

Article

A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission

Francesco Castro *, Donato Impedovo * and Giuseppe Pirlo

Department of Computer Science, University of Bari Aldo Moro, 70125 Bari, Italy; giuseppe.pirlo@uniba.it

* Correspondence: francesco.castro@unicampus.it (F.C.); donato.impedovo@uniba.it (D.I.)

Featured Application: The proposed scheme enables the protection of medical images transmission by ensuring visual image security, image encryption and fingerprint-based authentication.

Abstract: Secure transmission of medical images and medical data is essential in healthcare systems, both in telemedicine and AI approaches. The compromise of images and medical data could affect patient privacy and the accuracy of diagnosis. Digital watermarking embeds medical images into a non-significant image before transmission to ensure visual security. However, it is vulnerable to white-box attacks because the embedded medical image can be extracted by an attacker that knows the system's operation and does not ensure the authenticity of image transmission. A visually secure image encryption scheme for secure fingerprint-based authenticated transmission has been proposed to solve the above issues. The proposed scheme embeds the encrypted medical image, the encrypted physician's fingerprint, and the patient health record (EHR) into a non-significant image to ensure integrity, authenticity, and confidentiality during the medical image and medical data transmission. A chaotic encryption algorithm based on a permutation key has been used to encrypt the medical image and fingerprint feature vector. A hybrid asymmetric cryptography scheme based on Elliptic Curve Cryptography (ECC) and AES has been implemented to protect the permutation key. Simulations and comparative analysis show that the proposed scheme achieves higher visual security of the encrypted image and higher medical image reconstruction quality than other secure image encryption approaches.



Citation: Castro, F.; Impedovo, D.; Pirlo, G. A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission. *Appl. Sci.* **2023**, *13*, 6099. <https://doi.org/10.3390/app13106099>

Academic Editor: Elias N. Zois

Received: 22 April 2023

Revised: 11 May 2023

Accepted: 12 May 2023

Published: 16 May 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: image security; visual security; image encryption; medical image; fingerprint; discrete wavelet transform

1. Introduction

In healthcare systems, artificial intelligence (AI) and machine learning (ML) approaches are increasingly used to support physicians in a variety of scenarios, such as the early detection of neurodegenerative disease [1–4] or cancer early detection in medical images [5–7]. Medical images are collected through techniques like computed tomography, ultrasound scanning, X-ray, magnetic resonance imaging, and positron emission tomography [8]. The anonymization or pseudonymization of the medical images is insufficient to ensure the patient's privacy [9,10] and presents various limitations. The anonymized data cannot easily be corrected or augmented by adding other patient information that is subsequently available [11]. Moreover, physicians share medical images and other medical information, such as the Electronic Health Record (EHR), through the hospital intranet or the internet in telemedicine [12]. The secure transmission of medical images and medical information is an essential requirement in healthcare systems, both for training a centralized AI model and for telemedicine applications. During transmission, an attacker could intercept and modify the medical images and EHR to compromise the diagnosis process [13] or the patient's privacy. Therefore, it is necessary to ensure medical data's

integrity, authenticity, and confidentiality during transmission. Digital watermarking is a technique that provides high data integrity and confidentiality for multimedia data. Digital watermarking involves embedding the image to be hidden in a non-significant reference image. The embedded watermark has imperceptible and robust properties that prevent it from being intentionally altered and visible to the naked eye [14]. However, the watermark approaches are not robust to white-box attacks because the embedded watermarked image is easily retrieved if an attacker is knowledgeable about the watermarking process applied. In addition, the authenticity of transmitted data is another security requirement that a medical image transmission scheme must have. Digital signatures, or blockchains, are commonly used to ensure the authenticity of data transmission over the Internet [15–18]. However, these approaches are economically and computationally costly, and they require the presence of a dedicated infrastructure. Biometric authentication is an innovative approach to ensuring the authenticity of data without the need for an exchange of keys between parties, as in digital signatures, or dedicated infrastructure, as in blockchains. Biometric data is unique, does not need to be generated at each transmission, and is extremely difficult to replicate by an attacker. Secure medical watermarking with a biometric authentication scheme has been proposed to solve the previous security and implementation issues. A physician's fingerprint has been used in the proposed scheme to ensure authenticity in medical image transmission. In the proposed scheme, a Singular Value Decomposition (SVD) has been applied to the medical image to obtain two unitary matrixes and a singular value vector. The two unitary matrixes have been embedded into two sub-bands of the reference image achieved by the 2D Discrete Wavelet Transform (2D-DWT). The singular value vector has been protected, along with the fingerprint feature vector, by a chaotic encryption scheme based on a random permutation key. It consists of mapping the singular value vector and the fingerprint feature vector into two random matrices achieved by the QR decomposition of a reference image sub-band. Subsequently, the mapped vectors are permuted and embedded into another reference image sub-band following the random permutation key. The random permutation key has been protected through a hybrid asymmetric cryptography scheme based on Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) algorithms. Subsequently, the reference image has been recreated along with an encrypted singular value vector and encrypted fingerprint feature vector through the 2D-Inverse Discrete Wavelet Transform (2D-IDWT) to obtain the final watermarked image, which is a visually meaningful encrypted image. Finally, the EHR has been embedded in the final watermarked image through the Least Significant Bit (LSB) algorithm, which is a steganography technique commonly used to directly encode the information in the host image [19]. The main research contributions of the proposed visually image encryption scheme are described below.

- Ensure the visual security of medical image transmission through a watermarking process.
- Protect the medical image and the physician's fingerprint through an encryption scheme to make the proposed scheme resistant to white-box attacks.
- Ensure the medical image's authenticity using the physician's fingerprint.
- Perform a proposed scheme simulation to evaluate the quality of the reconstructed medical image, the quality of the watermarking, and the accuracy of the reconstructed fingerprint feature in terms of peak signal-to-noise ratio (PSNR), mean structural similarity index measure (MSSIM), distance of histogram intersection, and the relative error.
- Perform a critical security analysis to evaluate the resistance of the proposed scheme to brute-force attacks.
- Compare the proposed scheme's performance with other visual encryption schemes to validate its effectiveness.

The paper is organized as follows: Section 2 introduces the related works and their limits; Section 3 describes the proposed scheme; Section 4 analyzes the quality performance of the proposed scheme; and Section 5 gives the conclusions and future developments.

2. Related Work

Traditionally, the images are protected by encryption algorithms that convert the original image into an unknown format, such as a noise-like or texture-like format [20–23]. In this way, it is evident that sensible information is presented in an unknown format, which leads to several tentative attacks. Digital watermarking enables image encryption with visual meaning by embedding sensitive information into a reference image with full visual meaning [24]. Digital watermarking is a widely used approach to ensuring the confidentiality of medical records and images. However, the transmission of the watermarked media in an insecure channel, such as the Internet, makes the technique less robust, with the possibility of attacks [25]. Watermarking is only a method of reliably embedding and decoding hidden information in a cover work [26], but it does not protect the hidden information. Encryption makes it possible to protect the information transmitted using cryptographic keys. Therefore, hybrid approaches have been proposed using cryptography techniques and watermarking to solve the security issue.

In [27], a chaotic sequence has been created by a chaotic logistic system, and it has been used to change the position of each pixel in the binary watermarking image achieved by two-dimensional Discrete Cosine Transform (2D-DCT). In [28], DCT has been combined with log-polar transform (LPT) to obtain robust watermarking for medical images. Subsequently, chaotic encryption and hash functions have been used to compensate for the weaknesses of traditional digital watermarking methods, which are unable to protect the medical image. In [25], the medical image and the sensible text data have been embedded in the sub-band of the cover image achieved by DWT. The obtained watermarked image has been encrypted using chaotic encryption.

The security of the cryptographic techniques depends on the secret key used to generate chaotic sequences [29,30] and, consequently, on secure key management. Biometric data has been used as a cryptographic key or mask to overcome this limit. In [31], the patient's biometric image is used to generate two keys. The first key is used to randomize the medical image, and the other key is used to encrypt the randomized image. The author proposed a new encryption technique based on the parameterized all-phase orthogonal transformation. In [32], the iris is used to generate two spiral phase masks. They are used with the lower-upper decomposition with partial pivoting to encrypt the medical image. In [33], the palmprint is used to generate a palmprint phase mask. The medical image is modulated by the palmprint phase mask, and then Fresnel transform and SVD operations are performed. The SVD is used to generate two different keys for encryption and decryption as well as in an asymmetric cryptosystem. In [34], an encryption method based on the face biometric to generate a chaotic face phase mask following the chaotic standard map [35] has been proposed. The random phase mask is used to encrypt the extracted region of interest (ROI) of the medical image. The ROI of the medical image has been selected and extracted by applying a mask image to the medical image. The mask image has been achieved through the Fuzzy C-Means Clustering (FRFCM) algorithm [36], which clusters the pixels in the original segmented image.

The encryption process has been applied after the watermarking process in all proposed hybrid approaches. However, the visual meaning of image encryption has not been realized in this way. In addition, several approaches use biometric data to ensure the authenticity of the image transmitted. Priya S. et al. [13] have proposed a visual meaning full image encryption to protect the medical image, the patient's electronic health record (EHR), and the doctor's fingerprint to ensure image authenticity. The EHR has been embedded into the original medical image using a watermarking technique to generate a watermarked medical image. Subsequently, the medical image watermarking and the doctor's fingerprint are visually encrypted using the Integer Wavelet Transform (IWT) along with an ordinary reference image. IWT is reversible without any loss by extracting the fingerprint from the encrypted medical image and matching it with the doctor's fingerprint. In this way, the EHR and the medical image are encrypted into an apparently insignificant image, and sender authentication is ensured by the doctor's fingerprint.

In [37], a medical image with digital watermarking based on fingerprints has been proposed. In the proposed method, the hash of the region of interest (ROI) of the medical image, fingerprint, and patient’s record (EHR) has been embedded into the medical image. The EHR has been encrypted using the elliptical cryptography (ECC) algorithm, and then a hexadecimal string has been obtained. The minutia points of the fingerprint image have been calculated, and then a binary string has been obtained. The hexadecimal string of the hashed medical image, the hexadecimal string of the EHR, and the binary string of the fingerprint have been concatenated into a single string, which is embedded in the original medical image. In this way, the watermarking image has been obtained. The biometric data used in these approaches has been embedded in the medical system without any protection. The original biometric data can be obtained simply by decoding the medical image in case of white-box attacks.

The proposed scheme realizes visually meaningful image encryption by protecting both medical images and biometric data through a chaotic encryption method based on random mapping and a random permutation key. The watermarking process has been applied after the encryption process to obtain the visually meaningful encrypted image and then ensures:

- a visual protection from black-box attacks;
- encryption protection from white-box attacks;
- an image authentication through a physician’s fingerprint

3. Materials and Methods

The proposed scheme consists of two main phases, illustrated respectively in Figures 1 and 2. The first is the encryption phase, which consists of embedding a medical image, the physician’s fingerprint feature, and the EHR to generate the encrypted image with visual meaning to be sent. The second is the decryption phase, where the embedded elements are extracted and reconstructed from the received image.

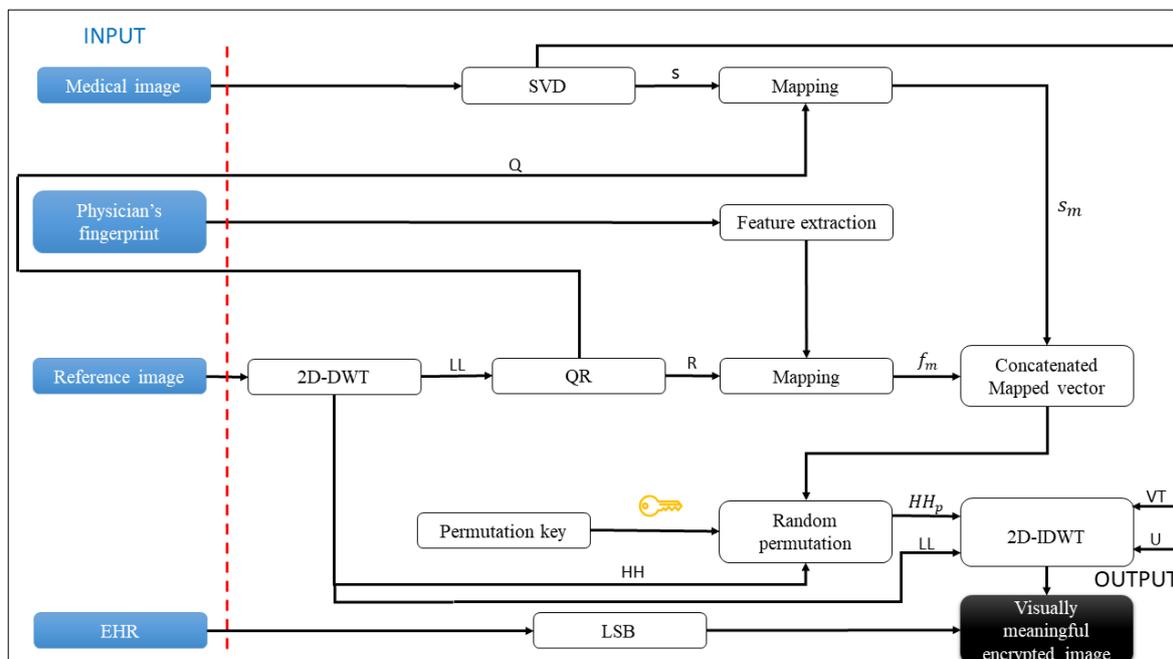


Figure 1. Visually secure image encryption scheme.

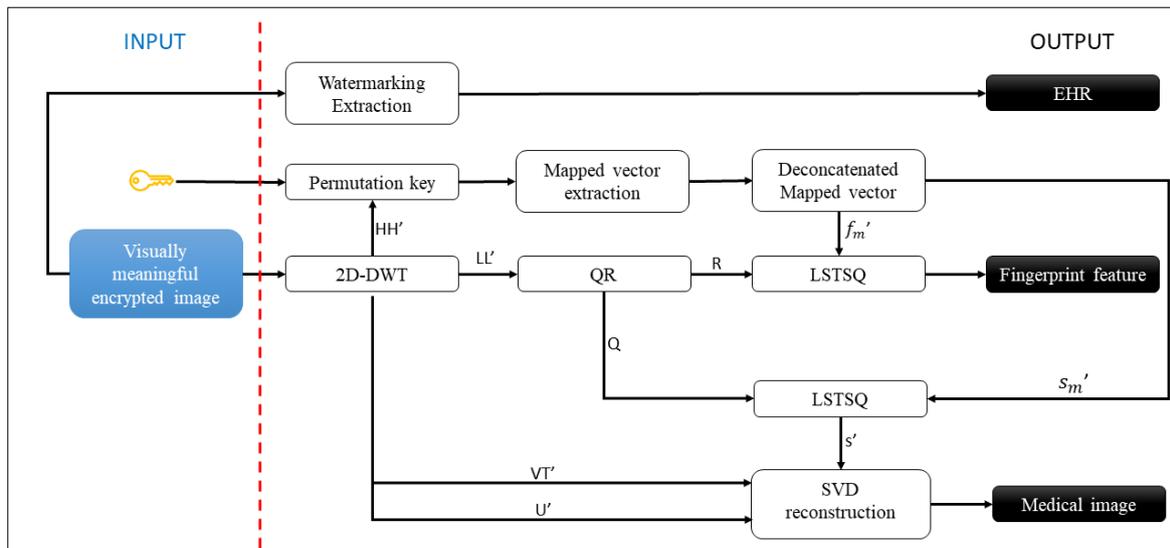


Figure 2. Visually secure image decryption scheme.

The two main phases of the proposed scheme shown in Figures 1 and 2 have been detailed in the following subsections.

3.1. Visually Secure Image Encryption Scheme

In this section, the proposed secure visual encryption scheme for medical image transmission with the inclusion of the physician’s fingerprint to authenticate the image and the EHR to provide medical information has been described. In the proposed encryption scheme, a medical image is first decomposed, encrypted, and then embedded into a non-significant reference image along with the fingerprint feature vector and the EHR.

The SVD is used to decompose a medical image into two orthogonal matrixes U and V^H , and in a singular value vector s . SVD enables a robust watermarking incorporation process, as small variations in singular values do not affect the visual quality of the reconstructed medical image [38]. The SVD of the gray-scale medical image with $N \times N$ size is stated in Equation (1).

$$X = U s V^H \tag{1}$$

where U and V^H have size $N \times N$ and s has size N .

In the next stage U , V^H and s are embedded into the reference image through a watermarking process. The reference image is a gray-scale image with $2N \times 2N$ size, and it is divided into four non-overlapping sub-bands through 2D-DWT, namely approximation (LL), horizontal detail (LH), vertical detail (HL) and diagonal detail (HH) according to Equation (2).

$$LL, LH, HL, HH = DWT2(I, w) \tag{2}$$

where $DWT2$ is 2D-DWT function, I is the reference image, and w is the wavelet used for the transformation.

LL represents low-frequency components, and the remaining LH , HL , HH represent high-frequency components [39]. The LL sub-band contains the main information of the image, and any operation or replacement of this sub-band is easily noticeable by the human eye. Therefore, LL ensures the robustness of the watermarking process and should not be altered. To obtain a good imperceptibility of the watermarking process HH is the best sub-band to embed the information to be hidden [25]. Figure 3 shows the 2D-DWT applied to the reference image, where each sub-band have $N \times N$ size.

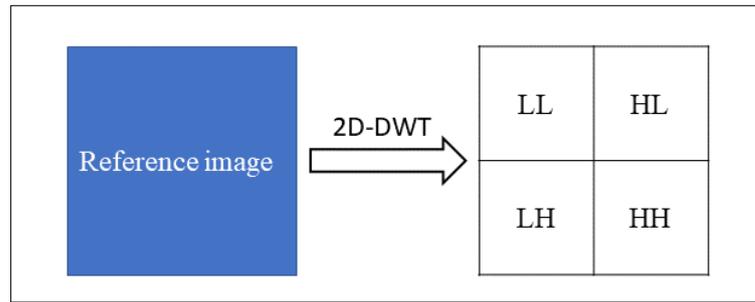


Figure 3. 2D-DWT process on reference image.

The U and V^H values are embedded into the sub-bands LH and HL , respectively, and s is embedded into HH after the encryption process. In this way LL remains unaltered, and the reference image remains visually meaningful despite the watermarking process. On the other hand, LL is used to generate the random matrixes for the encryption process. A QR decomposition is applied on LL to obtain an orthonormal matrix Q and upper-triangular matrix R following Equation (3).

$$LL = Q R \tag{3}$$

Q and R are used as random matrixes to map the vector s and the fingerprint feature vector, respectively. By mapping the values of s into Q according to Equation (4), the obtained vector s_m is a transformed vector, and the original vector s not be retrieved from s_m .

$$Q s = s_m \tag{4}$$

In the same way, the physician’s fingerprint feature vector f is mapped into R to obtain the mapped vector f_m according to Equation (5).

$$R f = f_m \tag{5}$$

The two mapped vectors s_m and f_m are concatenated to obtain a concatenated mapped vector c_m of size L and then c_m is permuted and embedded into HH following a random permutation key k . The key k is a matrix of integer numbers randomly generated in the range $[0, N]$ of size $L \times 3$. The first column of k defines the index of the values of c_m to be embedded in the position of HH determined by the values in the remaining two columns of k . Consequently, the first column of k has unique values in the range $[0, N]$ and the second and third columns have unique pairs of values same in the range $[0, N]$. The embedding process for each value of c_m into HH is detailed in Equation (6).

$$c_{m_{k_{i,j}}} \rightarrow HH_{k_{i,j+1}, k_{i,j+2}} \tag{6}$$

where \rightarrow defines the embedding operation, i and j are the row and column indexes of k , respectively. As a result of the embedding process, the new HH_p sub-band has been achieved. HH_p contains the original values of HH with the values of the c_m permuted vector in the position set by k . In this way a chaotic encryption has been realized to embed the vector s and the fingerprint feature vector in a safe manner. Moreover, k is encrypted through AES and ECC cryptography algorithms, as described in the next section, to increase the proposed scheme’s security.

The 2D-Inverse Discrete Wavelet Transform (2D-IDWT) is applied to reconstruct the reference image after the watermarking process, according to Equation (7).

$$I' = IDWT2(LL, U, V^H, HH_p, w) \tag{7}$$

where I' is the visually meaningful encrypted image and $IDWT$ is 2D-IDWT function. I' is visually very similar to I because the low frequency sub-band LL has not been altered

and the other new high frequency sub-bands (U, V^H, HH_p) do not contribute to the visual alteration of the image. Figure 4 shows the entire watermarking process applied to the reference image.

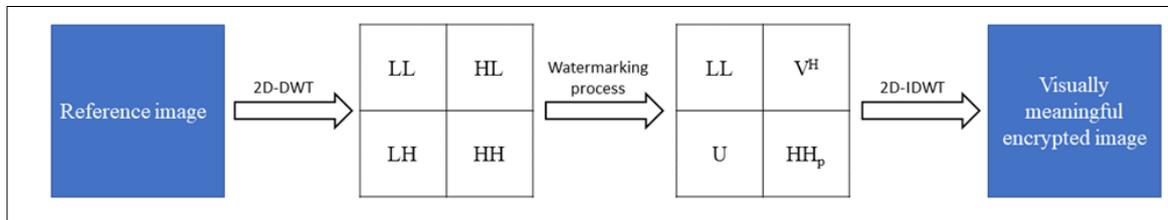


Figure 4. Watermarking process.

Finally, EHR is embedded into a visually meaningful encrypted image through the LSB algorithm. LSB consists of changing the least significant bit of each pixel in the image with each bit of text data. By changing the least significant bit of each pixel, the single pixel is not significantly altered, and the content of the image is preserved despite the manipulation. For example, given $p = [b_1^p, b_2^p, \dots, b_l^p]$ which represents the bit values of a pixel of I' , $e = [e_1, e_2, \dots, e_n]$ which represents the byte of EHR, and $e_1 = [b_1^{e_1}, b_2^{e_1}, \dots, b_m^{e_1}]$ which represents the bit values of the first byte of EHR, the LSB is applied according to Equation (8) for each p in the image I' .

$$b_l^p \leftarrow b_l^{e_j} \text{ with } i = 1, \dots, m \text{ and } j = 1, \dots, n \tag{8}$$

3.2. Key Protection Scheme

The permutation key k is the essential component to ensure the security of the watermarking process. To protect k , a hybrid asymmetric cryptography scheme based on ECC and AES has been implemented. ECC is an efficient type of public key cryptography. Its security is based on the difficulty of solving discrete logarithms on a field defined by specific equations computed over an elliptic curve. AES is a symmetric block cipher standardized by NIST with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. AES is the standard algorithm for symmetric encryption because it is very fast and secure. The disadvantage of AES is that the same key is used to cipher and decipher the data, and then the key represents a severe vulnerability. The proposed hybrid asymmetric cryptography scheme has been implemented to ensure a safe AES key exchange.

ECC generates an ECC public + private key pair for the message recipient and calculates the shared secret key for AES symmetric encryption and decryption. The shared secret key is an Elliptic Curve (EC) point, so it is then transformed into a 256-bit AES secret key. The EC points have the following property:

$$(a * G) * b = (b * G) * a$$

where a represents the private key, $a * G$ represents the public key, b represents the cipher private key, and $b * G$ represents the cipher public key. During the encryption process, the shared secret key is computed according to Equation (9).

$$sharedKey = cipherPrivateKey * publicKey \tag{9}$$

Additionally, the cipher public key is encapsulated in the encrypted message and will be used to recover the shared key during the decryption. Finally, the permutation key k is encrypted by using the shared secret key through the AES algorithm. The shared secret key is not directly sent to the receiver to decipher k but it is obtained from the private key

that is owned exclusively by the recipient. In the decryption phase, the shared secret key is computed by the private key and the cipher public key according to Equation (10).

$$sharedKey = cipherPublicKey * privateKey \tag{10}$$

The shared key is used to decrypt the permutation key k . Figure 5 shows the hybrid asymmetric encryption and decryption schemes, respectively.

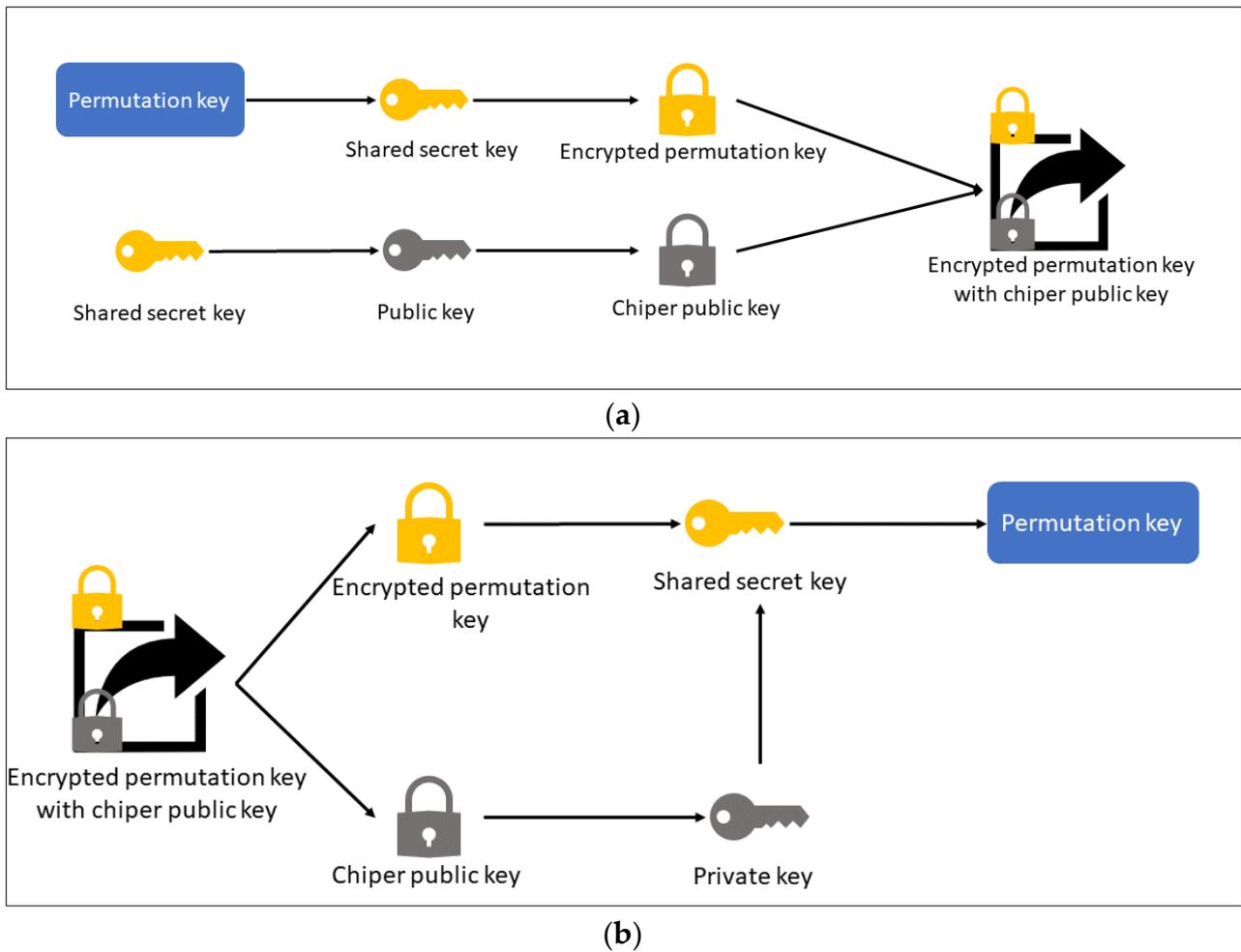


Figure 5. (a) Hybrid asymmetric encryption scheme; (b) Hybrid asymmetric decryption scheme.

3.3. Visually Secure Image Decryption Scheme

The proposed decryption scheme, shown in Figure 2, starts with the visually meaningful encrypted image received. The first step is to extract the EHR previously embedded by the LSB algorithm. The least significant bits are retrieved from each image pixel and decoded to achieve the medical information contained in the EHR. Subsequently, the medical image and the physician’s fingerprint feature have been retrieved. The 2D-DWT is performed on the visually meaningful encrypted image to obtain the four sub-bands LL' , LH' , HL' according to Equation (11).

$$LL', LH', HL', HH' = DWT2(I', w) \tag{11}$$

The wavelet w is the same wavelet used in the encryption scheme in order to ensure the correct decomposition. The sub-band LH' contains the values of matrix U , the sub-band HL' contains the values of matrix V^H , and HH' contains the c_m permuted vector in the position set by the permutation key k . The permuted vector c_m is extracted from HH'

following the permutation key k according to Equation (12). k is obtained after the hybrid asymmetric decryption scheme described in the previous section.

$$HH_{k_{i,j+1}, k_{i,j+2}} \rightarrow c_{m_{k_{i,j}}} \quad (12)$$

Equation (12) is the inverse of the embedding process from Equation (6). The obtained vector c_m is the vector permuted, and it is sorted following the first column of k to achieve the original mapped vector. The original mapped vector contains the mapped vector s_m and the mapped feature vector f_m concatenated. After the de-concatenation process, the singular value vector s' and fingerprint feature vector f' are computed by applying the least-squares method (LSTSQ) to Equations (4) and (5). LSTSQ computes an approximate solution x to a linear matrix equation in the form $ax = b$. So, the least-squares method is used to compute s' and f' that are approximate solutions of Equations (4) and (5), respectively. The coefficient matrixes Q and R to solve the Equations (4) and (5) are achieved through QR decomposition of sub-band LL' as performed in the image encryption scheme.

The fingerprint feature vector f' is used to ensure the authenticity of the received image by matching f' with the fingerprint feature of the physician sender contained in the hospital database. The vector s' is used to retrace the medical image by the SVD reconstruction process according to Equation (13). The vector s' is first converted into a diagonal matrix $D = (d_{i,j})$ of size $N \times N$ and then the dot product with U and V^H has been computed.

$$\begin{aligned} d_{i,j} &= 0 \quad i \neq j \\ d_{i,j} &= s'_i \quad i = j \\ \text{medical_image} &= U \cdot (D \cdot (V^H)) \end{aligned} \quad (13)$$

The medical image is recovered without any loss, as shown in Section 4.

4. Simulation Results and Analysis

The proposed visually secure image encryption scheme is simulated using different medical images embedded into different not significant images to analyze the scheme's performance in terms of the visual quality of image encryption, the quality of the image reconstruction, the relative error of the extracted physician's fingerprint feature, computational cost, and scheme security. The medical images used are collected by six different medical image datasets [40–45]. For each dataset, one medical image is selected to obtain the medical test images, namely "lungs", "pelvic", "head", "skin", "breast", and "kidney", as shown in Figure 6a. To show a relatively fair simulation result and be comparable with other image encryption schemes, six classical and widely used images are used as reference non-significant images, namely "Barbara", "Lena", "airplane", "pepper", "baboon", and "girl", as shown in Figure 6b. To simulate the embedding process of the physician's fingerprint feature into the encrypted image, a fingerprint image is selected by the FVC2002 dataset [46], and the features are extracted through a Fingerprint Feature Extraction algorithm [47].

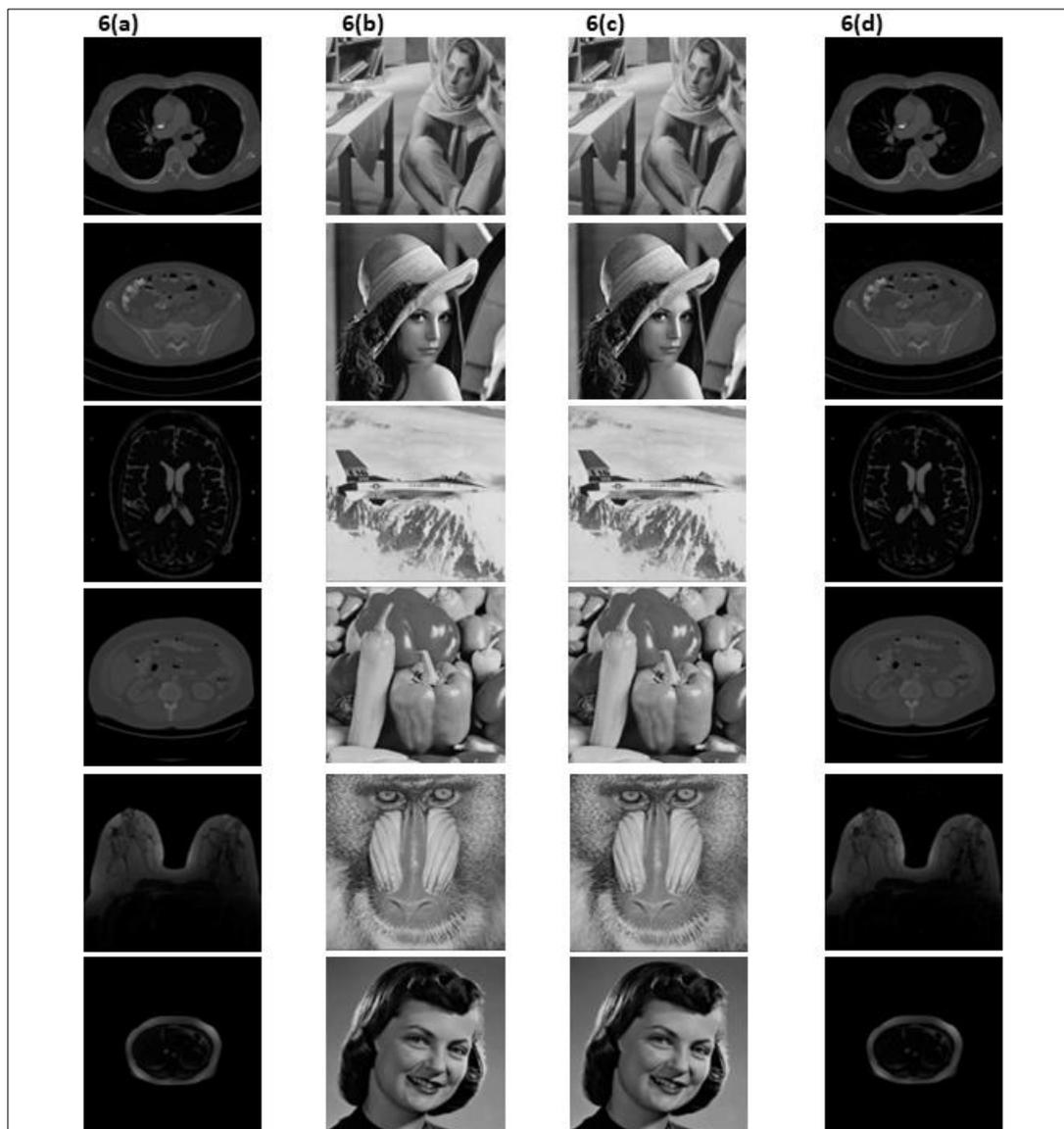


Figure 6. (a) medical images to be transmitted and protected; (b) not-significant reference images; (c) visually meaningful encrypted images; (d) reconstructed medical images.

4.1. Simulation Results

The proposed visually secure image encryption scheme is simulated using one medical image as an image to embed and one not significant image as a reference image for each test image. The wavelet used in 2D-DWT is ‘haar’, and the public and private keys for the key protection scheme are generated using Brainpool elliptic curves of 256 bits.

Figure 6c shows the simulation results of the visually meaningful encrypted images obtained given Figure 6a,b images as input. After embedding the medical images (Figure 6a) into reference images (Figure 6b), the generated encrypted images (Figure 6c) have the same visual effects as the reference images. This reduces the attention of the attackers and their tentative attacks, thus protecting the medical images. Subsequently, the proposed visually secure image decryption scheme enables the reconstruction of medical images by ensuring high quality and the same visual effect as the original medical images, as shown in Figure 6d.

To qualitatively assess the proposed scheme’s performance, the PSNR and MSSIM have been computed. PSNR is a mathematical metric used to calculate the quality of the

reconstructed image [48]. It is computed between an original image and the corresponding reconstructed image according to Equation (14).

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right) \tag{14}$$

where *MSE* is the mean squared error, and it defines the average squared difference between the estimated values and the actual values. *MSE* between two images *I* and *I'* is computed following Equation (15).

$$MSE = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (I(i, j) - I'(i, j))^2}{N \times N} \tag{15}$$

MSSIM is a metric used for measuring the structural similarity between two images [49]. MSSIM considers image degradation as the perceived change in structural information that is based on the high interdependencies between the pixels, especially when they are spatially close. MSSIM between two images *I* and *I'* is computed according to Equation (16).

$$MSSIM = \frac{1}{M} \sum_{k=1}^M \frac{(2\mu_I \mu_{I'} + C_1)(2\sigma_{II'} + C_2)}{(\mu_I^2 + \mu_{I'}^2 + C_1)(\sigma_I^2 + \sigma_{I'}^2 + C_2)} \tag{16}$$

where *M* is the number of image block, μ_I and $\mu_{I'}$ are the pixel sample mean of image *I* and *I'* respectively. σ_I^2 and $\sigma_{I'}^2$ are the variance of *I* and *I'*, respectively. $\sigma_{II'}$ is the covariances of *I* and *I'*. *C*₁ and *C*₂ are two parameters to stabilize the division with a weak denominator. MSSIM values are in the range −1 and 1 where 1 means that the two images are identical.

Table 1 shows the PSNR and MSSIM results. To evaluate the quality of the reconstructed medical image, the PSNR and MSSIM are computed between the original medical image (Figure 6a) and the reconstructed medical image (Figure 6d). To evaluate the visual quality of the visually meaningful encrypted image, the PSNR and MSSIM are computed between the original reference image (Figure 6b) and the encrypted image (Figure 6c).

Table 1. The PSNR and MSSIM values between the reconstructed medical images and the original medical images and between the original reference images and visually meaningful encrypted images.

Medical Image	Reference Image	Reconstructed Medical Image		Visually Meaningful Encrypted Image	
		PSNR	MSSIM	PSNR	MSSIM
lungs	Barbara	52.163	0.992	32.291	0.860
pelvic	Lena	52.952	0.996	38.786	0.967
head	airplane	54.401	0.997	38.586	0.972
skin	pepper	54.861	0.998	39.718	0.971
breast	baboon	54.590	0.996	32.998	0.920
kidney	girl	60.526	0.999	40.316	0.975

The PSNR values between the reconstructed medical images and the original medical images are above 52 dB, and all the MSSIM values are above 0.99. Both indices show that the reconstructed medical images have high similarity to the original medical images. It is the main requirement for the proposed scheme because the medical images must be reconstructed without any loss to ensure a correct medical diagnosis. Moreover, all the visually meaningful encrypted images also achieve high PSNR and MMSSIM values compared to the original reference images. Therefore, the proposed scheme can not only encrypt and embed a medical image into a less significant image but also generate an encrypted image of high quality to ensure visual security. The proposed scheme fulfills the requirements of visual security, medical image encryption, and reconstruction quality.

4.2. Histogram Analysis

The histogram of an image graphically represents the intensity distribution of pixel values. A different histogram from an original image and a cover image can disclose the presence of embedded data in the image. To ensure high visual security, the histogram of the reference image and the visually meaningful encrypted image must be very similar. Figure 7b shows the histograms of the original reference image (Figure 7a). Figure 7d shows the comparison between the histograms of the encrypted images achieved after the proposed secure image encryption scheme (line red) and the histograms of the reference images (line blue).

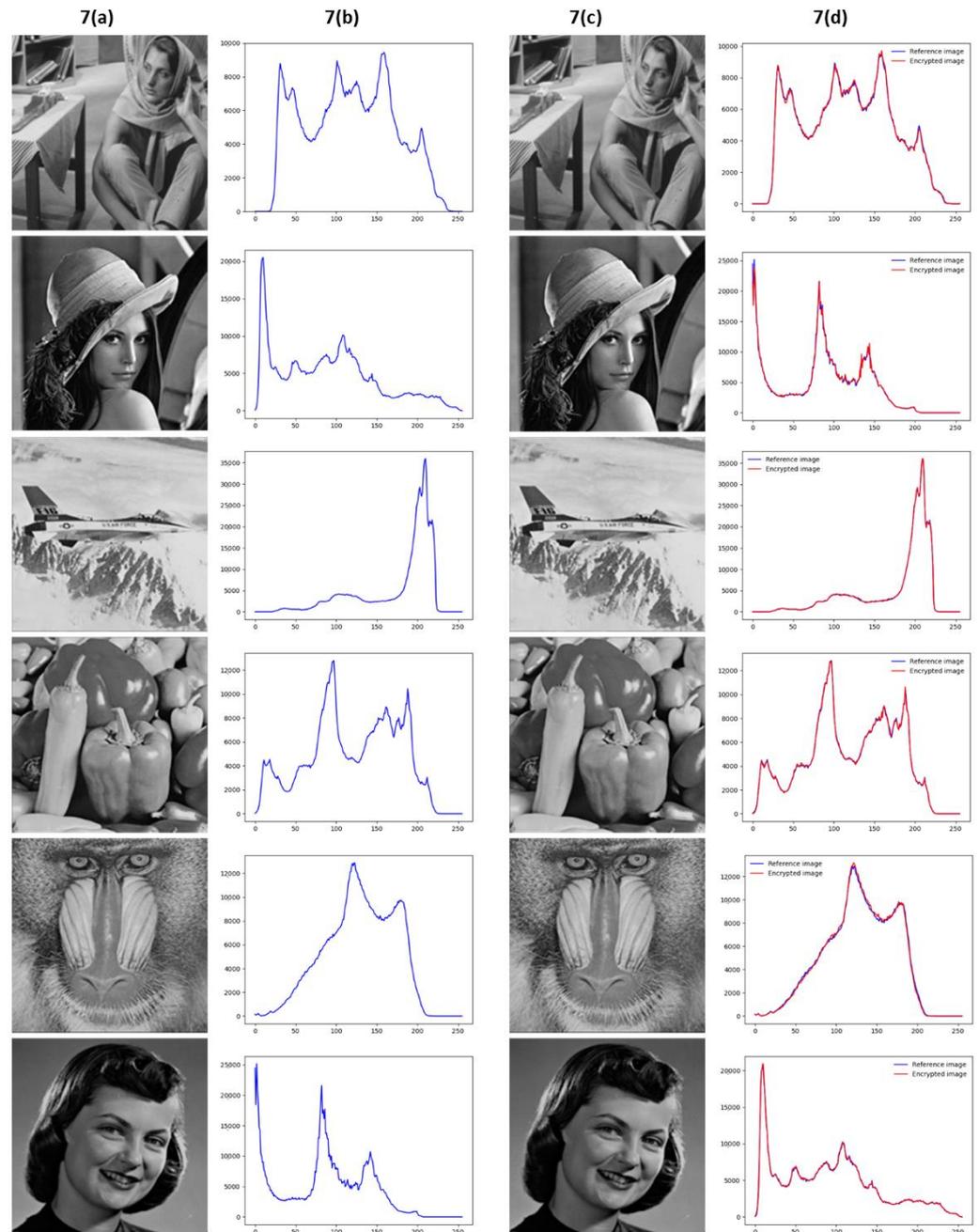


Figure 7. Histogram analysis of reference images and their corresponding visually meaningful encrypted images. (a) reference images; (b) histograms of reference images; (c) visually meaningful encrypted images; (d) comparison between the histograms of the encrypted images and the histograms of the reference images.

Figure 7d shows that the histograms of the reference images and the histograms of the visually meaningful encrypted images are very similar because the two histograms are nearly perfectly overlapped at every point for each image. To test the difference between two histograms, the distance of histogram intersection has been computed following Equation (17). A value close to 1 indicates that the two histograms are very similar.

$$d(H_1, H_2) = \frac{\sum_I \min(H_1(I), H_2(I'))}{N \times N} \quad (17)$$

Table 2 shows the distances of histogram intersection between the reference images and the visually meaningful encrypted images.

Table 2. The distances of histogram intersection between the reference image and the visually meaningful encrypted image.

Reference Image	Embedded Medical Image	Distance of Histogram Intersection
Barbara	lungs	0.968
Lena	pelvic	0.989
airplane	head	0.992
pepper	skin	0.992
baboon	breast	0.987
girl	kidney	0.980

The distance values in Table 2 are above 0.98, and thus the visually meaningful encrypted images do not provide any information about the presence of embedded data.

4.3. Comparison Analysis

The proposed scheme is compared to other schemes of visually secure image encryption introduced in [48–52]. The quality of the reconstructed image is the main requirement in a medical image encryption scheme. The averages of PSNR and MSSIM obtained between the embedded image (medical image) and the image reconstructed by the proposed scheme have been compared with the other schemes to evaluate the quality of the reconstructed image. Table 3 shows the comparison results. On the other hand, the visual security of the visually meaningful encrypted image is another essential requirement. The PSNR achieved between the reference images and the visually meaningful encrypted image has been compared to evaluate the visual security of the proposed system, and the results have been shown in Table 4. The same images used as carrier images in the other approaches have been used as reference images in the comparison analysis to provide a fair comparison. N/A in Tables 3 and 4 refers to information not available in the comparison schemes.

Table 3. Comparison of the average PSNR and MSSIM values of reconstructed images (the best results are shown in bold).

	[48]	[50]	[51]	[52]	[53]	[54]	Proposed Scheme
PSNR	49.137	35.107	33.4204	32.4235	51.6860	31.62	54.947
MSSIM	0.92339	0.95564	N/A	0.8855	N/A	0.9887	0.9963

Table 4. Comparison of the PSNR values of the visually meaningful encrypted images (the best results are shown in bold).

	[48]	[50]	[51]	[52]	[54]	Proposed Scheme
Barbara	N/A	N/A	N/A	N/A	N/A	32.291
Lena	55.5123	N/A	N/A	N/A	N/A	38.786
airplane	56.5828	N/A	N/A	N/A	N/A	N/A
pepper	55.5071	40.9310	32.3513	35.1347	34.51	39.718
baboon	55.1570	40.9187	37.1058	36.4906	N/A	32.998
girl	57.3175	N/A	N/A	N/A	N/A	40.316

The proposed scheme achieves the highest PSNR and MSSIM values of reconstructed images compared to other approaches, as shown in Table 3. Therefore, the proposed scheme is appropriate for medical image protection, where accurate image reconstruction is the most crucial requirement. Table 4 shows that the PSNR values of the visually meaningful encrypted images are not the highest compared to other approaches. However, the visual security of the encrypted image is, in any case, ensured, as shown in Tables 1 and 2.

4.4. Extracted Fingerprint Feature Analysis

The physician's fingerprint features are encrypted and embedded into the reference image. During the decryption scheme, the features are extracted and reconstructed through the LSTSQ algorithm. To evaluate the correctness of the feature reconstruction, the relative error between the original feature vector f and the reconstructed feature vector f' has been computed following Equation (18).

$$e_r = \frac{|f - f'|}{|f|} \quad (18)$$

The relative error computed after the fingerprint feature reconstruction for each test image is equal to 8.32411×10^{-10} . As shown, the values of the relative error between f and f' are very low. Therefore, the reconstructed feature vector can be used for an accurate fingerprint matching with the fingerprint stored in the database.

4.5. Key Security Analysis

The security of the proposed scheme is based on visual security, and a random permutation key k . Without k is extremely complex to know the mapped vector c_m embedded in reference image sub-band to reconstruct the singular value vector and fingerprint feature vector. The space of possible values of c_m is equal to the size of sub-band. Furthermore, to correctly reconstruct the singular value vector and fingerprint feature vector from c_m through LSTSQ algorithm, the order of the vector values is essential. Therefore, the values of c_m extracted must be in the same order as the original vectors to ensure a correct reconstruction. Figure 8 shows the reconstructed medical images using the random shuffle of mapped vector s_m values to simulate the scenario where an attacker tries to reconstruct a medical image without knowing k .

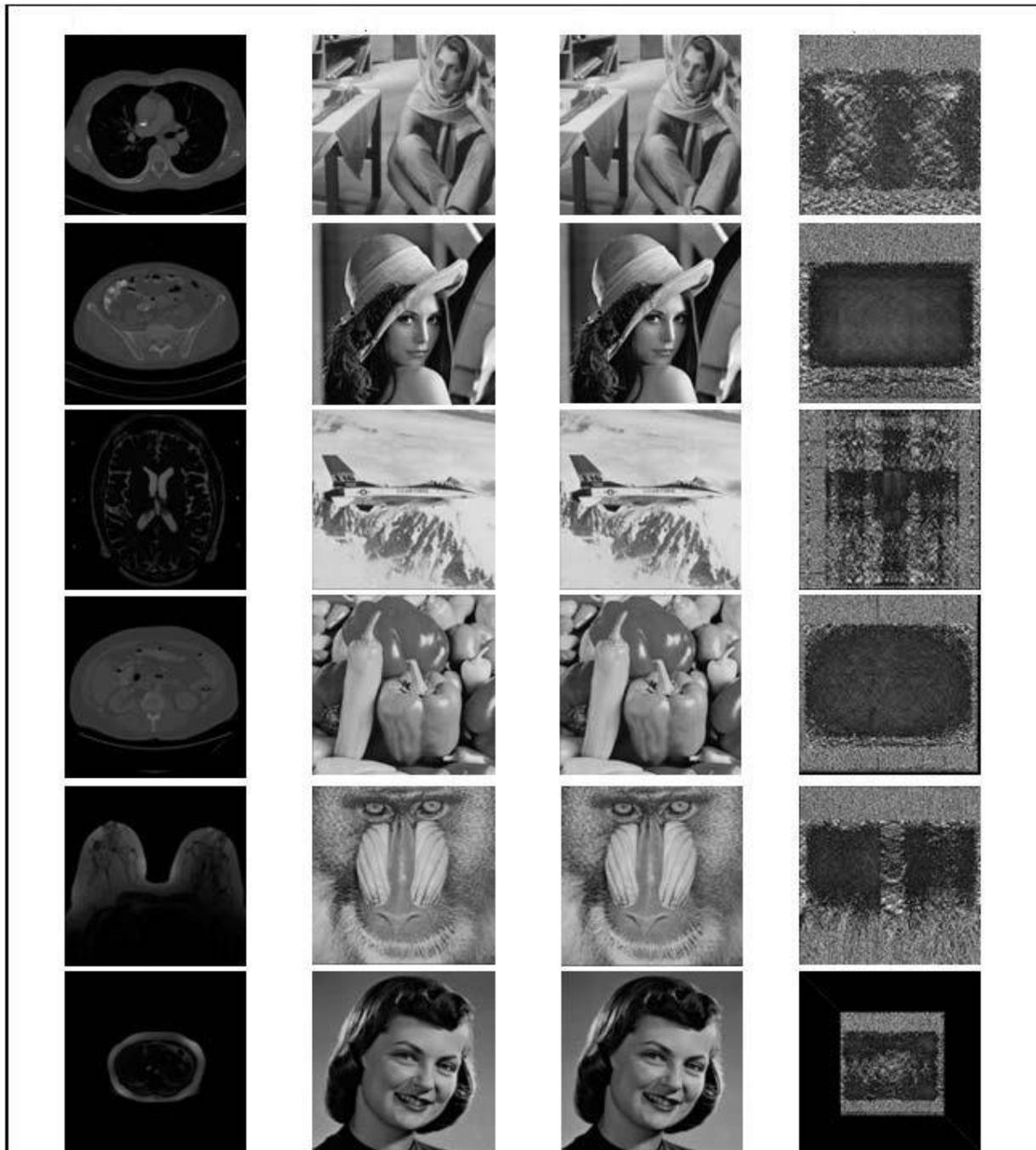


Figure 8. Reconstructed medical images with the random shuffle of mapped vector s_m .

To correctly reconstruct a medical image without knowing k it is necessary to make a number of possible attempts equal to the number of ordered sequences of N distinct elements and extracted from the set of M elements. Therefore, the number of possible attacks attempts with a medical image size of 512×512 and a reference image size of 1024×1024 is given in Equation (19).

$$D_{M,N} = \frac{M!}{(M - N)!}; \frac{(512 \times 512)!}{((512 \times 512) - 512)!}; \frac{262144!}{(262144 - 512)!} \quad (19)$$

Without k is computationally costly correctly reconstructed medical image for an attacker, as shown from Equation (19).

The security of k is given by the hybrid asymmetric cryptography scheme based on ECC and AES. The secret key used in the proposed scheme to encrypt and decrypt k consists of 256 bits, and thus the key space is 2^{256} . It is a key space sufficiently large to resist brute-force attack. Without the secret key, it is not possible to retrieve k and thus is not possible reconstructed medical image.

4.6. Running Efficiency Analysis

Medical image transmission is a real time task, and thus the running time of the proposed system is an important requirement. Table 5 shows the encryption and decryption times (in seconds) of the proposed scheme for each medical image of a test. The encryption and decryption times depend on the size of the medical image because, when the image is larger, there is more data to embed and extract from the reference image. The medical image size is 512×512 , and the reference images size is 1024×1024 . To test running time, the experiment is performed on a computer with an AMD A10-9620P @ 2.50 GHz and 8 GB of RAM.

Table 5. Encryption and decryption time.

Medical Image	Refence Image	Encryption Time (s)	Decryption Time (s)
lungs	Barbara	13.547	10.143
pelvic	Lena	53.109	57.433
head	airplane	3.419	6.188
skin	pepper	3.316	3.665
breast	baboon	4.884	4.156
kidney	girl	4.056	3.345

Table 5 shows that the proposed scheme achieves high encryption and decryption efficiency with images of high size. Therefore, the proposed scheme can be used to protect medical image transmission in real-world applications.

5. Conclusions

A visually secure image encryption scheme with fingerprint-based authentication has been proposed to ensure integrity, authenticity, and confidentiality during medical image transmission. A watermarking process ensures visual security by embedding a medical image into a non-significant reference image to achieve a visually meaningful encrypted image without compromising its visual quality. In addition, an encryption scheme based on random mapping and a random permutation key has been implemented to protect the medical image and fingerprint features and ensure security against white-box attacks. Simulation results show high mean PSNR values of 54.947 dB between the original and reconstructed medical images. However, the distances of histogram intersection between the original reference images and visually meaningful encrypted images are above 0.98. These values demonstrate the quality of the image reconstruction and the visual security of the proposed scheme. Comparison results show that the proposed scheme achieved the best performance in reconstructed image quality compared to other visually secure image encryption schemes.

On the other hand, the proposed scheme ensured both visual protection and encryption of medical images and the physician's fingerprint, compared with other single-protection approaches. In future work, multimodal biometric data will be used to improve the image authentication process. Moreover, the running time of the proposed scheme can be improved by reducing the data to be embedded using small images.

Author Contributions: Conceptualization, F.C. and D.I.; methodology, F.C. and G.P.; software, F.C.; validation, F.C.; formal analysis, F.C.; investigation, F.C.; resources, F.C. and D.I.; data curation, F.C.; writing—original draft preparation, F.C.; writing—review and editing, F.C. and D.I.; visualization, D.I. and G.P.; supervision, D.I. and G.P.; project administration, D.I. and G.P.; funding acquisition, D.I. and G.P. All authors have read and agreed to the published version of the manuscript.

Funding: FAIR PNRR.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Francesco Castro is a PhD student enrolled in the National PhD in Artificial Intelligence, XXXVIII cycle, course on health and life sciences, organized by “Università Campus Bio-Medico di Roma”. This work is partially supported by the co-funding of the European Union -Next Generation EU: NRRP Initiative, Mission 4, Component 2, Investment 1.3–Partnerships extended to universities, research centres, companies and research D.D. MUR n. 341 del 15.03.2022–Next Generation EU (PE0000013–“Future Artificial Intelligence Research–FAIR”–CUP: H97G22000210007).

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

References

1. Arbabshirani, M.R.; Plis, S.; Sui, J.; Calhoun, V.D. Single subject prediction of brain disorders in neuroimaging: Promises and pitfalls. *Neuroimage* **2017**, *145*, 137–165. [[CrossRef](#)] [[PubMed](#)]
2. Sharma, S.; Mandal, P.K. A Comprehensive Report on Machine Learning-Based Early Detection of Alzheimer’s Disease using Multi-modal Neuroimaging Data. *ACM Comput. Surv.* **2023**, *55*, 1–44. [[CrossRef](#)]
3. Gattulli, V.; Impedovo, D.; Pirlo, G.; Semeraro, G. Early Dementia Identification: On the Use of Random Handwriting Strokes. In *Lecture Notes in Computer Science*; (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2022; Volume 13424 LNCS, pp. 285–300.
4. Dentamaro, V.; Giglio, P.; Impedovo, D.; Moretti, L.; Pirlo, G. AUCCO ResNet: An end-to-end network for COVID-19 pre-screening from cough and breath. *Pattern Recognit.* **2022**, *127*, 108656. [[CrossRef](#)] [[PubMed](#)]
5. Litjens, G.; Kooi, T.; Bejnordi, B.E.; Setio, A.A.A.; Ciompi, F.; Ghafoorian, M.; van der Laak, J.A.W.M.; van Ginneken, B.; Sánchez, C.I. A survey on deep learning in medical image analysis. *Med. Image Anal.* **2017**, *42*, 60–88. [[CrossRef](#)] [[PubMed](#)]
6. Wang, X.; Du, Y.; Yang, S.; Zhang, J.; Wang, M.; Zhang, J.; Yang, W.; Huang, J.; Han, X. RetCCL: Clustering-guided contrastive learning for whole-slide image retrieval. *Med. Image Anal.* **2023**, *83*, 102645. [[CrossRef](#)]
7. McKinney, S.M.; Sieniek, M.; Godbole, V.; Godwin, J.; Antropova, N.; Ashrafian, H.; Back, T.; Chesus, M.; Corrado, G.S.; Darzi, A.; et al. International evaluation of an AI system for breast cancer screening. *Nature* **2020**, *577*, 89–94. [[CrossRef](#)]
8. Balasamy, K.; Suganyadevi, S. A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. *Multimed. Tools Appl.* **2021**, *80*, 7167–7186.
9. Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 18–21 May 2008; pp. 111–125.
10. Schwarz, C.G.; Kremers, W.K.; Therneau, T.M.; Sharp, R.R.; Gunter, J.L.; Vemuri, P.; Arani, A.; Spsychalla, A.J.; Kantarci, K.; Knopman, D.S.; et al. Identification of Anonymous MRI Research Participants with Face-Recognition Software. *N. Engl. J. Med.* **2019**, *381*, 1684–1686. [[CrossRef](#)]
11. Kaissis, G.; Ziller, A.; Passerat-Palmbach, J.; Ryffel, T.; Usynin, D.; Trask, A.; Lima, I.; Mancuso, J.; Jungmann, F.; Steinborn, M.-M.; et al. End-to-end privacy preserving deep learning on multi-institutional medical imaging. *Nat. Mach. Intell.* **2021**, *3*, 473–484. [[CrossRef](#)]
12. Zear, A.; Singh, A.K.; Kumar, P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed. Tools Appl.* **2018**, *77*, 4863–4882. [[CrossRef](#)]
13. Priya, S.; Santhi, B. A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images. *Mob. Netw. Appl.* **2021**, *26*, 2501–2508. [[CrossRef](#)]
14. Wan, W.; Wang, J.; Zhang, Y.; Li, J.; Yu, H.; Sun, J. A comprehensive survey on robust image watermarking. *Neurocomputing* **2022**, *488*, 226–247. [[CrossRef](#)]
15. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [[CrossRef](#)]
16. Parida, P.; Pradhan, C.; Gao, X.Z.; Roy, D.S.; Barik, R.K. Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps. *IEEE Access* **2021**, *9*, 76191–76204. [[CrossRef](#)]
17. Yang, X.; Li, T.; Pei, X.; Wen, L.; Wang, C. Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology. *IEEE Access* **2020**, *8*, 45468–45476. [[CrossRef](#)]
18. Sun, Y.; Zhang, R.; Wang, X.; Gao, K.; Liu, L. A decentralizing attribute-based signature for healthcare blockchain. In Proceedings of the International Conference on Computer Communications and Networks, ICCCN 2018, Hangzhou, China, 30 July–2 August 2018.
19. Kanwal, S.; Tao, F.; Almogren, A.; Rehman, A.U.; Taj, R.; Radwan, A. A Robust Data Hiding Reversible Technique for Improving the Security in e-Health Care System. *CMES Comput. Model. Eng. Sci.* **2023**, *134*, 201–219. [[CrossRef](#)]

20. Salunke, S.; Ahuja, B.; Hashmi, M.F.; Marriboyina, V.; Bokde, N.D. 5D Gauss Map Perspective to Image Encryption with Transfer Learning Validation. *Appl. Sci.* **2022**, *12*, 5321. [[CrossRef](#)]
21. Wang, D.; Zhang, X.; Yu, C.; Tang, Z. Reversible Data Hiding in Encrypted Image Based on Multi-MSB Embedding Strategy. *Appl. Sci.* **2020**, *10*, 2058. [[CrossRef](#)]
22. Lin, C.-H.; Hu, G.-H.; Chan, C.-Y.; Yan, J.-J. Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm. *Appl. Sci.* **2021**, *11*, 1329. [[CrossRef](#)]
23. Liang, H.; Zhang, G.; Hou, W.; Huang, P.; Liu, B.; Li, S. A Novel Asymmetric Hyperchaotic Image Encryption Scheme Based on Elliptic Curve Cryptography. *Appl. Sci.* **2021**, *11*, 5691. [[CrossRef](#)]
24. Wen, W.; Zhang, Y.; Fang, Y.; Fang, Z. Image salient regions encryption for generating visually meaningful ciphertext image. *Neural Comput. Appl.* **2018**, *29*, 653–663. [[CrossRef](#)]
25. Anand, A.; Singh, A.K. An improved DWT-SVD domain watermarking for medical information security. *Comput. Commun.* **2020**, *152*, 72–80. [[CrossRef](#)]
26. Cox, I.J.; Doërr, G.; Furon, T. Watermarking is not cryptography. In *Lecture Notes in Computer Science*; (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2006; Volume 4283 LNCS, pp. 1–15.
27. Han, B.; Jhaveri, R.; Wang, H.; Qiao, D.; Du, J. Application of Robust Zero-Watermarking Scheme Based on Federated Learning for Securing the Healthcare Data. *IEEE J. Biomed. Heal. Inform.* **2021**, *27*, 804–813. [[CrossRef](#)] [[PubMed](#)]
28. Li, T.; Li, J.; Liu, J.; Huang, M.; Chen, Y.W.; Bhatti, U.A. Robust watermarking algorithm for medical images based on log-polar transform. *EURASIP J. Wirel. Commun. Netw.* **2022**, *2022*, 1–11. [[CrossRef](#)]
29. Hua, Z.; Zhu, Z.; Yi, S.; Zhang, Z.; Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **2021**, *546*, 1063–1083. [[CrossRef](#)]
30. Wang, X.; Liu, C.; Jiang, D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Inf. Sci.* **2021**, *574*, 505–527. [[CrossRef](#)]
31. Singh, S.P.; Bhatnagar, G. A Novel Biometric Inspired Robust Security Framework for Medical Images. *IEEE Trans. Knowl. Data Eng.* **2021**, *33*, 810–823. [[CrossRef](#)]
32. Wang, X.; Zhu, Z.; Wang, F.; Ni, R.; Wang, J.; Hu, Y. Medical image encryption based on biometric keys and lower-upper decomposition with partial pivoting. *Appl. Opt.* **2021**, *60*, 24. [[CrossRef](#)]
33. Tao, S.; Tang, C.; Shen, Y.; Lei, Z. Optical image encryption based on biometric keys and singular value decomposition. *Appl. Opt.* **2020**, *59*, 2422. [[CrossRef](#)]
34. Shen, Y.; Tang, C.; Xu, M.; Lei, Z. Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image. *Opt. Laser Technol.* **2021**, *138*, 106911. [[CrossRef](#)]
35. Lian, S.; Sun, J.; Wang, Z. A block cipher based on a suitable use of the chaotic standard map. *Chaos Solitons Fractals* **2005**, *26*, 117–129. [[CrossRef](#)]
36. Lei, T.; Jia, X.; Zhang, Y.; He, L.; Meng, H.; Nandi, A.K. Significantly Fast and Robust Fuzzy C-Means Clustering Algorithm Based on Morphological Reconstruction and Membership Filtering. *IEEE Trans. Fuzzy Syst.* **2018**, *26*, 3027–3041. [[CrossRef](#)]
37. Aparna, P.; Kishore, P.V.V. Biometric-based efficient medical image watermarking in E-healthcare application. *IET Image Process.* **2019**, *13*, 421–428. [[CrossRef](#)]
38. Singh, N.; Joshi, S.; Birla, S. Color Image Watermarking with Watermark Authentication against False Positive Detection Using SVD. In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Jaipur, India, 2 February 2019. [[CrossRef](#)]
39. Parida, P.; Bhoi, N. Wavelet based transition region extraction for image segmentation. *Future Comput. Inform. J.* **2017**, *2*, 65–78. [[CrossRef](#)]
40. Albertina, B.; Watson, M.; Holback, C.; Jarosz, R.; Kirk, S.; Lee, Y.; Rieger-Christ, K.; Lemmerman, J. The Cancer Genome Atlas Lung Adenocarcinoma Collection (TCGA-LUAD) (Version 4) [Data Set]. The Cancer Imaging Archive. 2016. Available online: <https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=6881474> (accessed on 28 March 2023).
41. Tong, T.; Li, M. Abdominal or Pelvic Enhanced CT Images within 10 Days before Surgery of 230 Patients with Stage II Colorectal Cancer (StageII-Colorectal-CT) [Dataset]. The Cancer Imaging Archive. 2022. Available online: <https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=117113567> (accessed on 28 March 2023).
42. Shapey, J.; Kujawa, A.; Dorent, R.; Wang, G.; Dimitriadis, A.; Grishchuk, D.; Paddick, I.; Kitchen, N.; Bradford, R.; Saeed, S.R.; et al. Segmentation of Vestibular Schwannoma from Magnetic Resonance Imaging: An Open Annotated Dataset and Baseline Algorithm. *Sci. Data* **2021**, *8*, 286. [[CrossRef](#)] [[PubMed](#)]
43. National Cancer Institute Clinical Proteomic Tumor Analysis Consortium (CPTAC). *The Clinical Proteomic Tumor Analysis Consortium Cutaneous Melanoma Collection (CPTAC-CM) (Version 10) [Data Set]*. The Cancer Imaging Archive; CPTAC: Rockville, MD, USA, 2018; Available online: <https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=33948224> (accessed on 28 March 2023).
44. Saha, A.; Harowicz, M.R.; Grimm, L.J.; Weng, J.; Cain, E.H.; Kim, C.E.; Ghate, S.V.; Walsh, R.; Mazurowski, M.A. Dynamic Contrast-Enhanced Magnetic Resonance Images of Breast Cancer Patients with Tumor Locations [Data Set]. The Cancer Imaging Archive. 2021. Available online: <https://wiki.cancerimagingarchive.net/pages/viewpage.action?pageId=70226903> (accessed on 28 March 2023).

45. Clark, K.; Vendt, B.; Smith, K.; Freymann, J.; Kirby, J.; Koppel, P.; Moore, S.; Phillips, S.; Maffitt, D.; Pringle, M.; et al. The Cancer Imaging Archive (TCIA): Maintaining and Operating a Public Information Repository. *J. Digit. Imaging* **2013**, *26*, 1045–1057. [[CrossRef](#)] [[PubMed](#)]
46. Maio, D.; Maltoni, D.; Cappelli, R.; Wayman, J.L.; Jain, A.K. FVC2002: Second fingerprint verification competition. In Proceedings of the International Conference on Pattern Recognition, Quebec City, QC, Canada, 11–15 August 2002; Volume 16, pp. 811–814.
47. Wieclaw, L. A Minutiae-Based Matching Algorithms in Fingerprint Recognition Systems. *J. Med. Inform.* **2009**. Available online: https://www.academia.edu/2508970/A_minutiae_based_matching_algorithms_in_fingerprint_recognition_systems (accessed on 28 March 2023).
48. Patel, S.; Vaish, A. Block based visually secure image encryption algorithm using 2D-Compressive Sensing and nonlinearity. *Optik* **2023**, *272*, 170341. [[CrossRef](#)]
49. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–612. [[CrossRef](#)]
50. Hua, Z.; Zhang, K.; Li, Y.; Zhou, Y. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. *Signal Process.* **2021**, *183*, 107998. [[CrossRef](#)]
51. Wang, H.; Xiao, D.; Li, M.; Xiang, Y.; Li, X. A visually secure image encryption scheme based on parallel compressive sensing. *Signal. Process.* **2019**, *155*, 218–232. [[CrossRef](#)]
52. Ping, P.; Fu, J.; Mao, Y.; Xu, F.; Gao, J. Meaningful Encryption: Generating Visually Meaningful Encrypted Images by Compressive Sensing and Reversible Color Transformation. *IEEE Access* **2019**, *7*, 170168–170184. [[CrossRef](#)]
53. Dhall, S.; Gupta, S. Multilayered highly secure authentic watermarking mechanism for medical applications. *Multimed. Tools Appl.* **2021**, *80*, 18069–18105. [[CrossRef](#)]
54. Chai, X.; Wu, H.; Gan, Z.; Zhang, Y.; Chen, Y.; Nixon, K.W. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. *Opt. Lasers Eng.* **2020**, *124*, 105837. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.