applied sciences

MDPI

Article

Automatic Selective Encryption of DICOM Images

Qamar Natsheh [1,*], Ana Sălăgean [2], Diwei Zhou [3,*] and Eran Edirisinghe [4]

[1] School of Computer Science, University of Birmingham, Birmingham B15 2TT, UK
[2] Department of Computer Science, Loughborough University, Loughborough LE11 3TT, UK
[3] Department of Mathematical Sciences, Loughborough University, Loughborough LE11 3TT, UK
[4] Vice-Chancellor's Office, Keele University, Keele, Newcastle ST5 5BG, UK
* Correspondence: q.natsheh@bham.ac.uk (Q.N.); d.zhou2@lboro.ac.uk (D.Z.)

Abstract: Securing DICOM images is essential to protect the privacy of patients, especially in the era of telemedicine and eHealth/mHealth. This increases the demand for rapid security. Nevertheless, a limited amount of research work has been conducted to ensure the security of DICOM images while minimizing the processing time. Hence, this paper introduces a selective encryption approach to reduce the processing time and sustain the robustness of security. The proposed approach selects regions within medical images automatically in the spatial domain using the pixel thresholding segmentation technique, then compresses and encrypts them using different encryption algorithms based on their importance. An adaptive two-region encryption approach is applied to single and multi-frame DICOM images, where the Region of Background (ROB) is encrypted using a light encryption algorithm, while the Region of Interest (ROI) is encrypted using a sophisticated encryption algorithm. For multi-frame DICOM images (Approach I), additional time-saving has been achieved by almost 10,000 times faster than the Naïve encryption approach, and 100 times better compression ratio, using one segmentation map based on a pre-defined reference frame for all the DICOM frames. For single-frame DICOM image (Approach II), a multi-region selective encryption approach is proposed, where the ROI is further split into three regions based on potential security threats, using a mathematical model that guarantees shorter encryption time in comparison with the Naive and the two-region encryption approaches, with almost 47% and 14% saving times, respectively. Based on the estimated processing time, Approach I outperformed Approach II noticeably. Further, cryptanalysis metrics are utilized to evaluate the proposed approaches, which indicate good robustness against a wide variety of attacks.

Keywords: medical image encryption; selective encryption; region of interest; segmentation; LZ4 compression; multi-frame DICOM object

Citation: Natsheh, Q.; Sălăgean, A.; Zhou, D.; Edirisinghe, E. Automatic Selective Encryption of DICOM Images. *Appl. Sci.* **2023**, *13*, 4779. https://doi.org/10.3390/app13084779

Academic Editor: Jan Egger

Received: 20 March 2023
Revised: 3 April 2023
Accepted: 7 April 2023
Published: 11 April 2023

1. Introduction and Related Work

Several frameworks have been introduced to facilitate medical data processing, archiving, and exchanging, such as Picture Archiving and Communication System (PACS). PACS is recognized in medical organizations and institutes. Alongside PACS, there are workstations, imaging devices, networks, and many other hardware devices, which are utilized in medical organizations. This creates the need to integrate, exchange, secure, and archive medical data from all these devices, from different manufacturers with minimum cost. To this end, Digital Imaging and Communications in Medicine (DICOM) is the most common standard which is adopted by most of the medical institutes and manufacturers who define methods to achieve all required functionalities [1,2].

The security mechanisms were missing in the initial version of the DICOM standard [1], which means that sensitive medical data were exchanged as plain text. As a result of the exponential growth of using the Internet, more strict security requirements arose, especially in the medical sector. Accordingly, the DICOM standard introduces some security improvements which are integrated into DICOM objects and their related applications.

Nonetheless, most of these mechanisms are not enough to ensure a robust security solution, especially for multimedia data. Moreover, these recommendations do not include the pixel data of the DICOM object. Accordingly, many research works have proposed security mechanisms for pixel data to extend the DICOM standard.

Security requirements for medical images are derived from strong ethics and legal regulations for privacy, and they need to fulfill the confidentiality and reliability requirements, to prevent tampering that can occur during the transmission time through a malicious individual that leads to an incorrect diagnosis. Such acts might cause severe problems as well as patient death. Security needs for medical data (text, audio, image, and video) can be classified into three categories [3]: confidentiality, reliability, and availability. Patients' health data privacy is one of the most critical issues to be considered among individuals' information [4]. Therefore, medical data confidentiality is considered a crucial security requirement. Encryption is a technique used to provide data confidentiality by ensuring the incomprehensibility of data to unauthorized parties, and several encryption algorithms have been proposed to encrypt the entire pixel data and/or header data. However, traditional encryption algorithms, such as RSA, are not suitable for medical images, due to their pixels' redundancy and complexity [5]. Therefore, the DICOM image size and the complexity of encryption algorithms directly affect the delay time for viewing and exchanging DICOM images amongst distant medical entities and radiologists, in which, the encryption algorithm processing time is proportional to the DICOM image size [6,7].

Related Work

Many research works focus on the nature of the DICOM image data before and after the encryption, while ignoring the real-time requirements. Hence, encrypting large DICOM images using Naïve approach have a large processing time overhead. In the literature, many research works have proposed the use of a selective encryption approach to overcome the processing time limitations for multimedia data. However, fewer numbers of research works have been conducted on the use of selective encryption on medical images, specifically DICOM images. The basic idea of selective encryption is to encrypt the informative subsets of the data using a robust encryption algorithm while encrypting other subsets using a lighter encryption algorithm. Further, the selection and encryption processes of data subsets can be performed in the frequency or spatial domain. Furthermore, the selective approach has a better processing time than the Naïve approach, but on the other hand, the Naïve approach is considered to be more robust.

Most of the utilized image encryption techniques for medical applications in the literature are chaotic-based Naïve encryption, while a small number of research works have presented conventional-based image encryption approaches. Additionally, a smaller number of research works have proposed the use of both conventional and chaotic-based approaches (hybrid). Moreover, most of the presented encryption research works in the multimedia domain have proposed encryption approaches in the frequency domain with selective chaotic-based techniques.

The idea of selective encryption was first presented by Spanos and Maple [8] in 1995. Many research works have proposed to conduct selective encryption in the spatial domain as in [9–17]. Nonetheless, the frequency domain predominates the selection encryption as proposed in [18–22]. Though, spatial domain selective encryption is an attractive choice as it is simple and does not require any transformation of pixel intensities into other domains.

The primary goal of using selective encryption algorithms is to minimize the encryption and decryption time. However, only a few research works have tried to optimize the encryption effort (time) while encrypting the data. In study [13], a novel selective symmetric encryption approach was reported for medical images. It employs GA to optimize the encryption process, in which the image is segmented into a number of regions, and the ROI is selected on the basis of pixel intensity and entropy measurements. After that, encryption algorithms with variable key lengths are selected to encrypt regions in the ROI, where each region is encrypted using an encryption algorithm that guarantees its confi-

dentiality while minimizing the processing time. However, the bitstream of this method is not coherent; also, GA does not guarantee to find the global minimum of the optimization problem, and it does not provide a comprehensive solution. Other research works have proposed the use of swarm optimization to identify the key length that improves security or reduces the encryption time [23]. The main drawback of these optimization-based approaches is that it increases the complexity of the encryption problem. Moreover, all the referenced approaches above did not consider an objective function based on the nature of the encryption approach.

Spatial domain selective encryption approaches in the literature require user input to perform segmentation (manual segmentation) and do not exploit any statistical properties of medical images. On the other hand, the frequency-based selective encryption approaches gain more attention than spatial-based ones, and most of the presented works in the frequency domain perform data selection automatically without a need for user input. In this work, we present an automatic selective encryption approach in the spatial domain that aims to reduce the processing time overhead of the utilized encryption algorithms and to adaptively threshold DICOM images based on their modalities, anatomy part, and pixel intensity range, while maintaining the security of the encrypted DICOM image, in comparison with the Naïve encryption approach, in which all pixel data are encrypted using sophisticated encryption algorithm, e.g., Advanced Encryption Standard (AES), as the bottleneck of securing a DICOM object is the processing time [24]. It is worthwhile to mention that AES is adopted by the DICOM standard.

This paper introduces encryption approaches for single- and multi-frame DICOM objects while utilizing a two-region selective encryption approach based on an automatic statistical-based segmentation approach to select important pixel data in DICOM images [25]. The single-frame encryption approach was adopted after a thorough investigation of a mathematical solution based on a linear equation system to work out multi-region sizes inside the ROI of the DICOM image to encrypt them based on their importance. However, the saving time was not highly improved in comparison with the proposed approach in study [25]. Therefore, a promising approach was adopted based on the idea of improving the redundancy of the segmented pixel data. This approach has two proposed segmentation mechanisms that segment DICOM images into ROI and ROB based on pixel intensities. Thus, segmented regions are compressed using a fast-lossless compression algorithm. Consequently, the encryption process of the selected data can be significantly reduced. The proposed approach aims to reduce the processing time of multi-frame DICOM image encryption in comparison with the Naïve encryption approach. Effective time performance and robustness of the proposed approach are verified by statistical assessments and cryptanalysis measurements. Therefore, the proposed approach can be exploited with various frameworks to attain data security requirements.

This paper is structured as follows: Section 2 gives an overview of the motivations and limitations of encrypting DICOM images. The proposed approach is detailed in Section 3. Performance evaluation, analysis, and discussions are described in Section 4. Concluding comments, challenges, and future work are given in Section 5. Calculations of regions' sizes of the multi-region encryption approach are presented in Appendix A.

2. The DICOM Image Encryption: Motivations and Limitations

The Health Insurance Portability and Accountability Act (HIPAA) recommended that all data that might be used to identify all entities (e.g., patient, physician, etc.) must be confidential and only authorized entities can access them. However, the DICOM standard does not support encryption for pixel data. DICOM secures patients' information using the Application Level Confidentiality Profile. However, this does not necessarily guarantee confidentiality. For instance, if an attacker already has access to the pixel data or part of it, it can be used to identify the patient's identity [1]. The supplementary documents of the DICOM standard highlight these risks on the NEMA website, as shown in [26–28].

Several research works have been conducted in the literature to extend the DICOM standard with pixel encryption mechanisms. However, these mechanisms increase the processing time overhead, which causes additional delay and requires more computational resources. Hence, it is very important to provide an efficient and simple mechanism, especially in the era of telemedicine and handheld devices.

2.1. Limitations

Generally speaking, DICOM images contain sensitive information about patients and are usually saved for a long time, so they should be stored safely and far from any malicious threats. Additionally, the images might need to be exchanged with different medical entities over public networks. However, there are no existing recommendations on how to secure the DICOM pixel data, while the only existing recommendations are intended to anonymize (de-identification) the patient information that is found in the header data of the DICOM images to preserve the privacy of the patient data. Hence, it is preferable to use quite accepted and adopted encryption standards to secure medical image databases such as 3DES and AES. These algorithms' processing time is not short, and the size of the medical images is large, so the encryption time of medical images may take a long processing time. Accordingly, encryption mechanisms should be developed to reduce the processing time while maintaining security robustness [20].

For instance, if the physician would like to secure the pixel data of 100,000 DICOM images (with 2760 $\times$ 1200 size and 16-bit depth) before sharing it with another hospital, she/he might use the Naïve encryption method to encrypt the pixel data of the DICOM frames using conventional (sophisticated) and adopted encryption algorithms by the DICOM standard, such as AES. In this case, the processing time of the encryption process will reach around 4 h, which is a lack of efficiency and a delay for the limited time of physicians. This represents a challenge to be implemented in real life, and therefore, the DICOM standard left this problem open for research, leaving the decision for the researchers on how to secure the DICOM standard.

Selective encryption mechanisms are promising methods that can overcome traditional encryption limitations. Since selective encryption mechanisms aim to reduce the sizes of the regions, which are subjected to sophisticated encryption algorithms such as AES, consequently, time and cost will be reduced. The main gap in selective image encryption is the classification (segmentation) of images into significant and insignificant regions. In the literature, most of the reported research works proposed a manual selection of regions which is impractical and added extra burden on the medical processing time. Moreover, within the author's knowledge, none of the reported research works has utilized the medical images' statistical properties to efficiently select regions for selective encryption. As image segmentation can be performed in the frequency or spatial domain, most of these research works segmented medical images into regions in the frequency domain. In this case, frequency-segmentation algorithms depend on image features that exist in the frequency domain; hence, additional computations are required to extract features prior to the segmentation process.

2.2. Proposed Extension to the DICOM Standard and Other Frameworks

The primary goal of this paper is to reduce the required encryption time of DICOM images. Most of the presented work in the literature developed codes in MATLAB. Hence, the encryption speed was limited. Nevertheless, this paper focuses on finding efficient libraries that have compiled C code implementation. Additionally, all the developed methods in this paper were implemented using Python and then compiled into C code using Cython Library. Hence, the presented work can be implemented in real platforms to support and extend DICOM applications.

It is worthwhile to mention that the work presented in this paper does not aim to provide security requirements (confidentiality, authenticity, and integrity). This paper provides an effective encryption mechanism to reduce the encryption time, as it is the

bottleneck to generating a secure DICOM object [24]. This mechanism can be used within a security framework to achieve these security requirements, such as authenticity and integrity in the presented framework by Kobayashi et al. [24] as shown in Figure 1. In this framework, a segmentation map is generated based on the proposed approach, will be stored in the header, and then used to encrypt pixel data as suggested in the Kobayashi framework. Interested readers can find out more about this framework in [24].

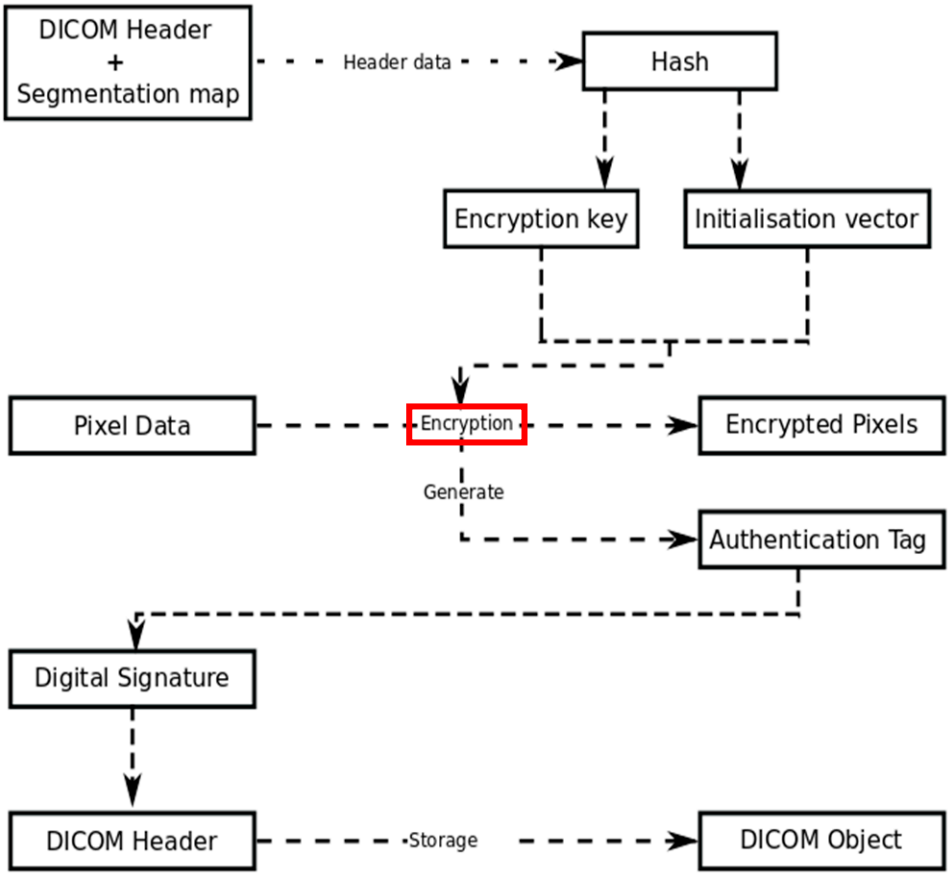


Figure 1. Encryption flow chart: Kobayashi framework, the proposed approach can contribute to reducing the computational overhead of the encryption process (red box).

In addition to the Kobayashi framework, the proposed approach can be used to achieve confidentiality goals, by extending the Kobayashi framework as shown in Figure 2. As the DICOM standard recommended certificate-based encryption [1], the encryption of the header data (including the segmentation map) can be achieved using RSA. This kind of secret data exchange is supported by Transport Layer Security (TLS) which is also recommended by the DICOM standard in Part 15, Annex B. In this extended framework, the private key on the sender side and the public key on the receiver side are embedded in a Digital Certificate (DC). The DC is generated by an independent Certification Authority (CA) which identifies network users and their authorities. In this framework, the proposed approach can efficiently contribute to reducing the required encryption time and achieving authenticity, integrity, and confidentiality.

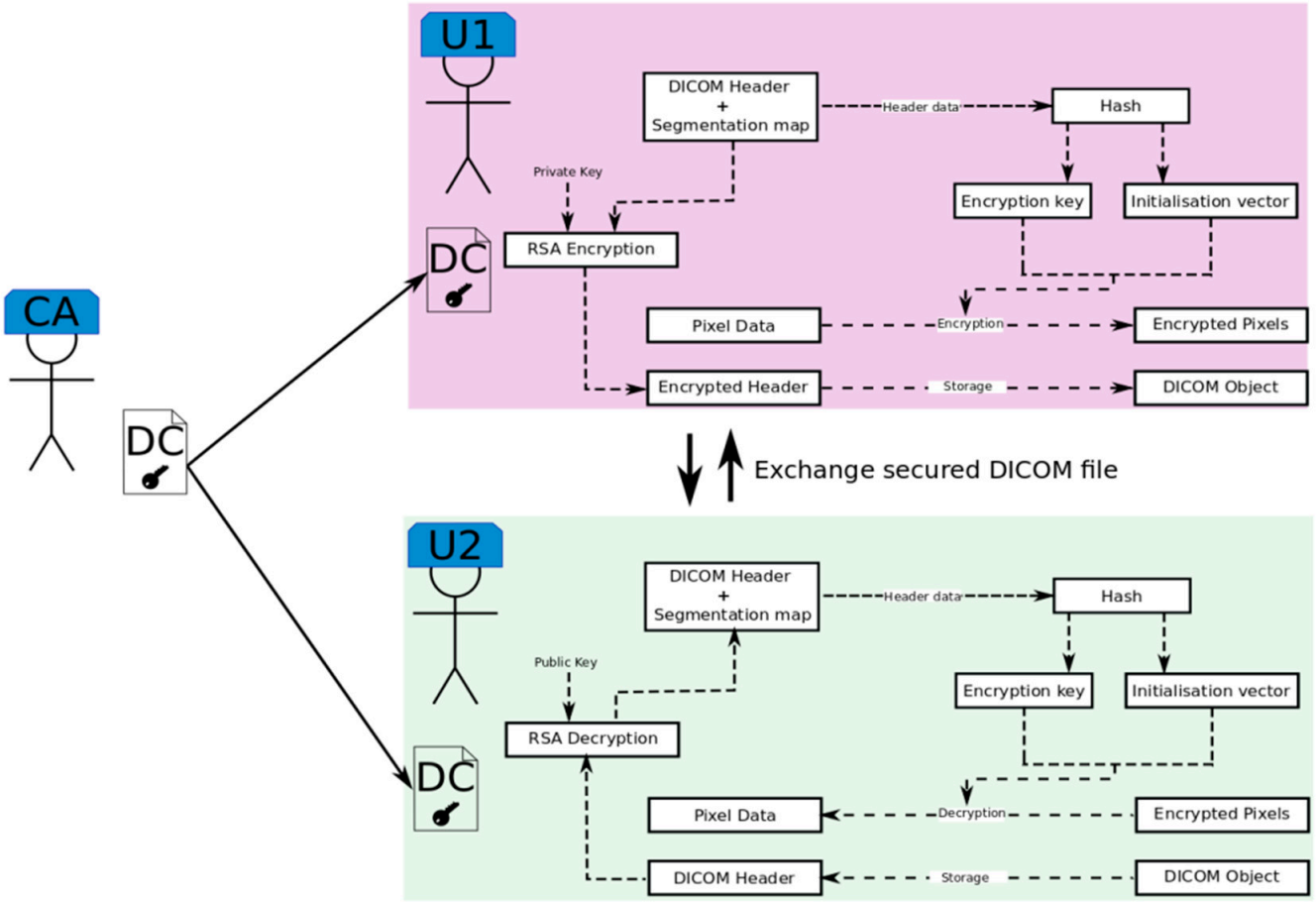


Figure 2. An encryption flow chart that achieves confidentiality on certificate-based encryption.

3. The Proposed Approach

The fundamental concept of the adopted methodology in this paper is depicted in Figure 3. This diagram shows three main stages within the proposed approaches, namely: selection, compression, and encryption. The essential input of the presented approaches in this paper is a DICOM medical image, which is composed of patient data and pixel data. Additional user input might be required to select regions, as in the study [29] and the presented approach in Section 3.2. The expected output is a secured DICOM object which contains anonymized patient data and encrypted pixel data.

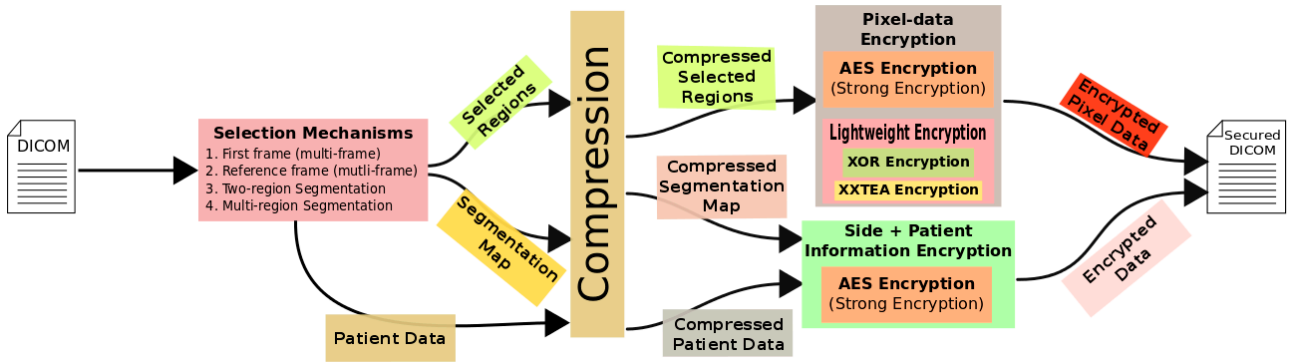


Figure 3. The fundamental concept of the proposed selective encryption process.

In this paper, several selection mechanisms that aim to extract and categorize data prior to the encryption process are adopted. Pixel data are segmented into regions based

on their importance. The output of the segmentation process includes a segmentation map as side information that preserves the original pixels' positions. Then, the patient data and the segmentation map are extracted and combined as side information. For a multi-frame DICOM object, the first DICOM frame is selected as the most crucial frame, as described in [29]. Additionally, in the presented approach in Section 3.2 (multi-frame DICOM object) a combination between a pre-defined reference frame and automatic thresholding based on the two-region encryption approach [25] is adopted. On the other hand, the two-region encryption approach [25] and the presented approach in Section 3.1 (multi-region encryption approach) present automatic selection mechanisms, which rely on the statistical properties of medical images.

Generally, the output from the selection process includes selected regions, a segmentation map, and patient data. In the presented approaches in Sections 3.1 and 3.2, the outputs from the selection mechanism are compressed using a lossless compression algorithm. While in studies [25,29], the outputs from the selection mechanism are directly encrypted. The adopted lossless compression algorithm in this research was Lempel–Ziv 4 (LZ4), which is well-known for its high compression speed and acceptable compression ratio.

In the encryption phase, important pixel data (compressed) were encrypted using AES with 256 key-length, while less critical data were encrypted using AES with 128 key-length, XXTEA, and XOR. The compressed side of information and patient data were encrypted using AES with 256 key-length. Finally, the encrypted data were appended within a secured DICOM object based on part 15 of the DICOM standard. It is worthwhile to mention that XXTEA is selected to demonstrate the proposed approach. However, there are several lightweight encryption methods that would be suitable to encrypt the ROB.

The following Sections 3.1 and 3.2 present two proposed approaches for single-frame DICOM images and multi-frame DICOM objects, respectively.

3.1. Approach I: Multi-Region Selective Encryption Approach for Mammography DICOM Images

A two-region selective encryption algorithm is proposed in the study [25], implemented and evaluated. The selection process for the proposed approach is based on pixels' intensities, where regions are identified based on the pixel thresholding technique. The proposed method is evaluated based on the cryptanalysis metrics, saved time, and the ratio of ROI size to image size. It is noticed that the saved time in images with large ROI size is much smaller than the saving time of images with small-medium ROI size. This highlights the need to enhance the saved time using a multi-region selective encryption algorithm as detailed in this approach.

In this section, a multi-region encryption approach is proposed to work out regions' sizes (R1, R2, R3 within ROI) automatically using some mathematical formulas that guarantee less processing time in comparison with the Naïve and two-region encryption approaches [25], while maintaining security robustness. This experiment was restricted to a Mammography DICOM dataset since each medical image modality and human body part has a different distribution [25,30,31], where dark pixel intensities represent the less informative regions of Mammography DICOM images, while bright pixel intensities represent the informative regions [32,33].

A detailed description of the proposed approach's procedures is given in the following sections after briefly describing pre-knowledge equations used to build the cost lookup table for different encryption algorithms employed in the proposed approach.

3.1.1. Encryption Cost Estimation

In this section, the encryption time for different DICOM images sizes using different encryption algorithms (AES and XXTEA) is modeled and analyzed to extract equations that are used as pre-knowledge information to build a cost lookup table for different encryption algorithms, and it will be used to estimate the processing cost of encrypting parts (regions) of the DICOM images.

A line-fitting tool in Python is used to fit linear equations for encryption time with different key lengths. For example, AES (256-bit) fitted equation is depicted in Figure 4, where its estimated equation is ($Y = 1.05 \times 10^{-8}X + 0.0002$). In general, it can be noticed that processing time is linearly proportional to the image size, and as expected, large images require more time to be encrypted. Moreover, in comparison with AES processing time, the XXTEA is around two times faster than the AES (128-bit) and AES (256-bit), respectively. One last important factor is the hardware specification; this work is performed using an Ubuntu machine, with an Intel i5 processor and 4 GB RAM.

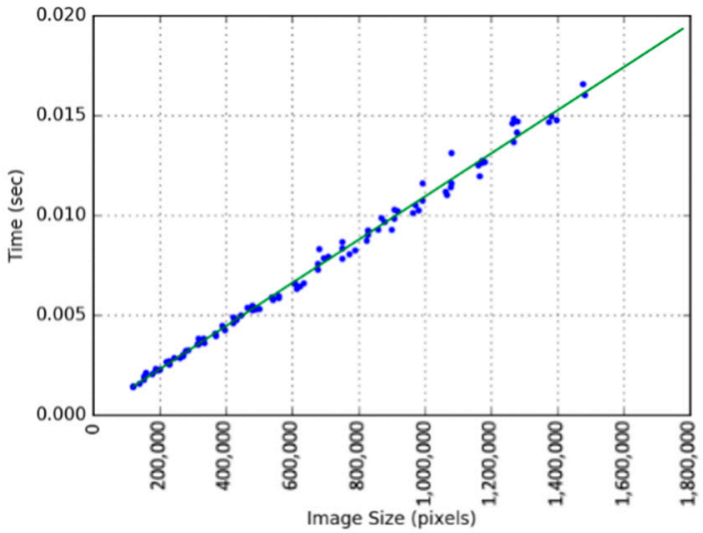


Figure 4. Estimated encryption time of AES 256.

3.1.2. Multi-Region Encryption Process

The elementary idea of the proposed approach is to split the DICOM image ROI into three regions, and then encrypt these regions using different encryption algorithms based on their importance, as it is believed that this will guarantee minimum encryption time in comparison with the Naïve and two-region encryption approaches [25]. In order to achieve that, the three regions' sizes must be calculated, such that the total encryption time of all three regions in addition to the ROB encryption time must be less than the Naïve encryption and the two-region encryption approach times. The reason behind segmenting ROI into three regions is to prove the concept, as two regions are not enough to investigate the efficiency of the proposed approach, and more than three regions will cost more time due to the extra operations of segmentation.

Figure 5 depicts the overall multi-region encryption approach. Firstly, DICOM image regions' sizes are calculated based on the ROI size, where the ROI is determined using extracted thresholds based on the approach described in [25]. Thus, if the ROI size with respect to image size is (~≥55%), pixel data will be segmented into three ROI regions (R1, R2, R3) and ROB. After that, the plain text of all regions is compressed using LZ4 lossless compression. Next, the compressed data are encrypted using AES 256, AES 128, and XXTEA based on their importance. Finally, the ciphertext of all regions is stored in the tag (07FE0, 0010). It is worthwhile to mention that AES is a sophisticated encryption algorithm, and it is adopted by the DICOM standard with an efficient processing time. Therefore, AES was utilized to encrypt the ROI due to its robustness and the importance of that region. While XXTEA is a lightweight encryption algorithm, it is selected to encrypt less important regions such as the ROB to demonstrate the proposed approach. However, there are several lightweight encryption methods that would be suitable to encrypt the ROB.

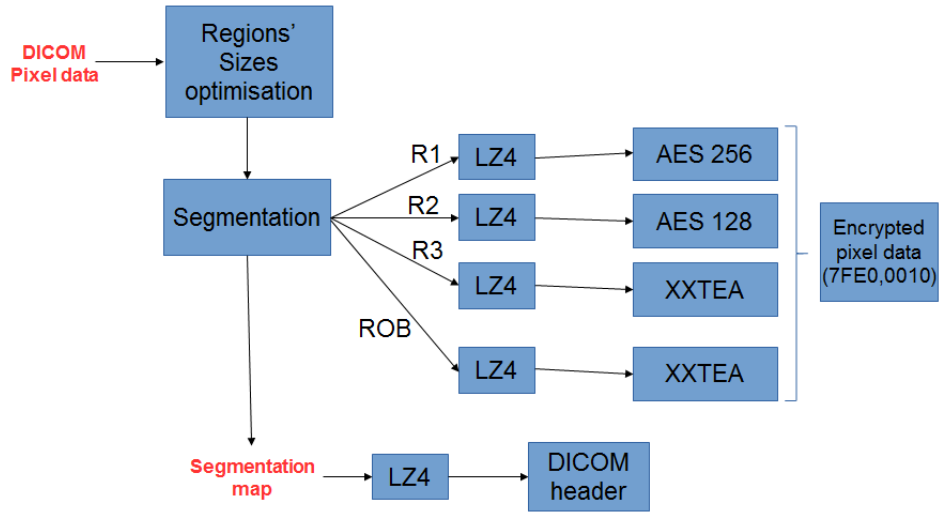


Figure 5. Multi-region encryption process.

3.1.3. ROI Data Distribution and Thresholds' Estimation

As detailed in Appendix A, optimal regions' sizes that guarantee minimum encryption time in comparison with Naïve AES encryption time were calculated based on the proposed Linear System (LSE). Equations (A8)–(A10) show the regions' sizes (number of pixels for each region), but it does not specify which pixels. To identify the pixels for each region, ROB pixels were removed based on the two-region adaptive pixel thresholding approach that was presented in [25]. Then, using pixel intensity distributions of ROI; pixel thresholds that specify each region were estimated as follows:

1. Calculate region probability:

$$P_{ri} = \frac{S_{ri}}{S_{roi}}$$

where S_{ri} is region i size and P_{ri} is region i probability.

2. Sort ROI pixels in descending order (based on pixel intensities).
3. Allocate pixels' intensities that have probability equal to the region probability (R_3), starting at the minimum value of pixels' intensities, until the region probability is reached. Then, assign the region threshold to the maximum reached pixel intensity (th_1). Next, after removing pixels corresponding to R_3, th_2 can be determined based on R_2 probability in the same manner as R_3. Henceforth, thresholds were determined based on the following order $K_3 \rightarrow K_2 \rightarrow K_1$.
4. Segment ROI into multi-region, using estimated pixels' thresholds, where regions are defined as shown below:

$$\begin{gathered} R_3 = ROI(p_x) \leq th_1 \\ R_2 = (th_2 > ROI(p_x) > th_1) \\ R_1 = ROI(p_x) \geq th_2 \end{gathered}$$

where R_1 is region one and it represents the most informative pixels around the mean value of ROI pixel data. R_2 and R_3 are regions two and three, respectively. th_1 and th_2 are the first and the second thresholds estimated in step 3, and $ROI(p_x)$ is pixel x intensity that belongs to the ROI.

3.1.4. Medical Images' Statistical Properties

It was noticed in study [25] that the ROI of each DICOM modality was segmented using different statistical values (thresholds), which indicates that different DICOM modalities have different distributions. A dataset of different modalities and different human body parts was used to fit distributions in this paper, and it is the same one used in study [25].

These distributions can be used as a pre-knowledge to determine threshold values for different modalities, as illustrated in [25].

In general, manual segmentation performed by physicians shows that the statistical properties of the segmented ROI significantly differ from one modality to another. For example, physicians consider the brightest regions as ROI in Mammography DICOM images [32,33]. Hence, as proof of this concept, the study conducted in this approach is restricted to Mammography DICOM images, where 75% of the Mammography dataset has Laplace distribution, and only 25% was Beta distribution. However, 99% of Mammography images are Laplace after removing the background [34]. Figure 6 shows a Mammography DICOM image and its corresponding histogram.

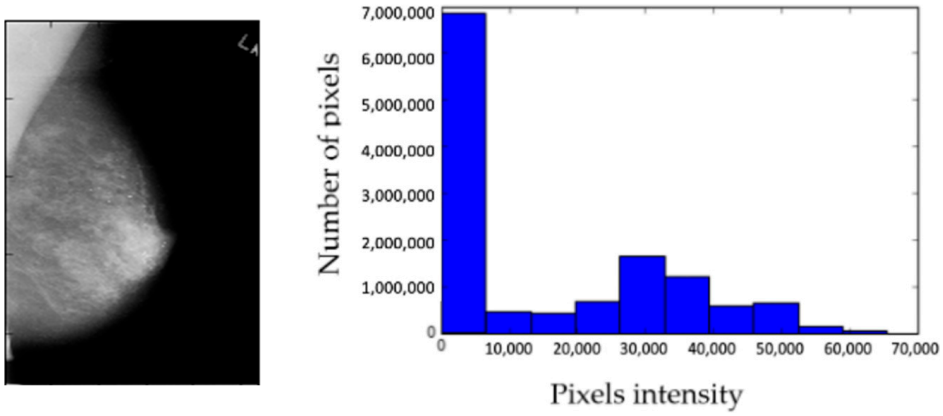


Figure 6. Mammography DICOM image (**a**) and its corresponding histogram (**b**).

The histogram in Figure 6 shows that the ROI's low pixel intensities (~<500) dominate the distribution. Additionally, the brightest region is tiny in comparison with other regions. In the literature, it has been reported that the manual segmentation of Mammography must focus on bright regions [33]. Therefore, the proposed approach in this paper considers pixels with high intensities as the most important regions within the ROI.

3.1.5. Managing Segmentation Map

After segmenting DICOM images, the key to reconstructing the encrypted image is called a segmentation map, which is a matrix that has the same size as the encrypted image and its element represents the region/pixel membership of that element. In the proposed approach, the segmentation map will be appended with the confidential DICOM profile tags. Then, the combined data are compressed using LZ4 as an efficient compression algorithm which can also provide integrity of the compressed data, as it provides a checksum mechanism. It is believed that the combination of the segmentation map with the header will not increase the header encryption time overhead as LZ4 can significantly reduce the size of the segmentation map due to its redundant nature. Finally, the encrypted compressed data (the segmentation map and confidential DICOM profile tags) are stored within the Encrypted Attributes Sequence (0400, 0500).

3.2. Approach II: Automatic Selective Encryption of Multi-Frame DICOM Images

3.2.1. The Multi-Frame DICOM Object

In general, the multi-frame DICOM object is a more compact illustration of a sequence of images (single-frame sequence), that can be transferred as a single entity (single DICOM object), and each frame is identified by a sequence number. The DICOM object attributes must be linked with the pixel data from all frames as one entity. Hence, a multi-frame DICOM object is very useful to save storage space. However, it imposes some limitations in comparison with the single-frame image series; in particular, all frames in the multi-frame

DICOM object must have the same characteristics such as frame size, pixel depth, etc. The total number of frames in the DICOM object is specified by tag (0028, 0008) in the header.

Historically, the multi-frame DICOM object has also not been widely supported by DICOM viewers and the PACS system [35]. Therefore, only a small number of research work has been conducted on how to secure the multi-frame DICOM object. Study [36] highlights the main difference between a multi-frame DICOM object and a single-frame one. It is noticeable that the network delay to store 10,000 single-frame DICOM is ten thousand times more than storing 10,000 multi-frame DICOM object. What is more, each frame requires multiple store requests, store, and store acknowledgement in the single-frame DICOM case, while the multi-frame DICOM object requires only one request, store, and store acknowledgement. In analogy to this, the presented approach in this section introduces a cascade encryption mechanism that is suitable for the storage procedure in [36], while reducing the processing time overhead.

3.2.2. The Multi-Frame Encryption Process

The proposed approach intends to decrease the encryption time burden of the multi-frame DICOM object. Hence, this section presents a hybrid encryption approach that combines a sophisticated encryption algorithm (AES) with a lighter encryption algorithm (XXTEA) to maintain minimum processing time. Thus, the most informative pixels must be encrypted using AES and the rest of the pixels will be encrypted using XXTEA.

In this approach, two segmentation mechanisms are proposed: the first one is a holistic approach that segments all frames simultaneously, while the second approach segments each frame individually. The holistic segmentation approach uses a pre-defined threshold value of [25] to segment all pixel data from all frames. Then, segmented ROI and ROB are compressed, encrypted, and stored in a secured DICOM object. This approach is called Holistic-Based Selective Encryption (Holistic-Based SE). The second segmentation process will be executed in an automatic manner where a specific frame in the middle of the multi-frame DICOM object is selected as a reference frame; then its pixel data can be segmented based on automatic thresholding using a pre-defined threshold value [25]. Thereafter, the resultant segmentation map from the segmented reference frame will be used to segment all other frames in the DICOM object. Afterwards, the segmented ROI and ROB from all frames are compressed and encrypted using AES and XXTEA, respectively. This approach is called Frame-Based Selective Encryption (Frame-Based SE).

Another essential feature that has been examined in this approach is the data redundancy within the multi-frame DICOM object. Since frames in a multi-frame DICOM object represent adjacent frames of the body part, adjacent frames have high similarity (redundancy). In order to employ this redundancy, the proposed approach employs an efficient lossless compression approach called LZ4 which is significantly fast and with a good compression ratio. The proposed approach can be classified as a selective approach as ROI pixels from all frames are encrypted using AES while the rest of the pixels are encrypted using XXTEA.

Holistic-Based SE Approach

A block diagram of the first proposed encryption routine is shown in Figure 7. The input to this procedure is the multi-frame DICOM object and a pre-defined threshold value. Next, the pixel data array that combines all frames is segmented into ROI and ROB. The resultant segmentation map based on this segmentation process has a similar size to the multi-frame pixel data. Hence, the segmentation map is massive in size. Then, the ROI and ROB can be compressed using LZ4 and then encrypted using AES (ROI) and XXTEA (ROB) encryption algorithms. It is worthwhile to mention that the holistic segmentation map of the multi-frame pixel data and the DICOM header data are combined, compressed, and finally encrypted using AES. The output DICOM object is a secured file such that patient data and pixel data are compressed and encrypted.

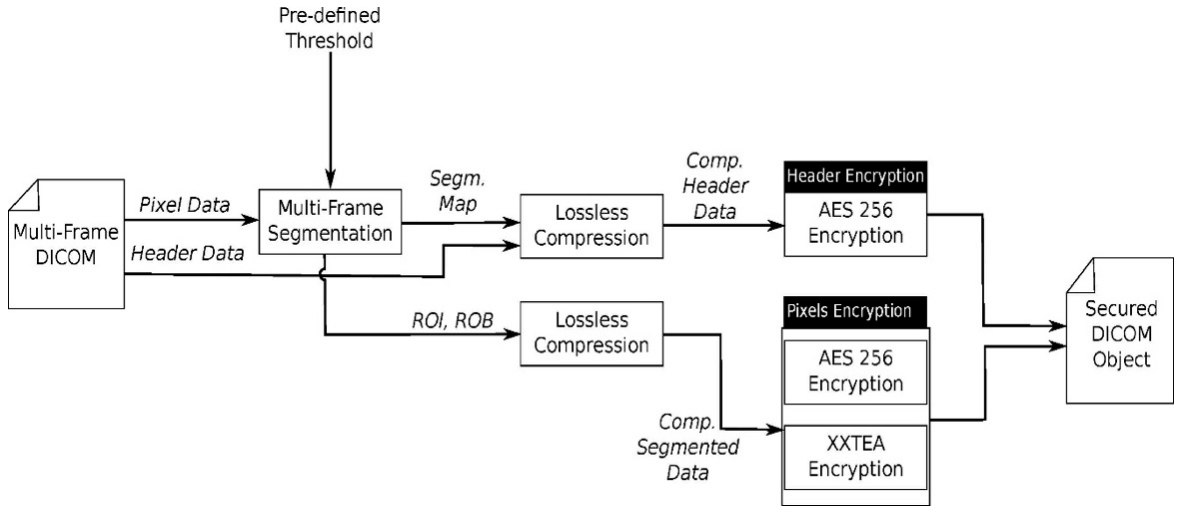


Figure 7. The proposed Holistic-Based SE approach.

Frame-Based SE Approach

Figure 8 illustrates a block diagram of the second proposed encryption procedure. The primary input to this procedure is the multi-frame DICOM object, a pre-defined threshold value and a pre-defined reference frame. Then, the pre-defined reference frame is extracted and segmented. The resultant segmentation map based on the reference frame is used to segment all the frames in the multi-frame DICOM object individually into ROI and ROB. It is believed that this improves data redundancy; hence, ROI and ROB can be compressed using lossless compression. Next, compressed data are encrypted using AES (ROI) and XXTEA (ROB). It is worthwhile to mention that the segmentation map of the reference frame and the DICOM header data are combined, compressed, and finally encrypted using AES. The output DICOM object is a secured file such that patient data and pixel data are compressed and encrypted.

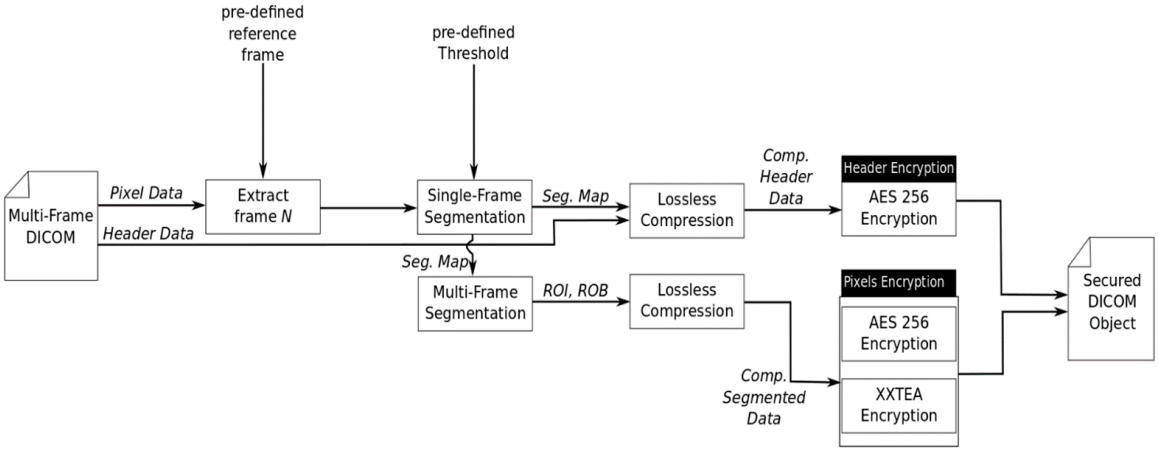


Figure 8. The proposed Frame-Based SE approach.

In comparison with the Holistic-Based SE, the segmentation map dimensions are equal to the dimensions of the single frame in the multi-frame DICOM object. This means that the segmentation map based on the Frame-Based SE is N (number of frames) times smaller than the segmentation map based on the Holistic-Based SE. Another important remark is that the segmentation of all frames' pixel data are performed based on matrix multiplication, which is significantly optimized and efficient due to years of developments in NumPy matrix multiplications on multicore processors. The segmentation map has the same dimensions as a single frame. However, the pixel data of the multi-frame DICOM

object has an additional dimension that represents the frames. NumPy library allows the multiplication of the segmentation map with all frames through an optimized C library. Henceforth, the segmentation process can be described as a single matrix multiplication of the segmentation map with the pixel data to extract the ROI and the ROB.

4. Performance Analysis and Discussion

4.1. Approach I

A Mammography DICOM dataset, with 60 scanned film studies and various sizes with 16-bit depth, is used to evaluate the proposed approach. This dataset is part of the Curated Breast Imaging Subset (CBIS) of Digital Database for Screening Mammography (DDSM) [37], and each image within the given dataset is manually segmented.

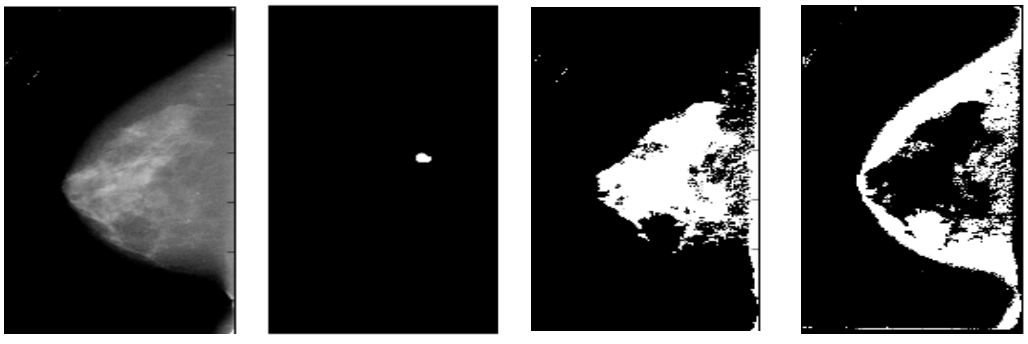
The Mammography dataset is used to evaluate the multi-region segmentation accuracy, and the encryption time based on two-region [25], multi-region, and Naïve encryption approaches. The experiment is conducted using Cython/Python on an Ubuntu machine (Intel i5 at 2.27 GHz). The proposed approach is evaluated based on the processing time and the encryption efficiency. The processing time can be evaluated merely based on the required encryption time, while encryption efficiency is evaluated using cryptanalysis metrics, as detailed in the next sections.

4.1.1. Segmentation Accuracy

As the goal of the presented work is to minimize the encryption time, segmentation accuracy is not crucial to this work. However, it is essential to secure data that is considered important by physicians using sophisticated encryption algorithms. Hence, it is important to provide acceptable accuracy in the segmentation stage in comparison with manual segmentation. Accordingly, the provided dataset is segmented based on the proposed approach, and then compared with the physicians' manual segmentation. A similarity metric in Equation (1) is used to evaluate the quality of the segmentation approach, where R_i is the segmented image of region $i \in \{1, 2, 3\}$ and O_m is the original image:

$$Acc = \frac{\sum R_i(pixels \in ground\ truth)\ AND\ O_m(pixels \in ground\ truth)}{\sum O_m(pixels \in ground\ truth)} \times 100\% \quad (1)$$

The multi-region segmentation of the adopted dataset shows that the adopted approach accuracy is 100% based on the LSE, where 100% of the manually selected area is segmented as the most important region (R1). Figure 9 presents an example of segmented images based on the LSE at security level 1, which means that ROI is segmented into three different regions. However, it was noticed that none of the important pixels was in region 3. As shown in these images, R1 and R2 contain the most important pixels (not the background pixels).



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

Figure 9. Mammography segmentation based on the multi-region approach at security level 1: (**a**) original image, (**b**) ground truth segmentation, (**c**) most important region, and (**d**) the second most important region.

4.1.2. Security Evaluation

PSNR, entropy [38], correlation coefficients (CORR) [39], NPCR [39,40] and UACI [39], and Chi-square [41] metrics are used to evaluate the robustness of the proposed encryption approach. Table 1 indicates the performance overview of the proposed approach, which shows a good level of robustness. The low correlation value indicates robustness against linear attacks as it shows that the proposed approach has a low correlation between the original and the cipher images. The low PSNR and high entropy values show that the encrypted images have a good randomness level. The MAE value shows that the encrypted images are significantly different from the original images. The high NPCR/UACI scores show robustness against differential attacks, which depicts a large difference between the plain and cipher images. On the other hand, the Chi-squared metric value indicates that the encrypted images' distribution is greatly different from the original images.

Table 1. Cryptanalysis results of the 60 CBIS-DDSM Mammography DICOM frames for the multi-region encryption approach.

Segmentation Approach	Security Level	CORR	Entropy (bits/pixel)	MAE	NPCR	Chi-Square	PSNR (dB)	UACI
LSE	0	-37.87×10^{-3}	14.54	3.07×10^{8}	100	2.99×10^{6}	3.82	4.68×10^{5}
	1	-50.57×10^{-3}	15.15	2.64×10^{8}	100	3.78×10^{6}	3.77	4.03×10^{5}
	2	31.11×10^{-3}	15.13	2.15×10^{8}	100	3.49×10^{6}	3.74	3.28×10^{5}
	Average	-39.84×10^{-3}	14.94	2.62×10^{8}	100	3.42×10^{6}	3.78	4.00×10^{5}

4.1.3. Time Performance and Discussion

The dataset in Section 4.1 is encrypted using the proposed multi-region encryption approach, two-region encryption approach [25], two-region encryption/compression approach, Naïve encryption approach, and Naïve encryption/compression approach. In the two-region encryption/compression approach, the ROI and ROB were compressed using LZ4 after the segmentation process and before the encryption process using AES-256 and XXTEA-128, respectively.

In Figure 10, the saved time using the proposed multi-region encryption approach is compared with other encryption approaches. Figure 10a,b illustrate the saved time in percentage with respect to the two-region encryption approach without and with compression, respectively. The proposed approach can save between 51–58% of the encryption time with respect to the two-region encryption approach, while it saves between 10–17.5% with respect to the two-region encryption/compression approach. On the other hand, the proposed approach saves almost ~60% with respect to the Naive encryption approach as shown in Figure 10c, while Figure 10d shows that the saved time varies between 44–49.5% with respect to the Naïve encryption/compression approach.

Another important aspect of the proposed approach is the compression ratio. Figure 11 shows the compression ratio based on different approaches. Even though LZ4 was used with all encryption approaches, the compression ratio differs significantly among these approaches. It is believed that the reason behind this variation is the consistency of the pixel data, where splitting ROI into multi-region creates more consistent groups of pixels, which results in a better compression ratio as in SL1 and SL2. This can also be confirmed by looking at the low compression ratio of the Naïve and two-region encryption approaches in comparison with the other approaches.

Table 2 depicts a brief comparison with similar selective encryption approaches in the literature. The approaches were executed using different datasets, hardware, and software implementations, and it is not fair to directly compare them with the proposed approaches in this paper. The reason for mentioning these works is that they have similarities with some of the proposed approaches in this paper, but their datasets and software implementations are not available and clear in order to compare them fairly with the proposed approaches in this paper. Additionally, any implementation in MATLAB (specifically the mentioned approaches in Table 2) will be several times slower than the C implementation that has been

conducted in this paper (Cython was used to compile the Python script of the proposed approaches of this paper into C code).

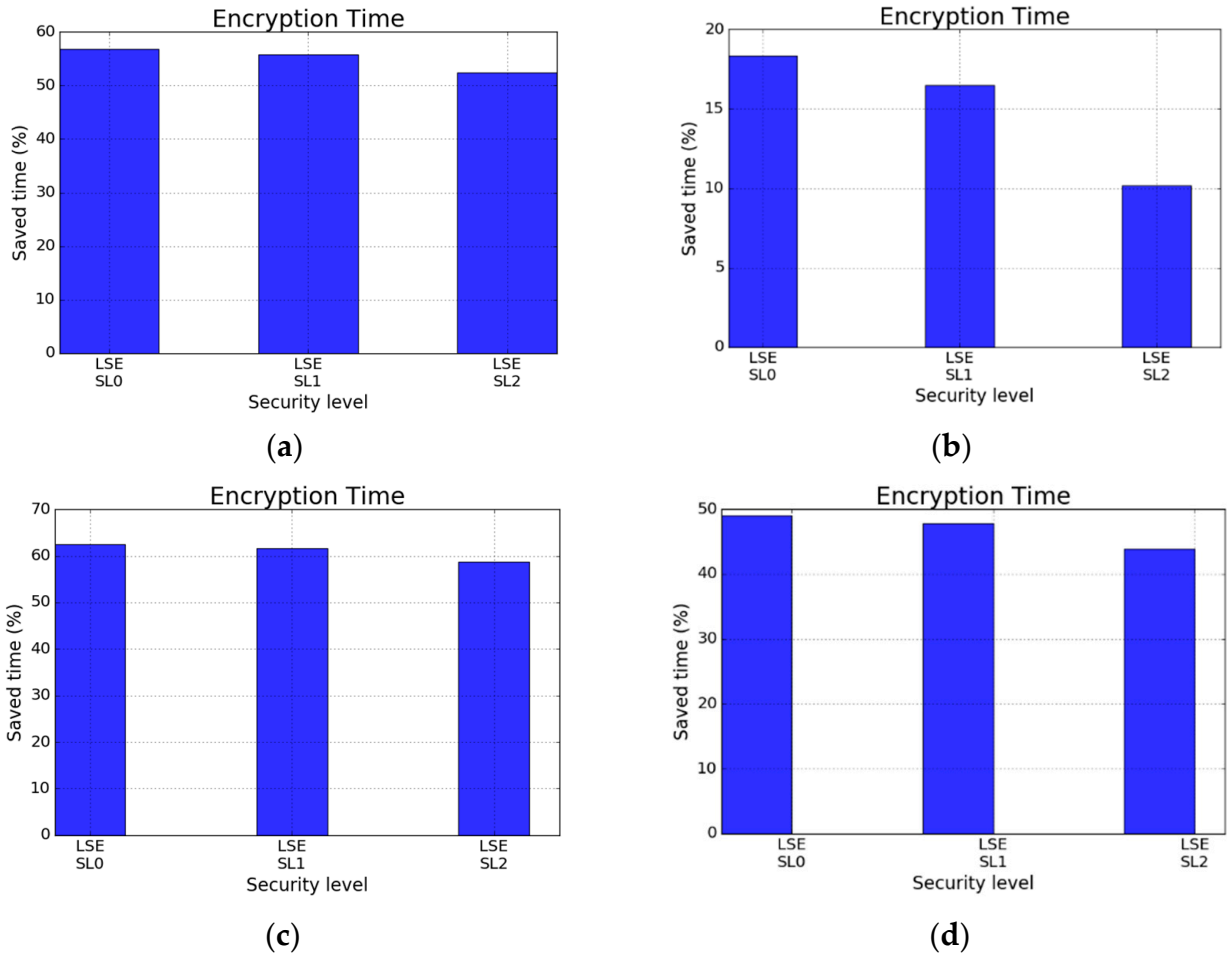


Figure 10. Saved time (%) with respect to (**a**) two-region encryption approach, (**b**) two-region encryption/compression approach, (**c**) Naïve encryption approach, and (**d**) Naïve encryption/compression approach.

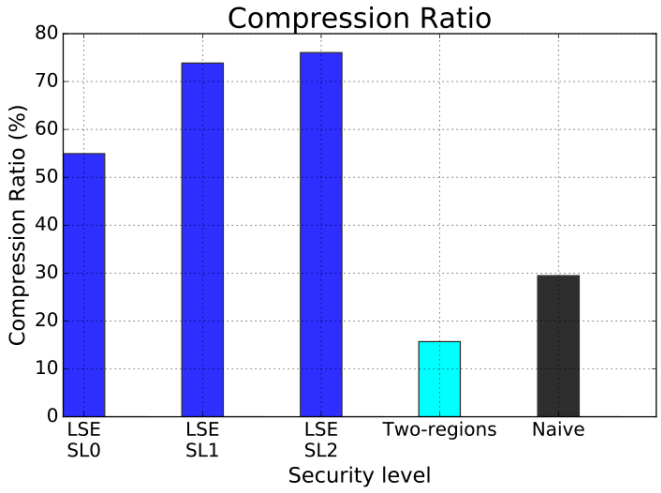


Figure 11. Compression ratio of the multi-region, two-region approach/compression, and Naïve approach/compression encryption approaches.

The proposed approaches in [42,43] employed similar hardware to the one used in Approach I; therefore, it is reasonable to restrict the comparison among these approaches. In study [42], a novel Fast Quaternion Feistel Cipher (F-QFC) for DICOM images was introduced. This approach employs the Feistel network that uses special properties of quaternions to execute rotations of data in 3D space for each cipher iteration. However, F-QFC has major security flaws. Thus, Dzwonkowski et al. [43] proposed a Secure Quaternion Feistel Cipher (S-QFC) algorithm that employs the concept of a modified Feistel network with modular arithmetic and the rotations of data sequences in 3D space, in order to enhance the security of F-QFC. Both approaches were deployed on Intel i5 processor with 8-bit grayscale DICOM images, and it can be noticed in Table 2 that the multi-region approach is thousands of times faster than F-QFC and S-QFC, due to the complex orientations in the 3D space. Another important work was presented in [33,44], which were tested on different hardware, and they have been reported here to indicate the processing speed, not for direct comparison. The work presented by Noura et al. [44] combines statistical segmentation with selective encryption to reduce the amount of data that needs to be encrypted using sophisticated encryption methods. Even though the presented approach was tested on a slower processor, it has an average of 44.87×10^6 bit/s $\approx$ 5.6 MB/s. Regardless of the hardware limitation in [44], the processing time of the multi-region approach was 18 times faster. The most similar work to the multi-region approaches was presented by Mahmood et al. [13,45], in which a GA was employed to estimate regions' sizes within ROI prior to the encryption process. Mahmood validated the presented approach using an Intel i7 processor which is more powerful than the one used in this paper. Nevertheless, the proposed multi-region approach achieved a much higher encryption speed. The encryption speed of the reported approach in [13] was 0.4×10^6 bit/s $\approx$ 0.05 MB/s, which is slower than the work presented in [44] on slower hardware.

Table 2. Brief comparison of the encryption time with approaches reported in the literature.

Approach	Hardware	Software	File Size	Encryption Time (s)	Decryption Time (s)	Encryption Speed (pixel/s)	Encryption Speed (bit/s)
Statistical Selective Approach [44]	Intel Core 2 Duo, 3 GHZ CPU, 2 GB RAM Intel	MATLAB R2013b and Microsoft Windows 7	512 × 512: 0.26 MB (8-bit depth)	0.0468	–	5.6×10^6	44.87×10^6
Secure Quaternion Fesistel Cipher (S-QFC) [43]	Intel(R) Core(TM) i5-3570 CPU @ 3.40 GHz, 16 GB RAM	MATLAB R2013b and Microsoft Windows 7	512 × 512: 0.53 MB (16-bit depth)	1.93×10^2	–	0.0014×10^6	0.0022×10^6
Fast Quaternion Fesistel Cipher (F-QFC) [42]	Intel(R) Core(TM) i5-3570 CPU @ 3.40 GHz, 16 GB RAM	MATLAB R2013b and Microsoft Windows 7	512 × 512: 0.26 MB (8-bit depth)	1.81×10^2	–	0.0015×10^6	0.0024×10^6
Adaptive multi-region encryption [13,45]	Intel i7-820, CPU @ 3.40 GHz, 16 GB RAM	MATLAB 7.10 and Microsoft Windows 7	512 × 512: 0.52 MB (16-bit depth)	10.63	–	0.0246×10^6	0.4×10^6
Proposed approach (LSE)	Intel(R) Core(TM) i5-3570 CPU @ 3.40 GHz, 16 GB RAM	Cython, Python 2.7 and Ubuntu 16.04	2430 × 2140: 41.60 MB (16-bit depth)	0.11	0.096	5.09×10^7	8.2×10^8

4.2. Approach II

4.2.1. Security Evaluation

A benchmark set of 69 grayscale MRI Neoadjuvant Chemotherapy (NACT) breast cancer DICOM frames [46] is utilized to evaluate the proposed approaches experimentally. The statistical properties of the given dataset before and after encryption are depicted in Tables 3 and 4, respectively, which show a significant difference between them. Original images have a median value of around 0, due to a large number of pixels with zero intensity in the background, while encrypted images have large median values.

Table 3. Statistical properties of the original images (average of the given dataset).

Number of Frames	Pixel Intensity			Frame Size
	μ	σ	Median	
69	847.975	960.537	0	2760 × 1200

Table 4. Statistical properties of the encrypted images (average of the given dataset).

Approach	Pixel Intensity		
	μ	σ	Median
Frame-Based SE	1358.45	745.62	1038.53
Holistic-Based SE	1739.14	940.98	2001.08

The performance overview of the proposed approaches is illustrated in Table 5. The low correlation between the encrypted and original images has good robustness against linear attacks, while the low PSNR values of the proposed approaches display good randomness. The UACI of encrypted images using Frame-Based SE is smaller than the UACI of the images encrypted using the Holistic-Based SE. The NPCR value was almost the same for all approaches with a very high score (~100%), and this means that all pixels' values have been changed in both cases as designated by the NPCR score. The Frame-Based SE has a higher MAE value in comparison with the Holistic-Based SE value, which indicates that the encrypted images based on the Frame-Based SE are significantly different from the original images. Entropy is a measure of the uncertainty present in the encrypted image, and a higher entropy of the encrypted image indicates a higher degree of randomness. As the bit depth of the DICOM datasets used in this approach is 16, the entropy value varies between 0–16 bits/pixel. The entropy values for both approaches were almost the same.

Table 5. Cryptanalysis results of the 69 encrypted frames.

Encryption Approach	CORR	Entropy (bits/pixel)	MAE	NPCR	PSNR (dB)	UACI (%)
Frame-Based SE	0.00098	15.28	531,628.3	100	16.03	92.27
Holistic-Based SE	0.000088	15.08	421,078.6	100	16.13	93.3

Histogram: This metric assists in distinguishing the correlation between the original and the encrypted image by showing each gray-level probability. Subsequently, if the difference between the original and encrypted image is large; the image is highly uncorrelated. Moreover, if the gray-level probabilities are distributed uniformly, the attacker cannot predict enough information to make a statistical attack by fitting the distribution [38]. Figure 12a shows the plain image, while Figure 13a shows its histogram. Figure 12b shows the encrypted image using Frame-Based SE, while Figure 13b shows its histogram. Figure 12c shows the encrypted image using Holistic-Based SE, while Figure 13c shows its histogram.

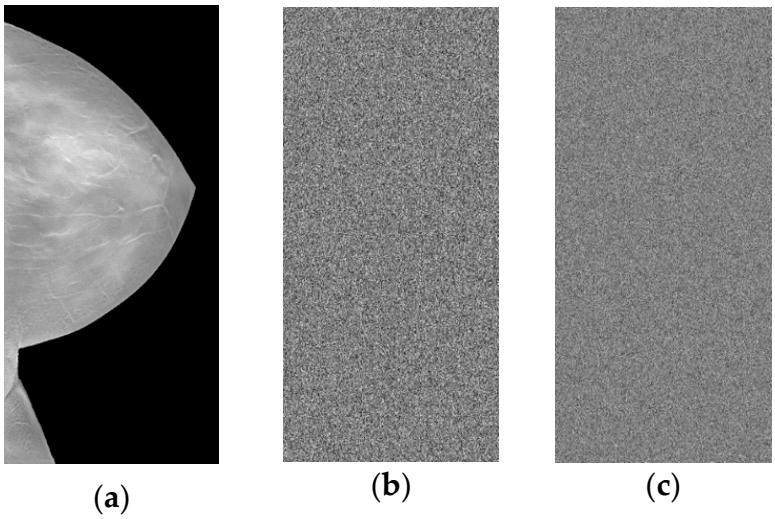


Figure 12. (**a**) the original image, (**b**) the encrypted image (Frame-Based SE), and (**c**) the encrypted image (Holistic-Based SE).

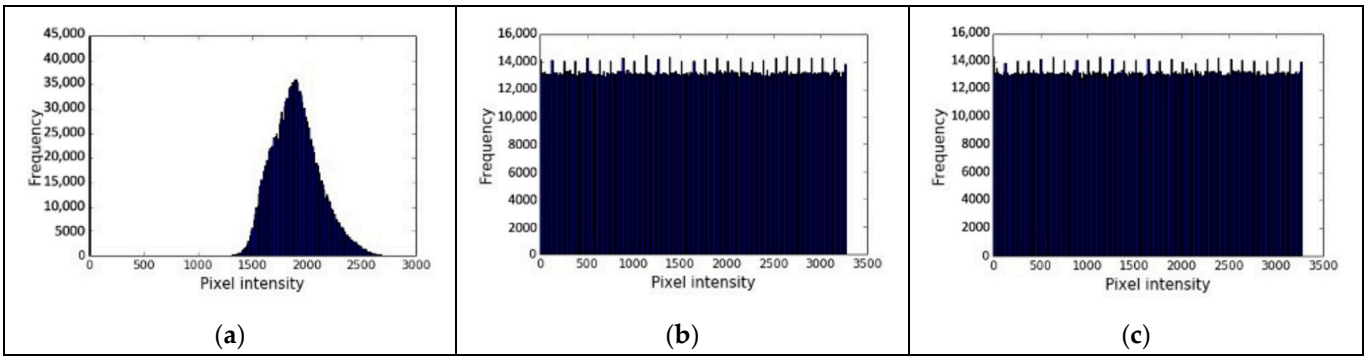


Figure 13. (**a**) Original image histogram, (**b**) Encrypted image (Frame-Based SE) histogram, and (**c**) Encrypted image (Holistic-Based SE) histogram.

Figure 13a depicts the pixel intensity distribution, which is almost a Gaussian distribution. The encrypted frame using the Frame-Based SE shows a flat pattern, as shown in its histogram in Figure 13b. Additionally, the histogram of the encrypted frame based on the Holistic-Based SE has nearly a flat histogram, as shown in Figure 13c, which shows a good level of randomness. Hence, both approaches have a similar distribution.

4.2.2. Time Performance and Discussion

As the main goal of the reported approaches in this section is to reduce the encryption time while maintaining high security, the encryption times of the proposed approaches are compared amongst each other and against the Naïve encryption approach, where all frames' pixel data are encrypted using AES cipher with CTR mode of operation.

The proposed Frame-Based SE is ~10,000 times faster than the Holistic-Based SE and the Naïve encryption approach as shown in Table 6. The main reason for this high speed for the Frame-Based SE is the fact that it relies on an optimized matrices multiplication library that significantly reduces the segmentation time. Moreover, the compression greatly reduces the sizes of the selected data to be encrypted as displayed in Table 7. Hence, the Frame-Based SE can significantly reduce the required time to secure the multi-frame DICOM images.

Table 6. Encryption speed of the multi-frame encryption approach.

Encryption Approach	Encryption Speed(Frame/s)
Frame-Based SE	10,572
Holistic-Based SE	30.25
Naïve Encryption Approach	24.64

Table 7. The original and encrypted data sizes.

Encryption Approach	Original Data Size (MB)	Encrypted Data Size (MB)
Frame-Based SE	457.06	3.12
Holistic-Based SE	457.06	406.23
Naïve Encryption Approach	457.06	204.50

Table 7 shows the data sizes before and after encryption. It can be noticed that the Frame-Based SE has a compression ratio of (146:1), which significantly reduces the image size. On the other hand, Holistic-Based SE has the worst compression ratio, which is (1.3:1).

To sum up, this is a novel approach that selectively encrypts the ROI in a multi-frame DICOM object using a sophisticated encryption algorithm (AES), while encrypting the ROB using a lighter encryption algorithm (XXTEA). The selection process in this approach is executed either in an automatic manner (combining the pre-defined reference frame and automatic thresholding) or by segmenting the pixels from all DICOM frames using the thresholding technique [25] in one go. Accordingly, it was noticed that the Frame-Based SE is very efficient and has a very short processing time with an efficient compression ratio. The novelty of this approach depends on improving redundancy within different frames by segmenting images into ROI and ROB based on a segmentation map that is obtained based on the automatic selection of a reference frame and the thresholding segmentation [25]. Therefore, the proposed approach can be used in various security frameworks to achieve various security goals, such as confidentiality.

5. Conclusions and Future Work

In this paper, a selective encryption approach was adopted to provide an efficient encryption mechanism for the pixel data of DICOM images in the spatial domain, which makes a trade-off between the processing time of the encryption process while sustaining the robustness of the encrypted DICOM images against different attacks. However, the selective encryption approaches require efficient segmentation mechanisms. Hence, in this paper, medical images' statistical properties were exploited to achieve this efficient segmentation. Then, in order to further reduce the processing time, this paper presented the use of lossless compression alongside efficient segmentation approaches. This paper adopted a selective encryption concept since it has a significant potential to shorten the processing time, by efficiently utilizing the data structure of image compression, optimization, and processing techniques to reduce the volume of data during encryption.

This paper proposed an efficient selective encryption approach for multi-frame and single-frame DICOM object. The proposed approach for single-frame DICOM image was successfully implemented, tested, and evaluated. However, the presented approach seems to be complicated, and the saving time with respect to the two-region encryption approach [25] was small (with added compression step). Hence, it is believed that splitting the ROI into three regions might overcomplicate the selection mechanisms. While the proposed approach for multi-frame DICOM object was more robust and efficient as it significantly reduced the encryption time, and it was ~10,000 times faster than the Naïve encryption approach, with a remarkable compression ratio due to the idea of improving the redundancy within the different frames of the DICOM object. Based on that, this proposed approach could be enhanced to be simpler for marketing goals. Further, increasing the dataset for the training stage could provide more accurate thresholds for any new input

DICOM dataset for hospitals and medical institutions. Furthermore, the high speed and efficiency of this approach could be utilized for encrypting 3D and colored DICOM images.

As mentioned in the Introduction, there are different security requirements in the cybersecurity field, which can be accomplished through the proposed approaches by combining them with a more comprehensive framework such as the framework presented by [24,47]. The proposed approaches are selective encryption mechanisms that facilitate security functionality when they are used in a holistic framework that supports these security requirements. Therefore, it is desirable to extend the presented work in order to achieve confidentiality, authenticity, and integrity.

Based on the developed approaches in this paper, it was noticed that the combination of lossless compression with an efficient segmentation algorithm could significantly improve the performance of selective encryption. Therefore, in future research, it will be conducted to integrate the encryption and compression at a lower structural level to attain faster encryption/compression processing time.

Author Contributions: Methodology, Q.N.; Writing—original draft, Q.N.; Writing—review & editing, A.S., D.Z. and E.E.; Supervision, A.S. and E.E.; Funding Acquisition, D.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Middle East University (Scholarship) and the APC was funded by Loughborough University.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original datasets for this study can be found in the Cancer Imaging Archive at: https://wiki.cancerimagingarchive.net/display/Public/CBIS-DDSM (accessed on 21 November 2018) and https://wiki.cancerimagingarchive.net/display/Public/Breast-MRI-NACT-Pilot (accessed on 19 March 2016).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The multi-region approach depends on the calculation of regions' sizes to minimize the required encryption time. In this research, an approach that exploits a straightforward linear system was developed to estimate regions' sizes that guarantee optimal performance.

Under the assumption that encryption cost is linear with respect to data size as investigated in Section 3.1.1, the encryption cost can be expressed as shown in Equation (A1):

$$T_{i,r} = B_i \times S_r + C_i \tag{A1}$$

where T_i is the encryption cost of region r using encryption algorithm i, S_r is the region r size, B_i is the slope, and C_i is the intercept value for the encryption algorithm i.

Assuming that ROI can be split into three different regions and each region will be encrypted using a different encryption approach, then the overall encryption time (including segmentation time) can be determined as shown in Equation (A2). Henceforth, our goal is to split the ROI into three different regions while guaranteeing that the processing time is less than the Naïve approach processing time. At the same time, it is important to facilitate different security requirements.

$$T_{total} = T_{1\_AES256} + T_{2\_AES128} + T_{3\_XXTEA128} + segmentation\_time \tag{A2}$$

Equation (A2) must satisfy the condition that is shown in Equation (A3), where T_{ROI_AES256} represents the Naïve encryption approach for the ROI.

$$T_{total} < T_{ROI\_AES256} \tag{A3}$$

Let us assume that $\in$ is a positive integer number that represents the desired saving time, then Equation (A3) can be rewritten as in Equation (A4):

$$T_{total} + \in = T_{ROI\_AES256} \tag{A4}$$

Based on Section 3.1.1, the processing time of different encryption algorithms is estimated using linear equations that correspond to encryption algorithms and have the form of ($T_i = B_i \times S_r + C_i$). Each algorithm has a linear relationship that estimates its processing time, as shown in Equation (A5):

$$\begin{aligned} T_{1\_AES256} &= B_1 \times S_{r1} + C_1 \\ T_{2\_AES128} &= B_2 \times S_{r2} + C_2 \\ T_{3\_XXTEA128} &= B_3 \times S_{r3} + C_3 \end{aligned} \tag{A5}$$

Image size can be defined as in Equation (A6a):

$$S_{img} = S_{ROB} + S_{ROI} \tag{A6a}$$

ROI size can be defined as in Equation (A6b):

$$S_{ROI} = S_{r1} + S_{r2} + S_{r3} \tag{A6b}$$

Let us assume that we have constants K_1, K_2, K_3, where:

$$K_1 + K_2 + K_3 = 1 \tag{A7}$$

Then regions' sizes, which are within ROI (r_1, r_2, r_3), can be considered as shown in Equations (A8)–(A10):

$$S_{r_1} = K_1 S_{ROI} \tag{A8}$$

$$S_{r_2} = K_2 S_{ROI} \tag{A9}$$

$$S_{r_3} = K_3 S_{ROI} \tag{A10}$$

Accordingly, Equation (A5) can be written using Equations (A8)–(A10), as shown in Equation (A11):

$$\begin{aligned} T_1 &= B_1 K_1 S_{ROI} + C_1 \\ T_2 &= B_2 K_2 S_{ROI} + C_2 \\ T_3 &= B_3 K_3 S_{ROI} + C_3 \end{aligned} \tag{A11}$$

Equation (A11) can be rewritten in matrix form as in Equation (A12):

$$\begin{bmatrix} T_1 \\ T_2 \\ T_3 \end{bmatrix} = \begin{bmatrix} B_1 S_{ROI} & 0 & 0 \\ 0 & B_2 S_{ROI} & 0 \\ 0 & 0 & B_3 S_{ROI} \end{bmatrix} \begin{bmatrix} K_1 \\ K_2 \\ K_3 \end{bmatrix} + \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} \tag{A12}$$

The overall desired encryption time can be expressed as shown in Equation (A13):

$$T_d = T_{ROI\_AES256} - segmentation\_time - \in \tag{A13}$$

Selective multi-region encryption must cover all security requirements, and this requires an adaptive security profile that can adapt to different levels of security risks. Such that, high-risk scenarios require that most of the ROI must be encrypted using AES-256 and AES-128. Hence, r_1 and r_2 sizes must be large in comparison with r_3. Then, r_1 and r_2

contributing to saving time will be minimum. On the other hand, for low-risk scenarios, r_1 and r_2 must highly contribute to saving processing time.

To perform the selective encryption adaptively, a security index that defined the security threats have been introduced. This security index $I = [\, I_1,\ I_2,\ I_3]$ is a vector that contains three elements (each element corresponds to a region (R1, R2 and R3)). Based on the description as mentioned above, Equation (A13) can be rewritten in vector form, as shown in Equation (A14):

$$\begin{bmatrix} T_1 \\ T_2 \\ T_3 \end{bmatrix} = \begin{bmatrix} I_1 \\ I_2 \\ I_3 \end{bmatrix} (T_{ROI\_AES256} - segmentation_{time} - \in) \tag{A14}$$

The regions' sizes can be determined by simply solving a linear system, including the constraint that ($\sum K = 1$), by rewriting Equation (A14), as shown in Equation (A15):

$$\begin{cases} T_1 = I_1 T_d \\ T_2 = I_2 T_d \\ T_3 = I_3 T_d \end{cases} \tag{A15}$$

From Equation (A15), T_{d_2} and T_{d_3} can be rewritten as shown in Equation (A16):

$$\begin{cases} T_2 = \frac{I_2}{I_1} T_1 \\ T_3 = \frac{I_3}{I_1} T_1 \end{cases} \tag{A16}$$

Let us assume $\frac{I_2}{I_1}$ and $\frac{I_3}{I_1}$ are equal to h_1 and h_2, respectively. Now by solving for that $K's$, considering Equation (A11), as shown in Equations (A17) and (A18):

$$K_2 = \frac{h_1(K_1 B_1 S_{roi} + C_1) - C_2}{B_2 S_{roi}} \tag{A17}$$

$$K_3 = \frac{h_2(K_1 B_1 S_{roi} + C_1) - C_3}{B_3 S_{roi}} \tag{A18}$$

By substituting Equations (A17) and (A18) in ($\sum K = 1$), then K_1 can be determined as shown in Equation (A19). Then, K_2 and K_3 can be calculated using Equations (A17) and (A18):

$$K_1 = \frac{\left(B_2 B_3 + h_1 \frac{C_2 B_3}{S_{roi}} + h_2 \frac{C_3 B_2}{S_{roi}}\right)}{B_2 B_3 + h_1 B_1 B_3 + h_2 B_1 B_2} \tag{A19}$$

From these equations, it can be noticed that K_2 is directly proportional with h_1; hence, it is also directly proportional to I_2 and inversely proportional to I_1. On the other hand, K_3 is directly proportional to h_2; hence, it is also directly proportional to I_3 and inversely proportional to I_1. Accordingly, for high-security risk, it is desirable to have large I_1 and small I_2 and I_3; i.e., $I = [5.0,\ 1.0,\ 0.005]$. At medium security threats, it is desirable to give all regions the same importance; hence, I_1 I_2, and I_3 can have the same values. Finally, at a low-security level, I_1 can have a very small value and I_2 and I_3 can have larger values, i.e., $I = [1,\ 2,\ 3]$. It is worth here mentioning that this security index can be defined based on the need and there is no thumb rule as to how to adjust these values as long as it follows the logic explained above.

References

1. DICOM. Part 15, NEMA. 2017. Available online: http://dicom.nema.org/medical/dicom/current/output/pdf/part15.pdf (accessed on 25 May 2018).
2. NEMA. Digital Imaging and Communication in Medicine (DICOM). NEMA. Available online: http://dicom.nema.org/ (accessed on 25 May 2018).

3. Cao, F.; Huang, H.; Zhou, X. Medical image security in a HIPAA mandated PACS environment. *Comput. Med. Imaging Graph.* **2003**, *27*, 185–196. [CrossRef] [PubMed]
4. Hodge, J.G., Jr.; Gostin, L.O.; Jacobson, P.D. Legal issues concerning electronic health information: Privacy, quality, and liability. *JAMA* **1999**, *282*, 1466–1471. [CrossRef] [PubMed]
5. Lian, S. *Multimedia Content Encryption: Techniques and Applications*; Auerbach Publications: Boca Raton, FL, USA, 17 September 2008.
6. Abd Elminaam, D.S.; Abdual-Kader, H.M.; Hadhoud, M.M. Evaluating the Performance of Symmetric Encryption Algorithms. *Int. J. Netw. Secur.* **2010**, *10*, 216–222.
7. Lee, H.; Lee, K.; Shin, Y. Aes implementation and performance evaluation on 8-bit microcontrollers. *arXiv* **2009**, arXiv:0911.0482.
8. Spanos, G.A.; Maples, T.B. Performance study of a selective encryption scheme for the security of networked, real-time video. In Proceedings of the Computer Communications and Networks, Las Vegas, NV, USA, 20–23 September 1995.
9. Laouamer, L.; Al Shaikh, M.; Nana, L.T.; Pascu, A.C. Informed symmetric encryption algorithm for DICOM medical image based on N-grams. In Proceedings of the 2013 Science and Information Conference, London, UK, 7–9 October 2013; pp. 353–357.
10. Marwan, M.; Kartit, A.; Ouahmane, H. A Novel Approach for Security in Cloud-Based Medical Image Storage Using Segmentation. In Proceedings of the International Symposium on Ubiquitous Networking, Casablanca, Morocco, 9–12 May 2017; Springer: Cham, Switzerland, 2017; pp. 247–258.
11. Lalitha, Y.S.; Latte, M.V. Lossless and lossy compression of DICOM images with scalable ROI. *Int. J. Comput. Sci. Netw. Secur.* **2010**, *10*, 276–281.
12. Mahmood, A.B.; Dony, R.D. Adaptive encryption using pseudo-noise sequences for medical images. In Proceedings of the 2013 Third International Conference on Communications and Information Technology (ICCIT), Beirut, Lebanon, 19–21 June 2013; pp. 39–43.
13. Mahmood, A.; Dony, R.; Areibi, S. An adaptive encryption based genetic algorithms for medical images. In Proceedings of the 2013 IEEE International Workshop on Machine Learning for Signal Processing (MLSP), Southampton, UK, 22 September 2013; IEEE: Piscatvie, NJ, USA; pp. 1–6.
14. Kanso, A.; Ghebleh, M. An efficient and robust image encryption scheme for medical applications. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *24*, 98–116. [CrossRef]
15. Mahmood, A.; Hamed, T.; Obimbo, C.; Dony, R. Improving the security of the medical images. *Int. J. Adv. Comput. Sci. Appl.* **2013**, *4*, 137–146. [CrossRef]
16. Sajjad, M.; Muhammad, K.; Baik, S.W.; Rho, S.; Jan, Z.; Yeo, S.S.; Mehmood, I. Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. *Multimed. Tools Appl.* **2017**, *76*, 3519–3536. [CrossRef]
17. Mahmood, A.B.; Dony, R.D. Segmentation based encryption method for medical images. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11–14 December 2011; pp. 596–601.
18. Brahimi, Z.; Bessalah, H.; Tarabet, A.; Kholladi, M.K. A new selective encryption technique of JPEG2000 codestream for medical images transmission. In Proceedings of the 2008 5th International Multi-Conference on Systems, Signals and Devices, Amman, Jordan, 20–22 July 2008; pp. 1–4.
19. Norcen, R.; Podesser, M.; Pommer, A.; Schmidt, H.P.; Uhl, A. Confidential storage and transmission of medical image data. *Comput. Biol. Med.* **2003**, *33*, 277–292. [CrossRef] [PubMed]
20. Zhou, Y.; Panetta, K.; Agaian, S. A lossless encryption method for medical images using edge maps. In Proceedings of the 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Minneapolis, MN, USA, 3–6 September 2009; pp. 3707–3710.
21. Puech, W.; Rodrigues, J.M. Crypto-compression of medical images by selective encryption of DCT. In Proceedings of the 2005 13th European signal processing conference, Antalya, Turkey, 4–8 September 2005; pp. 1–4.
22. Ou, Y.; Sur, C.; Rhee, K.H. Region-based selective encryption for medical imaging. In Proceedings of the International Workshop on Frontiers in Algorithmics, Lanzhou, China, 1–3 August 2007; Springer: Berlin/Heidelberg, Germany; pp. 62–73.
23. Elhoseny, M.; Shankar, K.; Lakshmanaprabu, S.K.; Maseleno, A.; Arunkumar, N. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural Comput. Appl.* **2020**, *32*, 10979–10993. [CrossRef]
24. Kobayashi, L.O.; Furuie, S.S.; Barreto, P.S. Providing integrity and authenticity in DICOM images: A novel approach. *IEEE Trans. Inf. Technol. Biomed.* **2009**, *13*, 582–589. [CrossRef] [PubMed]
25. Natsheh, Q.; Sălăgea, A.; Edirisinghe, E. Securing DICOM images based on adaptive pixel thresholding approach. In Proceedings of the 2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS), Karlstad, Sweden, 18–21 June 2018; pp. 280–285.
26. NEMA. DICOM. Supplement 142-Page 44. 2017. Available online: ftp://medical.nema.org/medical/dicom/final/sup142_ft.pdf; https://www.dicomstandard.org/News-dir/ftsup/docs/sups/sup142.pdf (accessed on 2 December 2022).
27. NEMA. DICOM Patient Identification Module–Page 8. 2017. Available online: http://dicom.nema.org/Dicom/News/june2014/docs/cp1343_ft.pd; https://dicom.nema.org/medical/Dicom/2016c/output/chtml/part03/sect_C.2.2.html (accessed on 2 December 2022).
28. NEMA; DICOM. Supplement 31-Page 5. 2019. Available online: Ftp://medical.nema.org/medical/dicom/Final/sup31_ft.pdf (accessed on 18 March 2023).
29. Natsheh, Q.N.; Li, B.; Gale, A.G. Security of multi-frame DICOM images using XOR encryption approach. *Procedia Comput. Sci.* **2016**, *90*, 175–181. [CrossRef]

30. Lei, T. *Statistics of Medical Imaging*; CRC Press: Boca Raton, FL, USA, 2011.
31. Andrews, L.C.; Phillips, R.L. *Laser Beam Propagation through Random Media: Second Edition*; SPIE Press: Bellingham, WA, USA, 2005.
32. The Cancer Imaging Archive (TCIA). The Cancer Imaging Archive (TCIA)-A Growing Archive of Medical Images of Cancer. Available online: http://www.cancerimagingarchive.net/ (accessed on 15 November 2017).
33. Nithya, R.; Santhi, B. Computer-aided diagnosis system Mammogram Density Classification. *Int. J. Biomed. Eng. Technol.* **2016**, *22*, 162–177. [CrossRef]
34. Fan, S.K.; Lin, Y.; Wu, C.C. Image thresholding using a novel estimation method in generalized Gaussian distribution mixture modeling. *Neurocomputing* **2008**, *72*, 500–512. [CrossRef]
35. Housley, R. "www.ietf.org" Internet Engineering Steering Group/RSA Laboratories, August 2002. Available online: https://www.ietf.org/rfc/rfc3369.txt (accessed on 15 December 2018).
36. Clunie, D.; Parisot, C.C.; Verduin, K.V.K.; Hassold, B.B. New Enhanced Multi-frame DICOM CT and MR Objects to Enhance Performance and Image Processing on PACS and Workstations. 22 May 2004. Available online: https://www.dclunie.com/papers/SCAR_20040522_CTMRMF.pdf (accessed on 15 December 2018).
37. Rubin, D.D. The Cancer Imaging Archive, CBIS-DDSM (Curated Breast Imaging Subset of Digital Database for Screening Mammography). Department of Biomedical Data Science, Radiology, and Medicine, Stanford University School of Medicine, 21 November 2018. Available online: https://wiki.cancerimagingarchive.net/display/Public/CBIS-DDSM; https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=22516629 (accessed on 18 March 2023).
38. Gray, R.M. *Entropy and Information Theory*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011.
39. Abd El-Samie, F.E.; Ahmed, H.E.; Elashry, I.F.; Shahieen, M.H.; Faragallah, O.S.; El-Rabaie, E.S.; Alshebeili, S.A. *Image Encryption: A Communication Perspective*; CRC Press: Boca Raton, FL, USA, 2013.
40. Etemadi Borujeni, S.; Eshghi, M. Chaotic image encryption design using tompkins-paige algorithm. *Math. Probl. Eng.* **2009**, *2009*, 762652. [CrossRef]
41. Lyons, J. Practical Cryptography, Practical Cryptography. 2009. Available online: http://www.practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/ (accessed on 30 May 2019).
42. Dzwonkowski, M.; Papaj, M.; Rykaczewski, R. A new quaternion-based encryption method for DICOM images. *IEEE Trans. Image Process.* **2015**, *24*, 4614–4622. [CrossRef] [PubMed]
43. Dzwonkowski, M.; Rykaczewski, R. Secure quaternion feistel cipher for DICOM images. *IEEE Trans. Image Process.* **2018**, *28*, 371–380. [CrossRef] [PubMed]
44. Noura, M.; Noura, H.; Chehab, A.; Mansour, M.M.; Sleem, L.; Couturier, R. A dynamic approach for a lightweight and secure cipher for medical images. *Multimed. Tools Appl.* **2018**, *77*, 31397–31426. [CrossRef]
45. Mahmood, A. Adaptive Approaches for Medical Imaging Security. Ph.D. Thesis, University of Guelph, Guelph, ON, Canada, 2015.
46. Newitt, D.; Hylton, N. The Cancer Imaging Archive, Single Site Breast DCE-MRI Data and Segmentations from Patients Undergoing Neoadjuvant Chemotherapy. 2016. Available online: https://wiki.cancerimagingarchive.net/display/Public/Breast-MRI-NACT-Pilot; https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=22513764 (accessed on 2 December 2022).
47. Al-Haj, A. Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. *J. Digit. Imaging* **2015**, *28*, 179–187. [CrossRef] [PubMed]