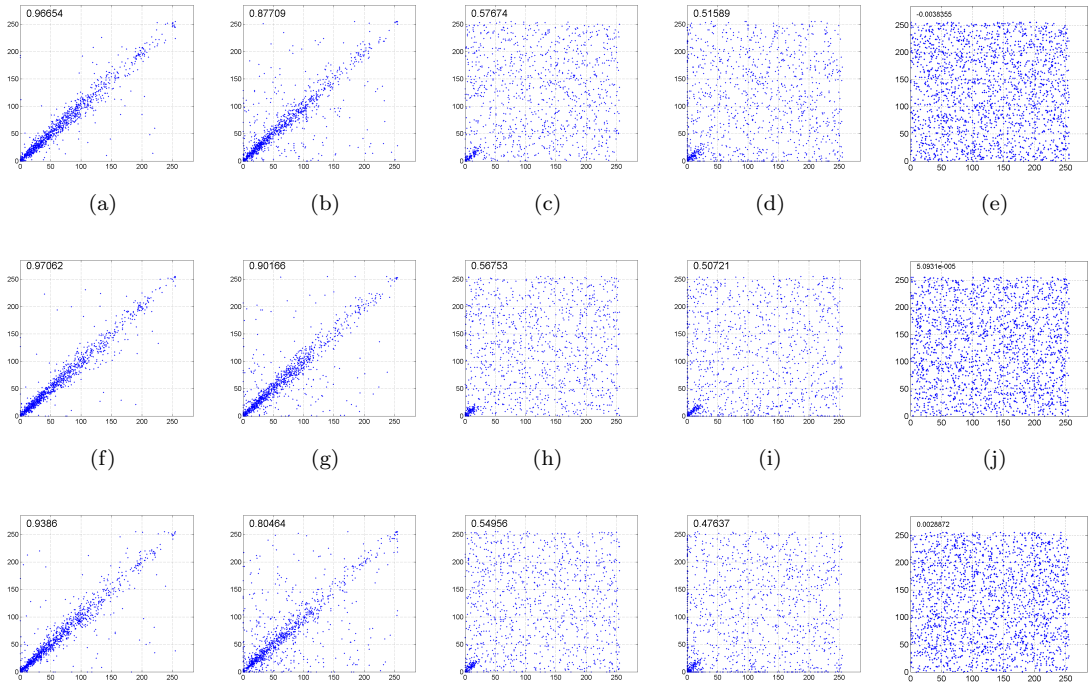



Fig. 14: For Aorta image , (a), (b), (c), (d), (e) represent the vertical correlation: original, after permutation, after masking, after global encryption and full encryption respectively. (f), (g), (h), (i), (j) represent the horizontal correlation: original, after permutation, after masking, after global encryption and full encryption respectively. (k), (l), (m), (n), (o) represents the diagonal correlation: original, after permutation, after masking, after global encryption and full encryption respectively.

### 7.3 Correlation Analysis

Correlation is an important metric that must be assessed. Removing the correlation among the pixels of an image is a successful indication that the cipher is immune to statistical attacks. Having a correlation

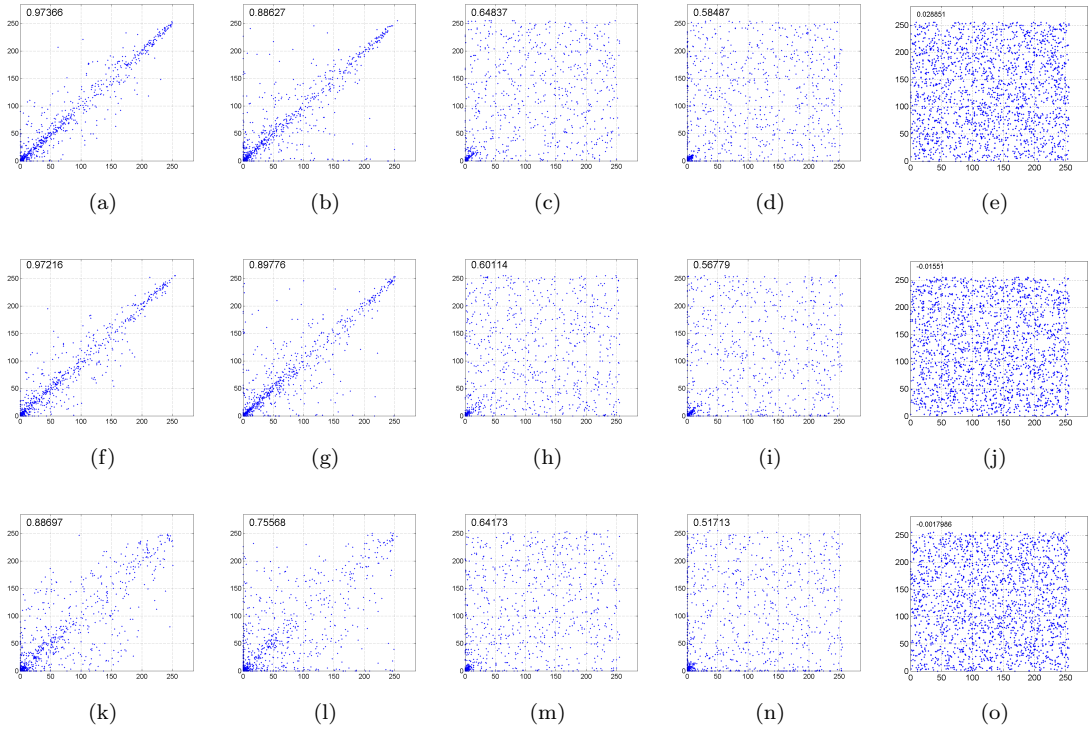



Fig. 15: For Spectral Doppler image , (a), (b), (c), (d), (e) represent the vertical correlation: original, after permutation, after masking, after global encryption and full encryption, respectively. (f), (g), (h), (i), (j) represent the horizontal correlation: original, after permutation, after masking, after global encryption and full encryption, respectively. (k), (l), (m), (n), (o) represent the diagonal correlation: original, after permutation, after masking, after global encryption and full encryption, respectively.

coefficient close to zero means that the cipher ensures a high degree of randomness. The correlation test is applied by taking randomly $N$ random pairs of adjacent pixels from the known plain image and their corresponding encrypted ones. The correlation coefficient $r_{xy}$ is calculated using the following equation:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \tag{4}$$

where

$$E_x = \frac{1}{N} \times \sum_{i=1}^{N} x_i \ , \qquad D_x = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))^2$$

and

$$cov(x,y) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

The correlation is done in the horizontal, vertical and diagonal directions. In Fig. 14, the correlation test for the different plain and encrypted medical images with their corresponding vertical, horizontal, and diagonal correlations are shown for the different proposed approaches. Notice that the first variant of selective encryption, which is based only on permutation of sub matrices doesn't ensure low correlation (still linear as the original image (see Fig. 14-(b, g,l)) since the correlation is quantified at the pixel level and not at the sub-matrix level.

While for the second variant, which entails, in addition to the permutation process, a masking process applied to each sub-matrix of ROI, the correlation is removed between adjacent pixels of ROI sub-matrices (see Fig. 14-(c, h,m)). The middle-full approach gives similar correlation results as the second selective approach (see Fig. 14-(d, i, n)) since the sub-matrices of ROB are not masked. Note that the global permutation of the middle-full approach is very important to ensure a better visual degradation, which permits to hide the structure of the medical image and consequently, its type. See Fig. 14-(e, j, o)).

The lower correlation result is obtained for the encrypted images that use the full encryption approach as shown in Fig. 14-(e, j, o). Correlation in the proposed approach is dependent on the encryption variant, while the best correlation results (close to 0) can be obtained by employing the full approach. In fact, the obtained results for the middle-full and for the second variant of selective encryption algorithm are also sufficient to provide protection since a masking process is applied for the ROI sub-matrices.

### 7.4 Key Sensitivity

In this section, we quantify the sensitivity of secret key $k$ and $IV$ and we show the recurrence of the produced dynamic initial matrices and the probability density function for 250 different $IM$.

The size of the secret and dynamic keys is flexible; it can be 128, 196, 256 bits for the secret key, and 512 for the dynamic key. It is chosen according to the desired level of security. These sizes are sufficient to make the brute force attacks unfeasible. Concerning $IV$, in Fig. 16-a, a random bit of a random bye of $IV$ is flipped. The results show that the difference in the produced cipher images is close to 50%. In addition, in Fig. 16-b, a random bit of a random byte of the secret key is flipped and the results show that the difference between the produced cipher images is also close to 50%. This criteria enhances the resistance of the system against brute force attacks and in particular, key-related attacks. On the other hand, the recurrence test is applied to 250 produced $IM$ and the results are shown in Fig. 17-a. The results confirm that the produced $IM$ is highly non-linear. Finally, in Fig. 17-b, we can see that the PDF of these produced $IM$ is very close to being uniform. Therefore, the technique for producing IM strongly enhances the cryptographic performance.

### 7.5 Sensitivity Analysis and Differential Attacks

Two metrics are commonly used in the sensitivity analysis of any approach: (1) Number of Pixels Change Rate (NPCR) and (2) Unified Average Changing Intensity (UACI). NPCR represents the number of pixels change rate between two images $I_1$ and $I_2$, while $UACI$ measures the changing intensity between the two cipher-texts. $NPCR$ and $UACI$ are represented by:

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$NPCR = \frac{\sum_{i,j} D_{i,j}}{M \times N \times P} \times 100\% \tag{5}$$

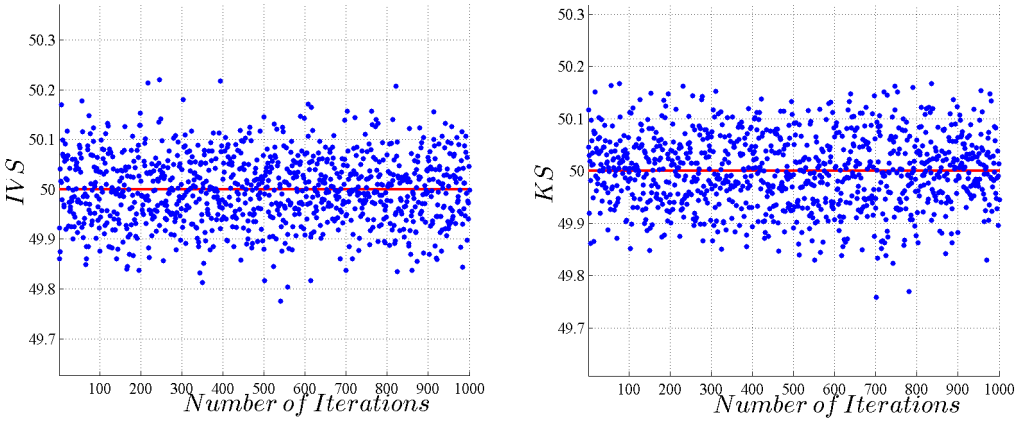
$$UACI = \frac{1}{M \times N \times P} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{6}$$

$NPCR$ between original and cipher image is $\geq 99.61$, which means that the pixels' positions are highly unrelated to each other. Moreover, an appropriate $UACI$ value is obtained that is close to 33.3, which means that most of the gray level pixels in the encrypted image are changed by the second variant of selective algorithm in addition to full and middle-full.

Figure 18 illustrates the probability of $NPCR$ and $UACI$ for 1,000 dynamic keys used to encrypt the Lenna plain-image of size $512 \times 512$. The theoretical results are $NPCR = 99.61$ and the mean value of $UACI$ is equal to 33.4. The proposed approach shows high values of $NPCR$ and $UACI$ that are needed for a good cipher scheme. Also, Tables 2 and 3 summarize the results.

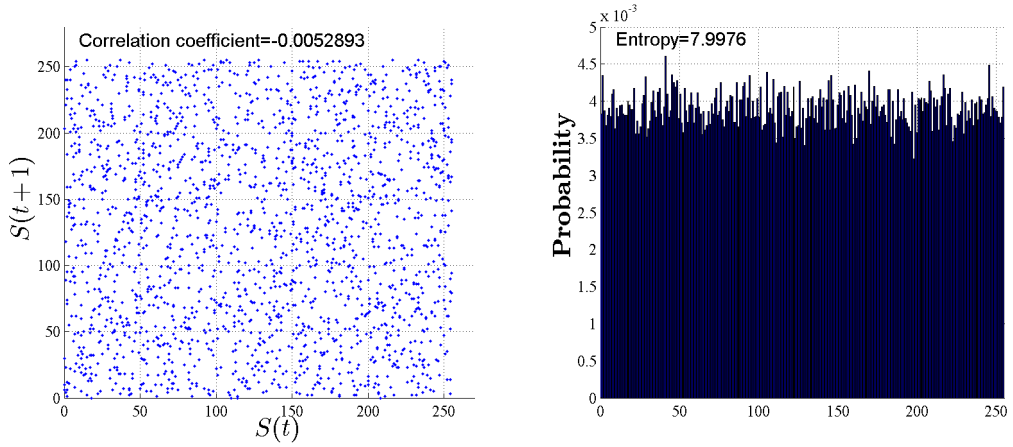
### 7.6 Visual Degradation

An important condition to ensure a robust image encryption algorithm is that the visual content of the original image must not be recognized in the ciphered image. Two well known parameters are considered to measure the encryption visual quality, which are Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity index (SSIM) that are described in (54). A low PSNR value indicates a high difference between the original and the cipher images. Concerning $SSIM$, it is defined after the Human Visual System (HVS) and it has evolved such that we can extract the structural information from the scene. Thus, the perceived quality of the image by the human eye is highly dependent on the loss of structural information in the image.




(a) (b)

Fig. 16: IV (a) and secret key(b) sensitivity for 1000 times.




(a) Recurrence (b) PDF

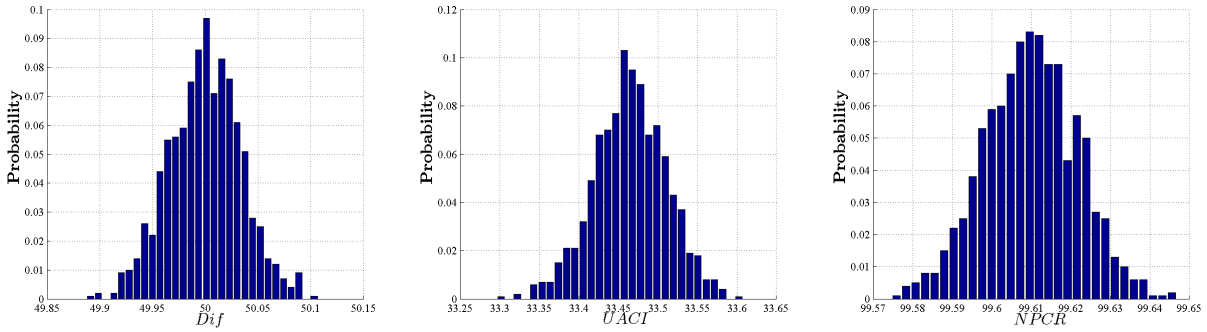
Fig. 17: The Independance (Recursivity) (a) and the PDF (b) of the produced pseudo-random masking sub-matrices by employing the proposed scheme (see Fig. 3) for a random secret key.

Table 4: SSIM and PSNR in selective approaches

| Images | Aorta | Head-3D | Brain |
|---|---|---|---|
| PSNR (SE1) | 15.019 | 11.268 | 9.168 |
| PSNR (SE2) | 13.1 | 10.44 | 7.91 |
| PSNR (MF) | 9.805 | 9.1841 | 7.038 |
| PSNR (Full approach) | 8.2682 | 8.2965 | 8.3262 |
| | | | |
| SSIM (SE1) | 0.53097 | 0.49250 | 0.0376 |
| SSIM- (SE2) | 0.4199 | 0.391 | 0.0114 |
| SSIM (MF) | 0.211 | 0.212 | 0.01291 |
| SSIM (Full approach) | 0.0313 | 0.0360 | 0.0408 |

$SSIM$ falls within the interval [0,1]; a value of 0 means that there exists no correlation between the original and the cipher image, while a value close to 1 means that the two images are approximately the same.

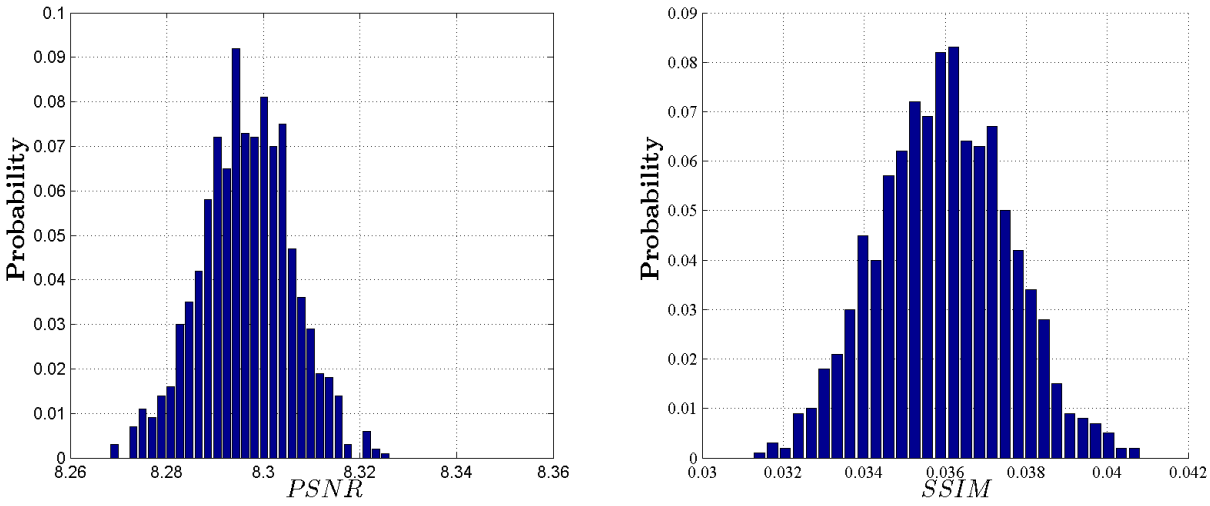
According to the obtained results of PSNR and SSIM, all cipher variants introduce visual degradation since low values of PSNR and SSIM are obtained. In fact, the full cipher variant reaches the maximum hard




(a) Diff (b) UACI (c) NPCR

Fig. 18: The PDF of the difference between original and encrypted Lenna in bits (a), UACI (b) and NPCR(c) for h=8

visual degradation, which is normal since all original sub-matrices are encrypted compared to the selective cipher variants. In addition, the visual degradation of the middle cipher approach achieves better visual degradation compared to the selective variants. Note that no useful information can be detected from the encrypted ROI sub-matrices, but only the type of the medical image can be known.




(a) (b)

Fig. 19: PDF of PSNR, and SSIM for the full encrption approach for $h = 8$

### 7.7 Execution Time

Execution time is a crucial metric for any cipher; a low computational complexity translates into low latency and hence, low resources are needed for the ciphering/deciphering process. This ensured the cipher applicability to real-time systems and for devices with limited resources. The average calculation time (for $1,000$ iterations) to encrypt the plain Lenna image of size $256 \times 256 \times 1$ is performed using the following software and hardware specifications: **Matlab R2013b simulator, micro-computer Intel Core 2 Duet,**

**3 GHZ CPU, 2 GB RAM Intel and Microsoft Windows 7**. The execution time of the three approaches were measured; when only permutation is done on Lenna image ($512 \times 512$), the average time is 0.0156 sec and designated by $t1$. For SE2, time is $t2 = 3 \times t1$. For the full encryption time is $t3 = 4 \times t1$. In case of full encryption, the execution time is dependent of the size of ROB. For example, if it is 50% of the plain image, the encryption time is $t4 = 2 \times t2 = 6 \times t1$. If the application is time- or resource- sensitive, the user can select the approach that best suits the application requirements.

## 8 Discussion and Cryptanalysis

The average of PSNR and SSIM between the original and encrypted images are presented for the different variants in Table 4 for $1,000$ dynamic keys. The results show that selective encryption has an average visual degradation since it is designed only for ROI zones. Also, the visual degradation of the MF variant is close to the full one. Sure, hard visual degradation can be ensured by using the full scheme. The user can choose any variant to protect the medical image contents. Our goal is to provide a flexible solution according to the limitations and requirements for the medical image.

In addition, the distribution of PSNR and SSIM are shown in Figure 19 for the full variant. The obtained results show that a low values of PSNR and SSIM are achieved and this confirms that the proposed encryption technique yields a high difference between the original and encrypted images. Consequently, a high and hard visual distortion is attained by using the proposed full encryption process. As a conclusion, the proposed scheme gives a sufficient visual degradation for the selective and MF variants and hard degradation for the full one. Indeed, for all these variants, no useful information about the original plain image could be revealed from the cipher image.

By only shuffling the data, the system will not be immune against the different attacks if the secret key is static. However, the proposed approach is based on a dynamic key in order to ensure the forward and backward secrecy. Permutation process is based on changing the pixels positions without affecting their values. hence, this motivates the introduction of the other variants to ensure better resistance against future powerful attacks. Indeed, introducing the masking function ensures the change in the pixels positions as well as values. Moreover, by employing a dynamic non-linear element, the substitution table (S-box), a better randomness degree is achieved and better immunity against powerful attacks is attained. We applied the proposed cipher with the different variants on different images. In selective and middle-full approaches, the PDF of cipher ROI sub-matrices or the whole cipher image in case of full variant tend to become uniform. This proves that the proposed scheme can resist statistical attacks since the spatial redundancy between adjacent pixels of the image is removed ensuring a good scrambling of the image. Moreover, other tests such as entropy analysis and correlation tests have validated the robustness of proposed variants (except SE1) and their high resistance to statistical attacks. Moreover, key sensitivity is analyzed and the results showed that the proposed cipher can resist chosen/known plain-text attacks.

Additionally, the key space of the secret key is flexible and can be $2^{128}$, $2^{196}$ and $2^{256}$, while the size of the dynamic key is $2^{512}$. These sizes are sufficiently large to make the brute-force attack unfeasible. Therefore, the system can resist the cipher-text-only attack. Also, an important issue that must be highlighted here is the use of a dynamic key instead of a fixed one. Even if a cryptanalyst has complete knowledge of the used primitives (substitution and permutation techniques) for a plain image, she/he will fail to extract information about the future plain images from the future cipher images, since they lack the dynamic key that is changed for every input image.

Table 5: Compare approaches

| Approach | SE-1 | SE-2 | MF | Full Encryption |
|---|---|---|---|---|
| Computation Complexity | + | ++ | +++ | +++ |
| Visual Degradtion | + | ++ | +++ | ++++ |
| Memory | + | ++ | +++ | ++++ |
| Pipelining | +++ | +++ | +++ | +++ |
| Error Propagation | +++ | +++ | +++ | ++++ |
| Level of Security | + | ++ | +++ | ++++ |

## 9 Conclusion

In this paper, a cipher scheme with three variants (selective, middle-full, and full) is presented to protect medical images. The scheme is based on dynamic diffusion and/or confusion primitives for each input image, which ensures good cryptographic performance. The round number is reduced without degrading the security level, which is a hard challenge that is solved in this paper. The proposed scheme presents a dynamic key derivation function that generates the dynamic key and consequently the required sub-keys that are used to construct the basic primitives of the cipher. To perform encryption/decryption, two main primitives are exploited: sub-matrix permutation and a proposed masking function were applied at the sub-matrix level. Then, several security analysis and system performance tests were conducted to prove the credibility of the proposed cipher scheme. As a conclusion, the proposed approaches can be considered as good competitors to the current medical image applications that have to ensure patients privacy and data confidentiality.


## Acknowledgement

This paper is partially funded by the Lebanese National Council for Scientific Research and by the Labex ACTION program (contract ANR-11-LABX-01-01).


## References


1. Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
2. Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.
3. Marie Babel, François Pasteau, Clément Strauss, Maxime Pelcat, Laurent Bédat, Médéric Blestel, and Olivier Déforges. Preserving data integrity of encoded medical images: the lar compression framework. In *Advances in Reasoning-Based Image Processing Intelligent Systems*, pages 91–125. Springer, 2012.
4. Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo M Eghan, and Nii Narku Quaynor. A security technique for authentication and security of medical images in health information systems. In *Computational Science and Its Applications (ICCSA), 2015 15th International Conference on*, pages 8–13. IEEE, 2015.
5. Miles E Smid and Dennis K Branstad. Data encryption standard: past and future. *Proceedings of the IEEE*, 76(5): 550–559, 1988.
6. Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.
7. Bruce Schneier. The idea encryption algorithm-the international data encryption algorithm (idea) may be one of the most secure block algorithms available to the public today. bruce examines its 128-bit-long key. *Dr Dobb's Journal-Software Tools for the Professional Programmer*, 18(13):50–57, 1993.
8. Jianzhong Li, Qun Lin, Chuying Yu, Xuechang Ren, and Ping Li. A qdct-and svd-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram. *Soft Computing*, 22(1):47–65, 2018.
9. Jian Xu, Laiwen Wei, Yu Zhang, Andi Wang, Fucai Zhou, and Chong-zhi Gao. Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. *Journal of Network and Computer Applications*, 2018.
10. Yuan-Gen Wang, Guopu Zhu, and Yun-Qing Shi. Transportation spherical watermarking. *IEEE Transactions on Image Processing*, 2018.
11. Chuan Qin and Xinpeng Zhang. Effective reversible data hiding in encrypted image with privacy protection for image content. *Journal of Visual Communication and Image Representation*, 31:154–164, 2015.
12. Chuan Qin, Xueqin Chen, Xiangyang Luo, Xinpeng Zhang, and Xingming Sun. Perceptual image hashing via dual-cross pattern encoding and salient structure detection. *Information Sciences*, 423:284–302, 2018.
13. Ya Li, Guangrun Wang, Lin Nie, Qing Wang, and Wenwei Tan. Distance metric optimization driven convolutional neural network for age invariant face recognition. *Pattern Recognition*, 75:51–62, 2018.
14. William Puech and Jose Marconi Rodrigues. Crypto-compression of medical images by selective encryption of dct. In *Signal Processing Conference, 2005 13th European*, pages 1–4. IEEE, 2005.
15. Alfred Bruckmann and Andreas Uhl. Selective medical image compression techniques for telemedical and archiving applications. *Computers in Biology and Medicine*, 30(3):153–169, 2000.
16. Ping Li, Tong Li, Zheng-An Yao, Chun-Ming Tang, and Jin Li. Privacy-preserving outsourcing of image feature extraction in cloud computing. *Soft Computing*, 21(15):4349–4359, 2017.
17. Tao Xiang, Kwok-wo Wong, and Xiaofeng Liao. Selective image encryption using a spatiotemporal chaotic system. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 17(2):023115, 2007.
18. Yang Ou, Chul Sur, and Kyung Hyune Rhee. Region-based selective encryption for medical imaging. In *Frontiers in Algorithmics*, pages 62–73. Springer, 2007.
19. Zahia Brahimi, Hamid Bessalah, A Tarabet, MK Kholladi, et al. Selective encryption techniques of jpeg2000 codestream for medical images transmission. *WSEAS Transactions on Circuits and Systems*, 7(7):718–727, 2008.
20. Sammoud Ali and Adnen Cherif. Performances analysis of image encryption for medical applications. *Journal of Information Sciences and Computing Technologies*, 1(1):78–87, 2015.

21. HT Panduranga and SK Naveenkumar. Selective image encryption for medical and satellite images. *International Journal of Engineering and Technology (IJET)*, 5(1):115–121, 2013.
22. Sukalyan Som and Sayani Sen. A non-adaptive partial encryption of grayscale images based on chaos. *Procedia Technology*, 10:663–671, 2013.
23. A Mostefaoui, H Noura, and Z Fawaz. An integrated multimedia data reduction and content confidentiality approach for limited networked devices. *Ad Hoc Networks*, 32:149–156, 2015.
24. Daniel Schonberg, Stark C Draper, Chuohao Yeo, and Kannan Ramchandran. Toward compression of encrypted images and video sequences. *IEEE Transactions on Information Forensics and Security*, 3(4):749–762, 2008.
25. Xinpeng Zhang, Guangling Sun, Liquan Shen, and Chuan Qin. Compression of encrypted images with multi-layer decomposition. *Multimedia tools and applications*, 72(1):489–502, 2014.
26. Jiantao Zhou, Xianming Liu, and Oscar C Au. On the design of an efficient encryption-then-compression system. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2872–2876. IEEE, 2013.
27. Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng. Compressing encrypted images with auxiliary information. *IEEE Transactions on Multimedia*, 16(5):1327–1336, 2014.
28. Yicong Zhou, Karen Panetta, and Sos Agaian. A lossless encryption method for medical images using edge maps. In *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*, pages 3707–3710. IEEE, 2009.
29. Ahmed B Mahmood and Robert D Dony. Segmentation based encryption method for medical images. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pages 596–601. IEEE, 2011.
30. A Kanso and M Ghebleh. An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation*, 24(1):98–116, 2015.
31. *Digital imaging and communications in medicine (DICOM) Part 15: Security and System Management Profiles.* National Electrical Manufacturers Association and American College of Radiology, 2004.
32. Marcelo Fornazin, Danilo BS Netto Jr, Marcos Antonio Cavenaghi, and Aparecido N Marana. Protecting medical images with biometric information. In *Advances in Computer and Information Sciences and Engineering*, pages 284–289. Springer, 2008.
33. Koredianto Usman, Hiroshi Juzoji, Isao Nakajima, Soegijardjo Soegidjoko, Mohamad Ramdhani, Toshihiro Hori, and Seiji Igi. Medical image encryption based on pixel arrangement and random permutation for transmission security. In *e-Health Networking, Application and Services, 2007 9th International Conference on*, pages 244–247. IEEE, 2007.
34. JB Lima, F Madeiro, and FJR Sales. Encryption of medical images based on the cosine number transform. *Signal Processing: Image Communication*, 35:1–8, 2015.
35. MS Baptista. Cryptography with chaos. *Physics Letters A*, 240(1):50–54, 1998.
36. Yin Dai and Xin Wang. Medical image encryption based on a composition of logistic maps and chebyshev maps. In *Information and Automation (ICIA), 2012 International Conference on*, pages 210–214. IEEE, 2012.
37. Med Karim Abdmouleh, Ali Khalfallah, and Med Salim Bouhlel. Dynamic chaotic look-up table for mri medical image encryption. In *the International Conference On Systems, Control, Signal Processing And Informatics (SCSI 2013)*, pages 16–19, 2013.
38. M Ghebleh, A Kanso, and H Noura. An image encryption scheme based on irregularly decimated chaotic maps. *Signal Processing: Image Communication*, 29(5):618–627, 2014.
39. Chong Fu, Ye Lin, Hui-yan Jiang, and Hong-feng Ma. Medical image protection using hyperchaos-based encryption. In *Medical Information and Communication Technology (ISMICT), 2015 9th International Symposium on*, pages 103–107. IEEE, 2015.
40. Li-bo Zhang and Ben-qiang Yang. An efficient cryptosystem for medical image encryption. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8(7):327–340, 2015.
41. Meghdad Ashtiyani, Parmida Moradi Birgani, and Hesam M Hosseini. Chaos-based medical image encryption using symmetric cryptography. In *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, pages 1–5. IEEE, 2008.
42. Yushu Zhang and Di Xiao. Cryptanalysis of s-box-only chaotic image ciphers against chosen plaintext attack. *Nonlinear Dynamics*, 72(4):751–756, 2013.
43. Yuansheng Liu, Jie Tang, and Tao Xie. Cryptanalyzing a rgb image encryption algorithm based on dna encoding and chaos map. *Optics & Laser Technology*, 60:111–115, 2014.
44. Li Zeng and RenRen Liu. Cryptanalyzing a novel couple images encryption algorithm based on dna subsequence operation and chaotic system. *Optik-International Journal for Light and Electron Optics*, 126(24):5022–5025, 2015.
45. Xingyuan Wang and Lintao Liu. Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos. *Nonlinear Dynamics*, 73(1-2):795–800, 2013.
46. Li-Bo Zhang, Zhi-Liang Zhu, Ben-Qiang Yang, Wen-Yuan Liu, Hong-Feng Zhu, and Ming-Yu Zou. Cryptanalysis and improvement of an efficient and secure medical image protection scheme. *Mathematical Problems in Engineering*, 2015, 2015.
47. Lei Chen and Shihong Wang. Differential cryptanalysis of a medical image cryptosystem with multiple rounds. *Computers in biology and medicine*, 65:69–75, 2015.
48. Feng Huang and Yong Feng. Security analysis of image encryption based on twodimensional chaotic maps and improved algorithm. *Frontiers of Electrical and Electronic Engineering in China*, 4(1):5–9, 2009.
49. David Arroyo, Chengqing Li, Shujun Li, Gonzalo Alvarez, and Wolfgang A Halang. Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. *Chaos, Solitons & Fractals*, 41(5):2613–2616, 2009.
50. Gonzalo Alvarez and Shujun Li. Cryptanalyzing a nonlinear chaotic algorithm (nca) for image encryption. *Communications in Nonlinear Science and Numerical Simulation*, 14(11):3743–3749, 2009.
51. Zhijie Jerry Shi. Bit permutation instructions: Architecture, implementation and cryptographic properties. *Princeton University, Princeton, NJ*, 2004.
52. Howard M Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.
53. Eli Biham and Adi Shamir. *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.