Journal of
Sensor and Actuator Networks

MDPI

Article

MID-Crypt: A Cryptographic Algorithm for Advanced Medical Images Protection

Ashraf Ahmad [1], Yousef AbuHour [2], Remah Younisse [1], Yasmeen Alslman [1], Eman Alnagi [1] and Qasem Abu Al-Haija [1,*]

[1] Department of Computer Science/Cybersecurity, Princess Sumaya University for Technology (PSUT), Amman 11941, Jordan; a.ahmad@psut.edu.jo (A.A.); r.baniyounisse@psut.edu.jo (R.Y.); yas20219006@std.psut.edu.jo (Y.A.); ema20219005@std.psut.edu.jo (E.A.)

[2] Jordan Design Development Bureau (JODDB), National Encryption Center, Amman 11180, Jordan; yousef.abu.hour@gmail.com

* Correspondence: q.abualhaija@psut.edu.jo

Abstract: Privacy-preserving of medical information (such as medical records and images) is an essential right for patients to ensure security against undesired access parties. This right is typically protected by law through firm regulations set by healthcare authorities. However, sensitive-private data usually requires the application of further security and privacy mechanisms such as encipherment (encryption) techniques. 'Medical images' is one such example of highly demanding security and privacy standards. This is due to the quality and nature of the information carried among these images, which are usually sensitive-private information with few features and tonal variety. Hence, several state-of-the-art encryption mechanisms for medical images have been proposed and developed; however, only a few were efficient and promising. This paper presents a hybrid crypto-algorithm, MID-Crypt, to secure the medical image communicated between medical laboratories and doctors' accounts. MID-Crypt is designed to efficiently hide medical image features and provide high-security standards. Specifically, MID-Crypt uses a mix of Elliptic-curve Diffie–Hellman (ECDH) for image masking and Advanced Encryption Standard (AES) with updatable keys for image encryption. Besides, a key management module is used to organize the public and private keys, the patient's digital signature provides authenticity, and integrity is guaranteed by using the Merkle tree. Also, we evaluated our proposed algorithm in terms of several performance indicators including, peak signal-to-noise ratio (PSNR) analysis, correlation analysis, entropy analysis, histogram analysis, and timing analysis. Consequently, our empirical results revealed the superiority of MID-Crypt scoring the best performance values for PSNR, correlation, entropy, and encryption overhead. Finally, we compared the security measures for the MID-Crypt algorithm with other studies, the comparison revealed the distinguishable security against several common attacks such as side-channel attacks (SCA), differential attacks, man-in-the-middle attacks (MITM), and algebraic attacks.

Keywords: medical information; key management; Elliptic-curve Diffie—Hellman (ECDH); Advanced Encryption Standard (AES); Merkel tree digital signature

check for updates

Citation: Ahmad, A.; AbuHour, Y.; Younisse, R.; Alslman, Y.; Alnagi, E.; Abu Al-Haija, Q. MID-Crypt: A Cryptographic Algorithm for Advanced Medical Images Protection. *J. Sens. Actuator Netw.* **2022**, *11*, 24. https://doi.org/10.3390/jsan11020024

Academic Editor: Mohamed Amine Ferrag

Received: 13 April 2022
Accepted: 10 May 2022
Published: 13 May 2022

1. Introduction

With the emergence of technology in all scopes and sectors, high-tech machines are widely used in medical centers to generate digital medical images. X-rays, MRIs, and CT scans are examples of different types of medical images. Physicians need such images for diagnosing many types of illnesses. These images are stored and need to be shared through several means, one of them being via the Internet. When sharing images over the Internet their privacy will be under threat of malicious attacks. Thus, encryption of medical images has become a vital scope for research and application.

Researchers have been highly motivated by the importance of the preservation of privacy for medical images, in addition to the massive generation of such images in most medical centers. In addition to the physical medical centers, medical applications and solutions have been widely used to connect patients and doctors with different specialties, in order to require and gain a fast diagnosis. Patients cannot use such applications without being comfortable that their information privacy has been preserved [1].

According to research databases, encryption algorithms have been proposed since the middle of the twentieth century. Image encryption on the other hand has started to evolve and tackle in the nineteens of it. Starting from 1998, research started to tackle the problem of how to secure medical images and preserve their privacy [2–4]. A considerable encryption scheme has to provide a secured data sharing method for patients' records, ensuring both confidentiality and integrity. It also should avoid changing medical images and stand robust against cybersecurity attacks [5] and the darkNets [6].

In this paper, we propose an efficient approach to address the privacy-preserving and ensure the security requirements of the medical images communicated between medical laboratories and doctors' accounts. We call this approach MID-Crypt. Specifically, the main contributions of this work can be summarized as follows:

- We propose a new hybrid cryptographic algorithm, MID-Crypt, that makes use of the ECDH for image masking and the updatable AES for image encryption.
- We present an inclusive crypto-architecture for MID-Crypt comprising modules for: key management module, medical image encryption module, Data Integrity module, Digital Signature module, and medical image decryption module.
- We provide a performance evaluation and benchmarking comparison results using standard key performance indicators: PSNR, entropy, and computational overhead. We also show the superiority of MID-Crypt over other state-of-art approaches.

The rest of this paper is organized as follows: Section 2 surveys some of the up-to-date solutions reported in the literature. Section 3 describes the proposed crypto-algorithm architecture along with each subsystem (module). Section 4 provides the performance evaluation environment, results, discussion, and comparison. Finally, Section 5 concludes the paper.

2. Related Work

In the last decade, the medical image encryption issue has been addressed and researched extensively in the preceding state-of-the-art research work. Several approaches have been applied to encrypt medical images and provide privacy-preserving for patients' records. In this section, we survey a number of recent related works in the field of medical image encryption. For instance, researchers of [7] presented two crypto-based algorithms for encrypting DICOM images. Robust cryptographic functions have been used, including hash codes and symmetric keys. The whirlpool hash function is employed with the Advanced Encryption Standard-Galois counter mode to give confidentiality and authenticity. Nevertheless, their algorithms are time-consuming since both algorithms' encryption processes took nearly 811 and 484 s, respectively. Also, Chen and Hu [8] have proposed an adaptive encryption algorithm for medical images based on the enhanced chaotic mapping. They have used Logistic sine chaos mapping to scramble the original image. Then the resulting image is divided into sub-blocks and then each of these sub-blocks is encrypted using the hyper-chaotic system. Later in 2018, Ismail et al. [9] have also worked on logistic mapping, by proposing a double-humbled logistic map that is used to generate a pseudo-random number key. They have claimed that this approach should enhance the control of the chaotic range of the map. Similarly, a simple chaotic system has been proposed by Liu et al. in the same year [10]. In their system, they used hyperbolic sine to provide nonlinearity. The performance of the system has been enhanced by the usage of decorrelation operation. It has been proved that the medical images that were encrypted using this system needed only one round to be encrypted effectively. Also, in 2019, Kumar et al. [11] have also used the chaotic maps. Their proposed scheme was to apply the coefficients of the fractional discrete cosine transform on the medical image, then apply the chaotic maps on these coefficients.

Apart from using chaotic mapping, Laiphrakpam and Khumanthem [12] have proposed an encryption algorithm for medical images based on the state-of-the-art algorithm ElGamal. They have removed the part of encoding the image into Elliptic curve coordinates and found that their technique has resulted in a strong cipher image in a considerably less executable time. As for Cao et al. [13] they have proposed an encryption algorithm based on deriving the edge maps from the plain image. Starting with the decomposition of the bit-plane, then generating of random sequence, and finally applying permutation. They have argued that their cryptosystem has provided flexibility in the image type, the bit-plane decomposition approach, and the usage of several permutation methods. The system keys are generated using the plain image, edge detector, and the arguments of the scrambling algorithm. This made their system secure against bruit-force attacks. In the same context, Hua et al. [14], proposed an encryption scheme based on scrambling the pixels of the plain medical image. They have started their approach by adding random noise around the image, then scrambling the image pixels twice to provide diffusion. This scrambling step should shuffle the neighboring pixels and distribute the added noise around the image. For diffusion purposes, two main operations were performed, XOR and modulo arithmetic, which enhanced the security level and speed of encryption.

On the other hand, a hybrid encryption scheme has been proposed by Nematzadeh et al. [15], using Genetic Algorithms and coupled map lattices. Their approach starts with generating a population of secured cipher images and then using the genetic algorithm to select the best ciphers according to a fitness function that combines both minimal loss and minimal computational time. It has been argued that because of using such a hybrid system the cipher images should be secure from traditional attacks. Likewise, Fofanah and Gao [16] have proposed another type of encryption algorithm for medical images. They have proposed two watermarking schemes. The first scheme is based on the combination of two transforms discrete cosine and discrete wavelet. The second scheme is based on genetic programming. Both schemes have achieved better performance than the state-of-the-art watermarking techniques.

In 2021, encryption of medical images has continued to be a common topic in research. Starting with Deb and Bhuyan [17] who have proposed an encryption system based on the linear feedback shift register (LFSR). They have created a nonlinear filter based on linear feedback shift register (LFSR) and used it as a Pseudo-Random Number Generator (PRNG) [18]. Their approach starts with randomizing the medical image and then scrambling it, using a Logistic-Tent map and Arnold transformation approach, respectively. The resulting images are then XORed with a sequence generated by PRNG to achieve the encryption. This operation should provide a high level of randomness in the cipher image. Adithya et al. [19] have also used LFSR to control the scrambling of pixels in medical images, along with Modified Logistic Maps (MLM). While LFSR has been found efficient in medical encryption by [17,19]. Nevertheless, the non-linear feedback shift register (NLFSR) is more resistant to several types of attacks. Trivium [20] is considered an NLFSR and is used in the proposed model to provide more resistance to such attacks.

Also, Masood et al. [21] have proposed a cryptosystem to preserve the privacy of medical images that consists of several steps. They have used images of size 512 × 512 and divided each image into 4096 blocks of size 8 × 8. They have used the Henon chaotic map (HCM) to apply confusion by shuffling pixels in each block. Then Brownian motion has been applied to generate particles in three directions. One of them is selected and multiplied with the result of HCM and then XORed with Chen's chaotic system result. By evaluating the performance of their system using several evaluation measures, such as NIST, Entropy, MSE, PSNR, and time complexity were used and proved the efficiency of the proposed systems in both security and time-wise. Their results have been compared with the results of the proposed encryption scheme. Guesmi and Farah [22] have proposed a hybrid cryptosystem of medical images that consists of using SHA-2 as a hash algorithm, to generate the encryption key. Then confusion is applied using DNA operations and diffusion is achieved by chaotic maps generated using the keys resulting from the hash algorithm. An XOR operation is applied in the final step to apply the final encryption and produce the cipher image. They have argued that their work increases the security of the encrypted medical images against statistical attacks and the encryption efficiency is enhanced.

Moreover, Barik and Changder [23] have proposed a complex cryptosystem with two phases of encryption. In the first phase, they apply an extension of DNA code, namely the Amino acid codon. The resulting image is then split into a certain number of blocks. Logistic maps are used to create chaotic confusion. Then a random number is generated from a random ASCII character seed, which is encrypted using the RSA algorithm. Then a circular shifting is applied on each block and XORed using a sequence of tent maps, as the second phase. Extra security is added by encrypting all resulting keys in both phases using the AES algorithm. They have tested their approach using several analysis techniques, such as correlation analysis, resistance to noise and bruit-force attacks, and others, and proved that their approach performance has outperformed previously proposed methods. Comparably, Mishra et al. [24] also proposed a cryptosystem of medical images that uses DNA cryptography. They increase the randomness of the image by a masking phase that proceeds with the actual encryption. For confusion, the proposed algorithm uses Arnold's Cat Map. As for diffusion, it uses 2D-logistic sine coupling map values along with DNA code and XOR operation. They argued that their algorithm is secured against statistical and brute force attacks. Key rotation is a recommended practice in encryption algorithms to enhance security. Also, several researchers have used this technique within images encryption algorithms, such as [25] who applied key rotation in the key generation phase and resulted in a more secured cryptosystem. Thus, this technique has been used in the proposed work. In addition, the authors of [26] have used a new technique for splitting images (color and gry-scale) into blocks. After performing some transformations to these blocks, a chaotic logistic map has been used to generate a key to defuse the image. Their results showed the effectiveness of their proposed algorithm using PSNR, histogram, entropy, and other evaluation metrics. However, all their test images were the size of 256 × 256, which is considered to be small for medical images.

Furthermore, several other research contributions were presented to improve the mutual information (MI) measures such as in [27] who proposed an MI measure for input variable selection (IVS) and incorporated it into optimized support vector regression (SVR) for the displacement prediction of seepage-driven landslides. Finally, our work makes use of several security modules (such as ECDH, AES, DSA, Merkle tree, and others) to provide high-security standards and ensure the privacy of patients' information against undesired access. Our system aims at providing a robust medical image cryptosystem with computational overhead. To sum up, Table 1 presents a summary of surveyed papers throughout this study.

Table 1. Summary of papers reviewed in Related Work Section.

Ref./Year	Model	Advantage	Limitations
[7] 2015	Crypto-based algorithm to encrypt DICOM images	Employment of whirlpool Hash function, providing authentication and confidentiality.	Very time consuming algorithms
[8] 2017	Adaptive encryption algorithm based on enhanced choetic mapping	- Easy to apply; - Large key space; - Secured against chosen plain text attack.	- Tested only on a picture of size 256 × 256, which is considered a small size compared to real medical images - They have presented an example of a typical image, not a medical one

Table 1. *Cont.*

Ref./Year	Model	Advantage	Limitations
[9] 2018	Double-humbed logistic map key generation	- Enhance the control on chaotic range of the map - Secure communication transfer - Secured against noise attacks	Tested on images of different sizes but do not exceed 1024 × 1024
[10] 2018	A simple chaotic system with hyperbolic sine	- Large key space - Entropy around 8 - Secured against known plaintext, ciphertext, statistical, differential and brute force attacks.	Tested on images of size 512 × 512 only
[11] 2019	Chaotic maps with fractional discrete cosine transform coeficients	- Five keys are used to encrypt the image - Secure against brute force attacks	- Entropy of encrypted image is 4.7453, which is low compared to the proposed system - Large key space; - The minimum time needed for encryption is 0.15946 s, which is slower than the time needed to encrypt images of the same size in the proposed system
[12] 2017	Improvement of ElGamal encryption by removement of encoding phase before encryption	Applied experiments on grey-scale and colored images	- Tested on images of different sizes but do not exceep 1024 × 1024 - Encryption time ranges between 0.093750 s to 1.718750 s
[13] 2017	Encryption algorithm based on edge maps	- Secured against brute force attacks - Secured against chosen cipher attacks	- Tested on images of sizes 256 × 256 and 512 × 512 only - Encryption time ranges between 0.0129 s to 1.846 s
[14] 2018	MIE-MA: High speed scrambling and pixel adaptive diffusion	- Reduces correlation between adjacent pixels - Secured against chosen-plaintext and differential attacks	- Tested on images of different sizes but do not exceed 1024 × 1024 - Encryption time ranges between 0.1043 s to 0.1057 s for images of size 512 × 512
[15] 2018	Hybrid model of Genetic Algorithm and coupled map lattices	Secured against brute force attack because of the large key space	- Tested on images of size 256 × 256 only - Execution time reaches 2.135 s
[16] 2020	Dual Watermarking scheme	- Secured against several types of attacks - Better performance when compared to other watermarking schemes	Tested on images of size 256 × 256 and 512 × 512
[17] 2021	Chaois-based encryption using LFSR	- Provides high level of randomness in the cipher image - Entropy of cipher images are close to 8 - Secured against brute force and known plaintext attacks	- Tested on images of size 256 × 256 and 512 × 512 - Encryption time for images of size 512 × 512 is 1.105 s, which is low compared with the proposed model.
[19] 2021	Chaois blend LFSR	Provides concurrent encryption	Tested on images of size 256 × 256 only
[21] 2021	lightweight chaos-based medical image encryption	- Secured against differential attacks - Cipher entropy is close to 8	- Tested on images of size 512 × 512 only - Execution time: 1.53 s, which is high considering small sized images

Table 1. *Cont.*

Ref./Year	Model	Advantage	Limitations
[22] 2021	Hybrid chaotic map and DNA code	- Secured against several typical attacks, such as chosen plaintext and chosen ciphertext attacks. - Entropy close to 8	Tested on images of sizes 256 × 256 and 512 × 512 only
[23] 2021	amino acid codon based scheme with multiple chaotic maps	- Based on RSA encryption - Extra security layer is added by encrypting the keys using AES. - Secured against noise and brute force attacks	- Tested on several sizes of images 256 × 256, 512 × 512 and 1024 × 1024. Larger sized images are not tested.
[24] 2021	bit-level diffusion with DNA coding	- Adding a masking phase before the encryption to increase randomness - Secured against statistical and brute force attacks	- Tested on small-sized images (256 × 256 and 512 × 512)
[26] 2021	Gray and colored image encryption technique	- Logistic map is used to generate the key - Encryption entropy is very close to 8	Tested on small-sized images (256 × 256)

3. MID-Crypt Algorithm

MID-Crypt Algorithm is a comprehensive cryptosystem that can be used to provide security services for the medical images communicated over insecure channels such as the internet. The following subsections discuss the subsystems (modules) of MID-Crypt.

3.1. Key Management System (KMS)

The proposed algorithm uses a multi-key process in medical image encryption to establish secure transmission. The **Public key Module (PKM)** module manages a shared secret value (SSV) between the laboratory and patients' doctors' accounts. The key management system starts with generating standard parameters of ECDHE. Doctors start the connection by sending their public keys to LAB, which generates a private value used in ECDHE to generate SSV. The same thing happens on the LAB side, where the LAB sends its public key to the doctors, generating the SSV using ECDHE. See Figure 1 which illustrate the PKM module.

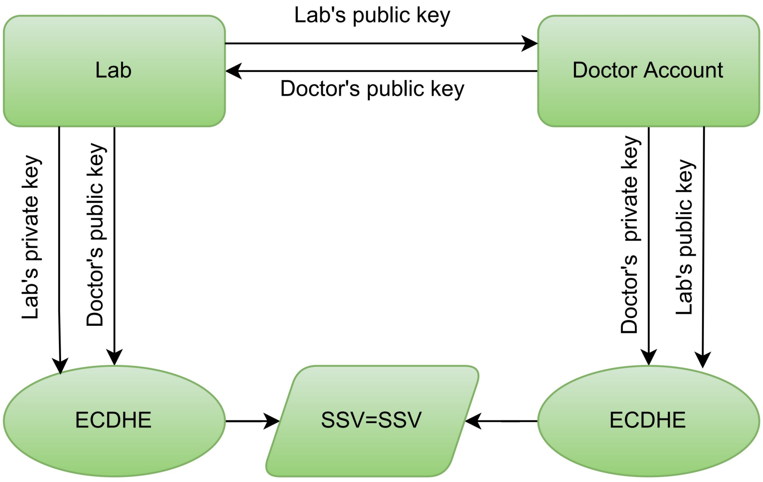


Figure 1. Public key Module.

Several modules are collaborating to fulfill the functionalities of this subsystem. Specifically, our KMS consists of four main modules: Encryption-Keys Module (EKM), Key Rotation Module (KRM), Key Agreement Module (KAM), and Patient PIN Module (PPM). **Encryption-Keys Module (EKM)**: All encryption keys used to encrypt MI, i.e., the AES input keys, will be derived using the hash key derivation function HKDF. Figure 2 illustrates the EKM module.

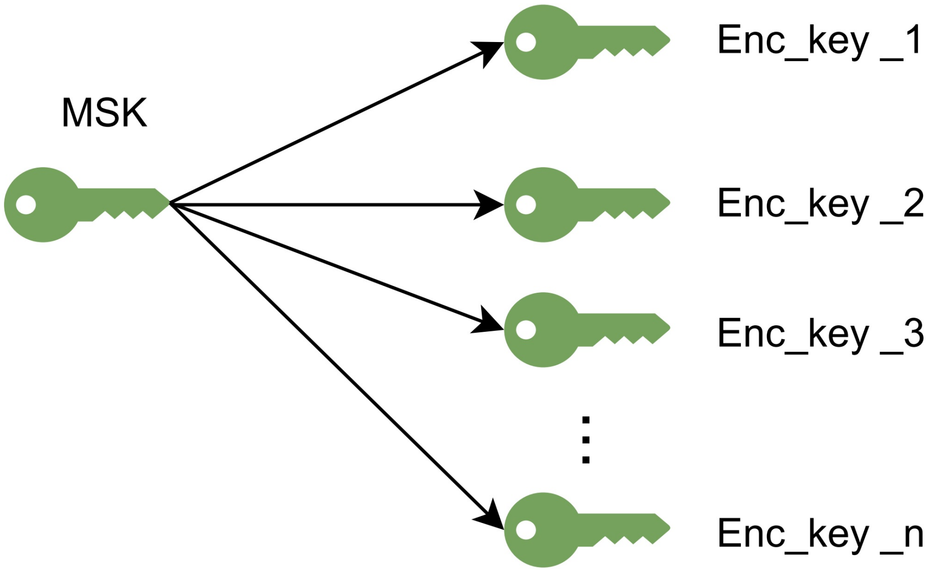


Figure 2. Encryption-Keys Module.

Key Rotation Module (KRM): The process of generating and updating master keys (MSK) is done by using SSV as a seed and the previous MSK. Using KRM reduces the number of bytes encrypted with encryption-key so that the amount of material leaked by one key compromise is less. Periodically and automatically rotating keys is a recommended security practice. For some industry standards, such as Payment Card Industry Data Security Standard (PCI DSS), key rotation is required [28,29]. In the proposed work, MSK and SSV were used to generate EKM. Therefore, the rotating formula we used is:

$$MSK_n = Hash(Hash(MSK_{n-1})||SSV) \tag{1}$$

where $MSK_0 = Hash(Hash(PIN)||SSV)$, and PIN is a secret value entered by patient. The rotation scheduler can be based on either the key's age, the number or volume of messages encrypted with a key version. In the proposed work, the key rotation period is fixed for every visit.

Key Agreement Module (KAM): The agreement on the encryption keys' values was done simply by using *tag* that AES-GCM offered. In the proposed work, there are many keys used in the MI encryption. Therefore, the encryption-keys agreements take place for every MI. Authentication tag of AES-GCM will contain keyed-hash message authentication code:

$$HMAC(K, R) = Hash(K||Hash(K||R)) \tag{2}$$

where, K is encryption-key and R is the patient info saved in the MI header. Figure 3 represents the key agreement module.

Patient PIN Module (PPM): Receives the PIN value for each patient to be used for signing, verifying, and encrypting MI. In addition, the initialization of the first MSK MSK_0 is done by using this PIN. In this work PPM value is derived by key derivation function from the received PIN value, such as SHA-512-based crypt ('sha512crypt'). See Figure 4.

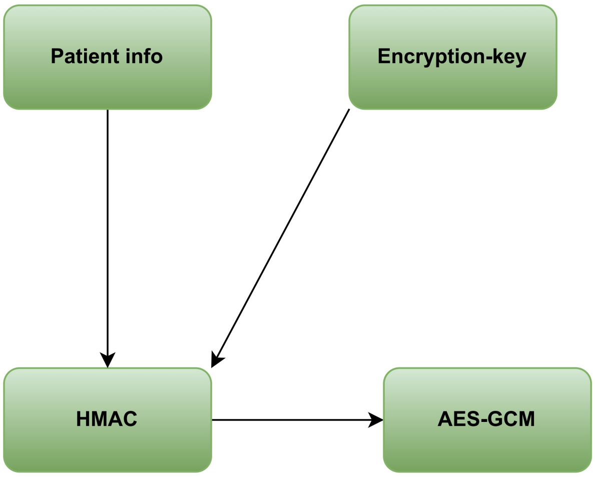


Figure 3. Key Agreement Module.

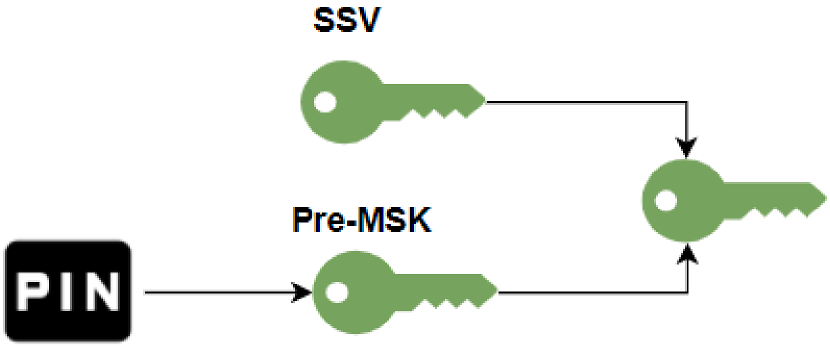


Figure 4. Patient PIN Module.

3.2. Proposed Medical Image Encryption Technique

The proposed algorithm is presented in Figure 5. The algorithm requires reading the image bytes. The Trivium used the EKM to generate the Trivium keystream, a randomly generated 10 Bytes used through the image masking process. As mentioned in related work, the researcher used LFSR for MI encryption. On the other hand, Trivium is lightweight and NLFSR. NLFSRs are known to be more resistant to cryptanalytic attacks than Linear Feedback Shift Registers (LFSRs). Moreover, Trivium security is based on the resistance of attacks such as Correlations, Period, Guess and Determine attacks, Algebraic attacks, and Resynchronization attacks [30]. Furthermore, in the proposed algorithm, the next process after masking is block ciphering using AES-GCM for the masking result, increasing security level, and providing auth tag used in KAM. The proposed algorithm can be further detailed in the following steps.

The encryption keys of EKM were used to generate a trivium cipher, as Trivium was used to create a random key-stream consisting of 32 bytes. Then the image bytes were masked using the xor process; the xor process was applied between the first 32 bytes of the image and the generated trivium cipher, the result of the xor process was then XORed with the next 32 bytes of the image, and so on until the xor passed all over the image. Figure 6 illustrates the masking process. MI masking here can be described as a diffusion process applied on the image where any minor change in the Trivium cipher would be reflected as a notable change in the result. On the other hand, bit-wise xor operation between the image and the Trivium cipher provides high means of efficiency in the case of hardware platform [5]. Image masking can be considered a first layer encryption operation followed by a block ciphering step, which produces the same bytes quantity as in the same image. Figure 7a represents the original image, and Figure 7b illustrates the output of the image masking process.

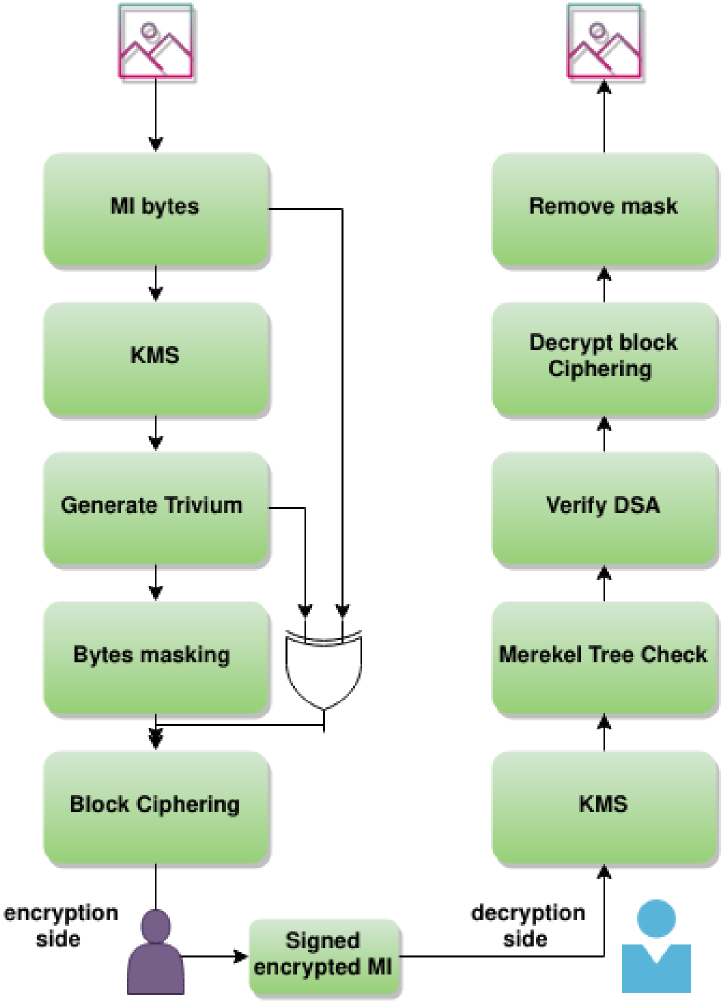


Figure 5. The proposed Algorithm.

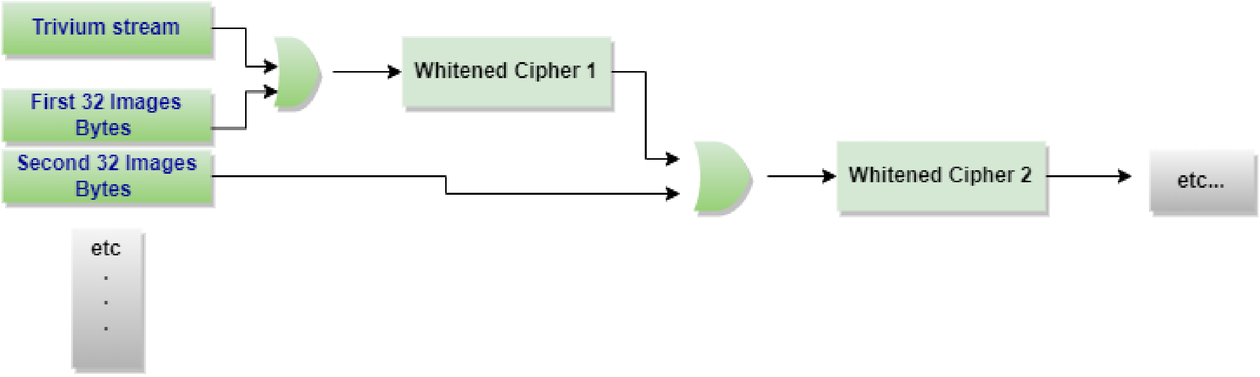


Figure 6. Image masking process.

The second encryption layer used is Block Cipher the cipher generated from the masking process can be described as an encrypted form of the image. Yet the encryption process goes on to the next step to add more distortion to the image and security. EKM generated a total number of 256 secret keys. The 256 secret keys were used to encrypt the masked image using the AES-GCM encryption scheme. The first 256 bytes of the masked image were encrypted using the generated 256 secret keys, and the process was repeated on the next 256 bytes till all the image bytes were encrypted using the secret keys. After encrypting the fundus image in Figure 7a, the output is shown in Figure 7c.

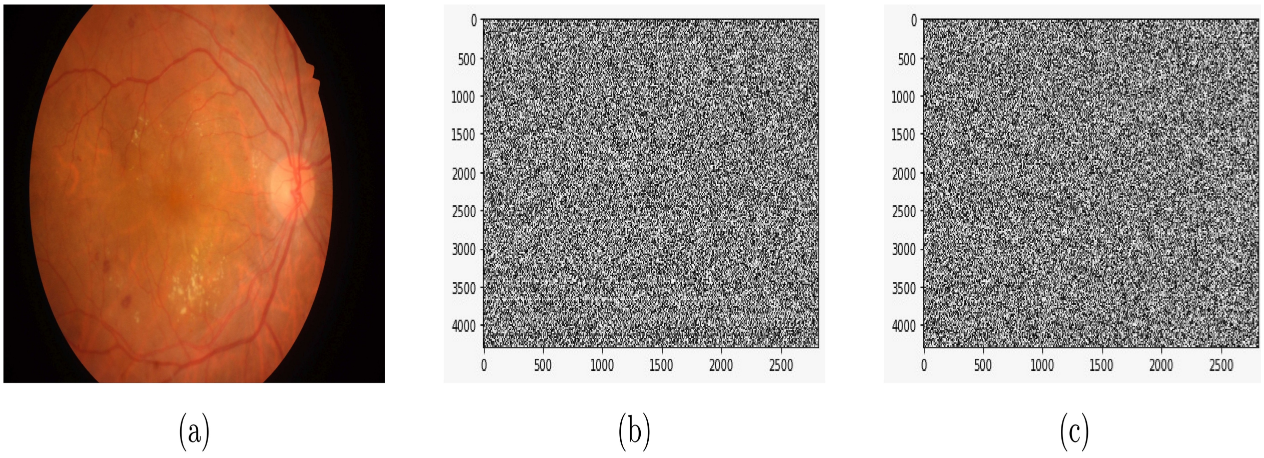


Figure 7. Image encryption steps: (**a**) Original Image, (**b**) The AES-GCM mask image, and (**c**) The encrypted image.

3.3. Data Integrity of Proposed Encrypted MI

Checksum data integrity used in proposed work based on Merkel tree hashes. Merkel Tree is considered a tree of hashes, where the leaf nodes are the hashes of the data blocks. Merkle tree was used to preserve the image integrity, where the receiver can ensure that the image has not been corrupt or damaged. Each leaf contains the hash of a data block with 256 bytes from the original image. The hash function used in the Merkle tree was SHA256. Figure 8 illustrates the Merkel tree hash performed on the image. The resulted Merkel tree has 17 levels according to the following formula:

$$\#levels = \log_2 a/b + 1 \tag{3}$$

where a is the number of bytes in the original image, and b is the data block size.

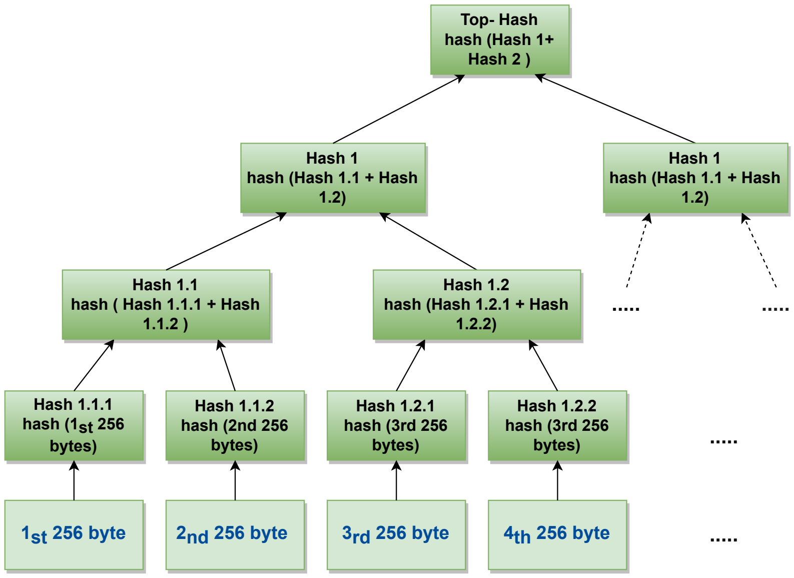


Figure 8. Merkle Tree.

3.4. Digital Signature Algorithm (DSA)

In this context, DSA aims to prove the patient's ID. Theoretically, the medical image is processed using the algorithm proposed in this study and should be signed using the patient's associated MSK and PPM. Only the Merkel tree's root part will be encrypted using the DSA algorithm to reduce generated cipher. DSA is considered an asymmetric encryption scheme.

We only share public keys over the channel, which reduces jeopardy when the key is revealed over malicious communication channels compared to traditional symmetric watermarking methods. The DSA algorithm used here is "El-Gamal" described in Figure 9.

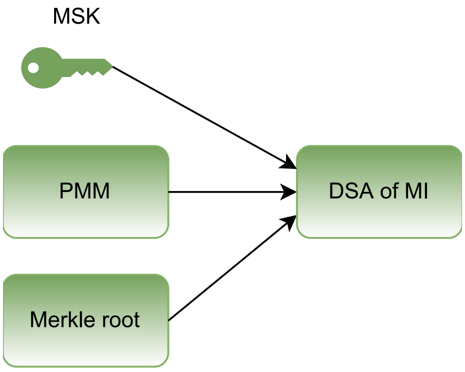


Figure 9. The proposed digital signature.

3.5. Doctor Side Decryption Process

So far, all the techniques and algorithms mentioned will only be applied to the encryption side of the lab in the hospital, where the image is generated and prepared to be shared with high privacy and security standard. In Figure 5 the decryption process is shown on the right-side part, which goes upwards. Following are the detail of all decryption steps:

- Checksum
  As mentioned before, the Merkle tree was used to ensure the integrity and check if the image has been corrupted or damaged through the communication channel. After decrypting the image, the receiver can build the Merkle tree of the decrypted image; if the root of the resultant tree is the same as the one received, then the image has not been corrupted. Otherwise, the receiver can locate where the damage occurred by comparing the hashes of each level with the received Merkle tree and then ask for a specific portion of the image to be sent again if needed.
- Verify DSA
  DSA verification is first applied at the receiver side as an authenticity procedure. In this step, the algorithm ensures that only verified people access the encrypted image. This step is also required to confirm the patient's ID on the decryption side. Failing this step will not allow the next steps to be processed either.
- Block Deciphering
  By using the shared key, the receiver can derive the same 256 keys used in the encryption process. After retrieving the keys, each row in the encrypted image was decrypted with its corresponding key. In other words, the first 256 rows in the encrypted image will be decrypted using the first 256 derived key then the process will be repeated until retrieving all rows in the encrypted image. The image resulting from the decryption process will be the same as the masking image.
- Unmasking
  After decrypting the image, the process of removing the masking started by using the shared key to generate the same Trivium used in masking the image. By reversing the XOR process, the original image was retrieved. The first xor process was applied between the first 32 bytes of the encrypted image and the generated trivium cipher. Then the resulting XORed bytes were XORed again with the next 32 bytes until the original image was retrieved.

4. Performance and Comparison Analysis

The experiments were conducted using the Google Co-Lab platform based on Python-3. Google Co-Lab offers 12 GB RAM and 128 GB Disk.

Performance analysis for the Proposed algorithm was conducted on many levels. Confidentiality was ensured by measuring the level of dissimilarity between original and encrypted images, entropy analysis, histogram analysis, and time analysis. Performance measurements are presented using three images that are listed in Table 2.

Table 2. The Images Used through Result Analysis.

Image ID	Type	Size (Pixels)
Images 1	Fundus Image	4288 × 2816
Images 2	Chest X-ray	1000 × 800
Images 3	Brain CT	512 × 512

The first measurement considered is the dissimilarity analysis. Encryption algorithms designed to work on medical images are demanded to produce a highly distorted image compared to the original image. Visual measurement is considered important, while we need to prove and measure dissimilarity between original and ciphered images mathematically. In this study, we use Peak signal-to-noise ratio (PSNR) measurements and correlation measurements to measure the dissimilarities degree between original and encrypted images. PSNR can be described as the ratio between the maximum possible power of an image and the power of the noise being applied to the image. In our study, the higher the PSNR value, the more the distortion is, which indicates good performance. Figure 10 below shows an example of an original and encrypted image presented with the PSNR value related. A PSNR value of 7.8006 can be considered relatively high. Correlation analysis measures how adjacent pixels in original and encrypted images are alike—The less the correlation factor, the better the results. In Table 3 we present the PSNR and correlation analysis for the three images listed in Table 1.

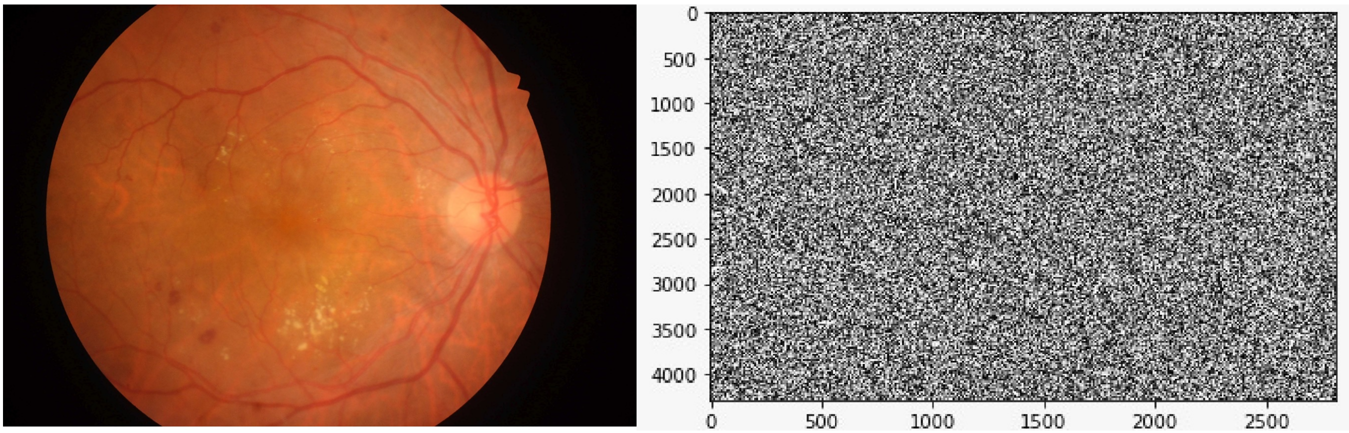


Figure 10. PSNR value = 7.8006, Correlation value = 0.0012.

Table 3. PSNR and Correlation Analysis.

Image ID	PSNR	Correlation
Images 1	7.8006	0.0012
Images 2	5.9605	0.0029
Images 3	7.1009	0.0071

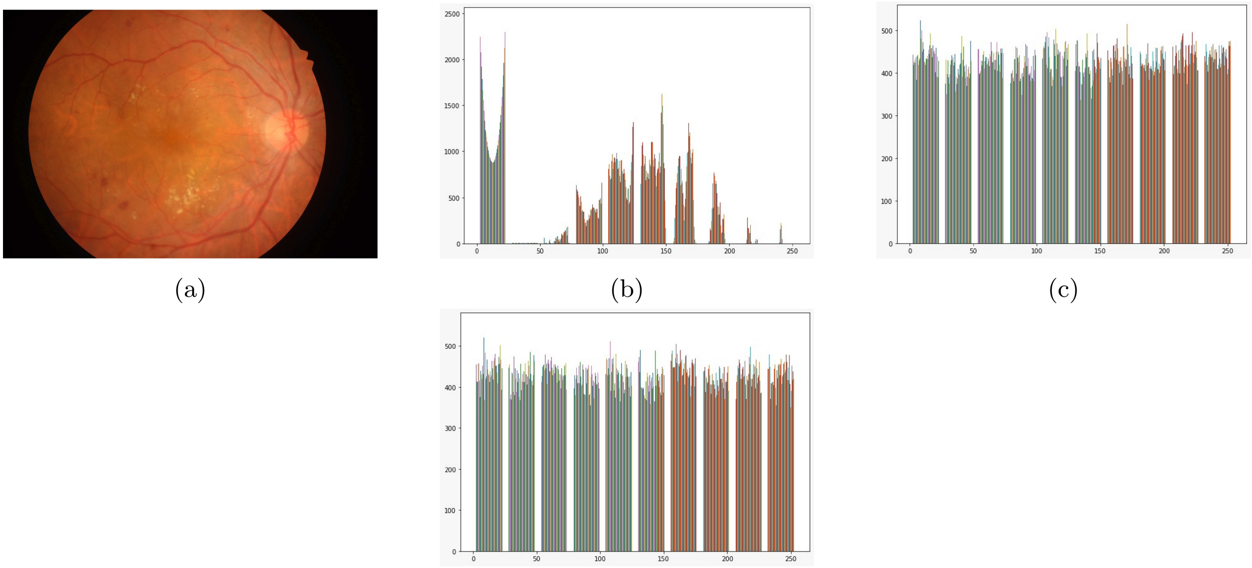
The second measurement is entropy analysis. Entropy analysis is another way to measure the algorithm's performance in hiding the details of the original image, and it is measured in bits per pixel. A high entropy value means more randomness in the image and high confidentiality measures for the algorithm. The maximum possible value for entropy is eight. We have measured image 1 used in this study; the other two encrypted images gave excellent entropy values indicating that the original image cannot be visually extracted from the encrypted image. Table 4 presents the results of entropy analysis.

Table 4. Entropy Analysis.

Image ID	Original Image Entropy	Encrypted Image Entropy
Images 1	6.5625	8
Images 2	7.5515	7.9998
Images 3	3.0867	7.9903

The third measurement is Histogram Analysis. An image histogram is a visual representation of gray levels distribution in the image. Every gray level is represented by the total number of pixels with that grey level. A histogram plot can directly reflect the tonal distribution of the image by just looking at it. For example, Figure 11a represents the original image. At the same time, Figure 11b illustrates the image histogram. Figure 11a shows that the image colors are biased towards dark grey levels; Figure 11b shows that dark gray levels with values closer to zero appeared more frequently in the image. Figure 11c shows the histogram for the XORed image with the Trivium, while Figure 11d shows the histogram for the encrypted image. The difference between the plain image and the encrypted image histograms indicates a low correlation between the two images. While the almost even distribution for ciphered image histogram means that not much information can be concluded from the image.

The fourth Measurement is Time Analysis. The time execution is detailed for image 1 in Table 1, with 4288 × 2816 pixels. Figure 12 illustrates the time execution for each step in the proposed model. The execution time for XORing the image with Trivium was 2.702 s, whereas the time execution for encrypting the resultant XORed image was 3.337 s. The decryption process took only 1.419 s. It can be noticed the reversed xor and reconstructing the image took the longest time, which is 4.152 s. The overall process took 11.61 s. The encryption time required to encrypt the images mentioned in Table 1 is listed in Table 5. According to the information listed in Table 1, the proposed algorithm can be considered a lightweight and practical algorithm that can be used with large high-resolution images without worrying about time.



(a) (b) (c)

(d)

Figure 11. Histogram graph. (**a**) Original Image, (**b**) image histogram, (**c**) Histogram for the XORed image with the Trivium, and (**d**) Histogram for the encrypted image.

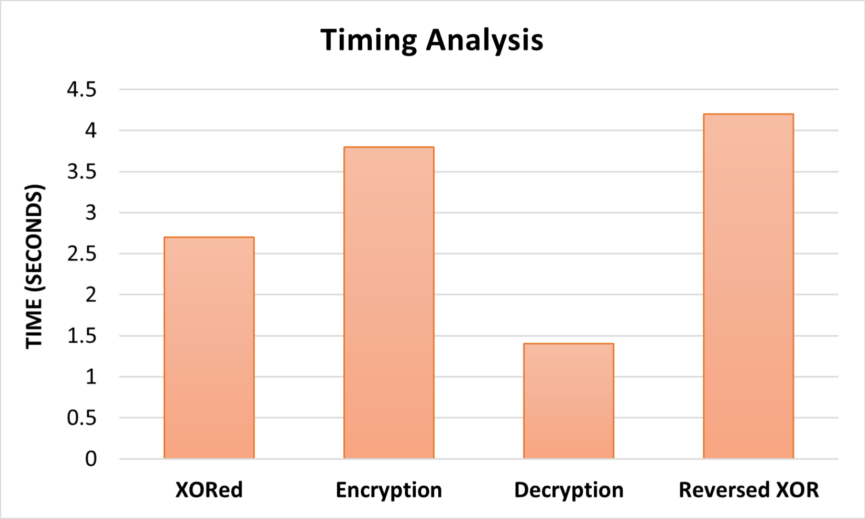


Figure 12. Time analysis on the proposed model.

Table 5. Timing Analysis.

Image ID	Encryption Time
Images 1	6.039 s
Images 2	220.46 ms
Images 3	72.0887 ms

Finally, we compare this work with other studies. The proposed algorithm can be considered simple and easy to mimic compared to other studies. While for the results we have generated, the comparison is listed in Table 6. The PSNR values we have generated are within the same range as other studies and are considered satisfying. The entropy values for encrypted images reflect highly visually distorted images. Encryption time is another comparison aspect that can distinguish practical algorithms. Obviously, the proposed algorithm requires less than one second to encrypt image 2 and image 3, while for image 1 it too around 6 s for encryption; we should take into consideration the size of image 1, mentioned in Table 1.

Table 6. Comparison With Other Studies.

Study	PSNR	Entropy	Time
Proposed, image 1	7.8006	8	6.039 s
Proposed, image 2	7.1009	7.9998	220.46 ms
Proposed, image 3	5.9605	7.9501	72.0887 ms
Ref. [21]	7.74	7.9993	1.53 s

5. Security Discussion

The proposed model is a hybrid cryptosystem composed of symmetric key encryption using (AES) and asymmetric key encryption using Elliptic Curves (EC). Both components are prone to side-channel attacks [31]. However, masking the data with trivium cipher before implementing AES ought to increase the security level. This increase is done by preventing side-channel attacks such as differential power analysis (DPA). Such masking algorithms are discussed in [32–35] and used to protect AES against DPA.

SCA for EC private exponent multiplication is a serious concern according to [36,37]. In our proposed cryptosystem, Key exchange is resistant to DPA because we use The Montgomery powering ladder [38].

Moreover, In MID-crypt we overcome one of the most weaknesses of a public-key system which is a Man-in-the-Middle attack (MITM). Generally, this attack scenario can be described as replacing the value of SSV with SSV′. The difficulty of generating MSK is knowing the PIN value, which is only used by the patient for encryption and decryption. Furthermore, PPM will provide identification of crypto principles.

Additionally, MID-Crypt KRM-module will reduce the number of encrypted data with an encryption key. Hence, the amount of data leaked by one key compromise has become less. This means that most popular attacks which need a large amount of data, such as known "plain text" and "algebraic" would fail with MID-Crypt.

Nowadays, the blockchain concept has spread to many fields and is implemented in many applications. Generally, enhancing security and privacy issues can be addressed on blockchain, anonymizing personal data and storing all authorized transactions. In MID-Crypto we do not use this mechanism utterly, but from Equation (1), we use key chaining, to connect all transmitted images of one patient together. Therefore, the proposed methodology can be applied to other fields requiring an extra flavor of security provided by cryptography. Table 7 shows that the proposed MIT-Crypto can stand against four famous possible attacks. Compared to other studies MIT-Crypto has shown distinguishable security measures since it is the only system covering SCA and MITM attacks.

Table 7. Security Measures Compared with Other Systems.

System	SCA	Differential Attacks	MITM	Algebraic Attacks
MID-Crypto	Yes	Yes	Yes	Yes
8	-	Yes	No, since symmetric	No
10	No	Yes	No	No
19	-	Yes	No, since symmetric	No
20	-	Good	No, since symmetric	Yes

The limitation we recognized on the MID-Crypto protocol is that the MID-Crypto stores MI inside the user profile, this limits the medical consulting between doctors. KMM and ENC need many calculations, therefore MID-Crypto cannot consider lightweight or used with most IoT applications. Handling privacy in MID-Crypto requires us to distribute MI with owners only, which causes distributed data set of having many MIs in one place.

6. Conclusions

This paper has proposed, developed, and investigated a new encryption algorithm for medical images, MID-Crypt. MID-Crypt provides three security services for medical images: confidentiality, integrity, and authenticity. Confidentiality is achieved through the steps shown in Figure 1: image bytes masking and block ciphering. Integrity is achieved through the Merkel tree algorithm, which ensures that the image content was not changed either by a malicious third party or accidentally via noisy transmission channels. While DSA is used to provide authenticity means, only users who have permission to view the image's content will be able to view and access the image. The DSA algorithm aims to confirm patients' IDs as well. We have provided mathematical and visual evidence to guarantee security and privacy issues. Initially, MID-Crypt generates a Trivium cipher for image masking by applying an XOR operation between the image and the Trivium cipher. After that, the masked image ID is digitally signed by the DSA algorithm. Merkel tree checks and the DSA process are added to guarantee integrity and authenticity. Moreover, the PSNR of values can be considered sufficient to destroy the visual characteristics of encrypted images. As for the correlation factor between the original and encrypted image, the correlation between the two images is low, indicating high distortion of the encrypted image. Finally, the entropy analysis provides an excellent value approaching the eight. The efficiency measurements performed in this study have shown high protection and security standards, considering the algorithm's simplicity and time efficiency. Therefore, MID-Crypt can be adopted as a good candidate to be deployed through the healthcare applications to provide security solutions in a comparable processing time. In the future, we will consider the use of multi-authentication factors to provide further security levels to private data. Also, we will seek to maintain multi-layer protection for the medical image data to improve the overall system confidentiality. Moreover, we will also attempt to adopt AI-driven techniques to automate the protection process and provide a more autonomous nature in the key management and distribution stages.

Author Contributions: Conceptualization, A.A. and Y.A. (Yousef AbuHour); methodology, A.A. and R.Y.; software, A.A. and R.Y.; validation, Y.A. (Yousef AbuHour), Y.A. (Yasmeen Alslman) and E.A.; formal analysis, Y.A. (Yousef AbuHour), Q.A.A.-H.; investigation, A.A., E.A. and Q.A.A.-H.; resources, A.A., R.Y. and E.A.; data curation, A.A., Y.A. (Yousef AbuHour) and Y.A. (Yasmeen Alslman); writing original draft preparation, A.A., Y.A. (Yousef AbuHour), R.Y., Y.A. (Yasmeen Alslman), E.A. and Q.A.A.-H.; writing review and editing, A.A., Y.A. (Yousef AbuHour), R.Y., Y.A. (Yasmeen Alslman), E.A. and Q.A.A.-H.; visualization, Y.A. (Yousef AbuHour), Y.A. (Yasmeen Alslman), E.A. and Q.A.A.-H.; supervision, A.A. and Y.A. (Yousef AbuHour); funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Electronic Health Solutions. 2022. Available online: https://ehs.com.jo/hakeem-program (accessed on 12 February 2022).
2. Anand, D.; Niranjan, U. Watermarking medical images with patient information. In Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society Vol. 20 Biomedical Engineering Towards the Year 2000 and Beyond (Cat. No. 98CH36286), Hong Kong, China, 1 November 1998; Volume 2, pp. 703–706.
3. Wang, J.Z.; Wiederhold, G. System for efficient and secure distribution of medical images on the Internet. In *Proceedings of the AMIA Symposium*; American Medical Informatics Association: Bethesda, MN, USA, 1998; p. 907.
4. Aslan, P.; Lee, B.; Kuo, R.; Babayan, R.K.; Kavoussi, L.R.; Pavlin, K.A.; Preminger, G.M. Secured medical imaging over the Internet. In *Medicine Meets Virtual Reality*; IOS Press: Amsterdam, The Netherlands, 1998; pp. 74–78.
5. Pavithra, V.; Jeyamala, C. A Survey on the Techniques of Medical Image Encryption. In Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 13–15 December 2018; pp. 1–8. [CrossRef]
6. Abu Al-Haija, Q.; Krichen, M.; Abu Elhaija, W. Machine-Learning-Based Darknet Traffic Detection System for IoT Applications. *Electronics* **2022**, *11*, 556. [CrossRef]
7. Al-Haj, A.; Abandah, G.; Hussein, N. Crypto-based algorithms for secured medical image transmission. *IET Inf. Secur.* **2015**, *9*, 365–373. [CrossRef]
8. Chen, X.; Hu, C.J. Adaptive medical image encryption algorithm based on multiple chaotic mapping. *Saudi J. Biol. Sci.* **2017**, *24*, 1821–1827. [CrossRef] [PubMed]
9. Ismail, S.M.; Said, L.A.; Radwan, A.G.; Madian, A.H.; Abu-Elyazeed, M.F. Generalized double-humped logistic map-based medical image encryption. *J. Adv. Res.* **2018**, *10*, 85–98. [CrossRef] [PubMed]
10. Liu, J.; Ma, Y.; Li, S.; Lian, J.; Zhang, X. A new simple chaotic system and its application in medical image encryption. *Multimed. Tools Appl.* **2018**, *77*, 22787–22808. [CrossRef]
11. Kumar, S.; Panna, B.; Jha, R.K. Medical image encryption using fractional discrete cosine transform with chaotic function. *Med. Biol. Eng. Comput.* **2019**, *57*, 2517–2533. [CrossRef]
12. Laiphrakpam, D.S.; Khumanthem, M.S. Medical image encryption based on improved ElGamal encryption technique. *Optik* **2017**, *147*, 88–102. [CrossRef]
13. Cao, W.; Zhou, Y.; Chen, C.P.; Xia, L. Medical image encryption using edge maps. *Signal Process.* **2017**, *132*, 96–109. [CrossRef]
14. Hua, Z.; Yi, S.; Zhou, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **2018**, *144*, 134–144. [CrossRef]
15. Nematzadeh, H.; Enayatifar, R.; Motameni, H.; Guimarães, F.G.; Coelho, V.N. Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. *Opt. Lasers Eng.* **2018**, *110*, 24–32. [CrossRef]
16. Fofanah, A.J.; Gao, T. Dual Watermarking for Protection of Medical Images based on Watermarking of Frequency Domain and Genetic Programming. In Proceedings of the 2020 the 4th International Conference on Innovation in Artificial Intelligence, Xiamen, China, 8–11 May 2020; pp. 106–115.
17. Deb, S.; Bhuyan, B. Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR. *Multimed. Tools Appl.* **2021**, *80*, 19803–19826. [CrossRef]
18. Abu Al-Haija, Q.; Jebril, N.A.; Al-Shuáibi, A. Implementing variable length Pseudo Random Number Generator (PRNG) with fixed high frequency (1.44 GHZ) via Vertix-7 FPGA family. *Netw. Secur. Commun. Eng.* **2015**, *1*, 105–108.

19. Adithya, N.; Nalajala, H.K.; Sivaraman, R.; Sridevi, A.; Rengarajan, A.; Rajagopalan, S. Chaos Blend LFSR—Duo Approach on FPGA for Medical Image Security. In *Emerging Technologies in Data Mining and Information Security*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 155–163.
20. Abu Al-Haija, Q.; Ibrahim, M.; Mohammad, M.A. A Double Stage Implementation for 1-K Pseudo RNG using LFSR and TRIVIUM. *J. Comput. Sci. Control Syst.* **2018**, *11*, 1–6.
21. Masood, F.; Driss, M.; Boulila, W.; Ahmad, J.; Rehman, S.U.; Jan, S.U.; Qayyum, A.; Buchanan, W.J. A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. In *Wireless Personal Communications*; Springer: Berlin, Germany, 2021; pp. 1–28.
22. Guesmi, R.; Farah, M. A new efficient medical image cipher based on hybrid chaotic map and DNA code. *Multimed. Tools Appl.* **2021**, *80*, 1925–1944. [CrossRef]
23. Barik, R.C.; Changder, S. A novel and efficient amino acid codon based medical image encryption scheme colligating multiple chaotic maps. *Multimed. Tools Appl.* **2021**, *80*, 10723–10760. [CrossRef]
24. Mishra, P.; Bhaya, C.; Pal, A.K.; Singh, A.K. A medical image cryptosystem using bit-level diffusion with DNA coding. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–22. doi: 10.1007/s12652-021-03410-7. [CrossRef]
25. Parikibandla, S.; Alluri, S. Low area field-programmable gate array implementation of PRESENT image encryption with key rotation and substitution. *ETRI J.* **2021**, *43*, 1113–1129. [CrossRef]
26. Kamal, S.T.; Hosny, K.M.; Elgindy, T.M.; Darwish, M.M.; Fouda, M.M. A new image encryption algorithm for grey and color medical images. *IEEE Access* **2021**, *9*, 37855–37865. [CrossRef]
27. Ma, J.; Wang, Y.; Niu, X.; Jiang, S.; Liu, Z. A comparative study of mutual information-based input variable selection strategies for the displacement prediction of seepage-driven landslides using optimized support vector regression. *Stoch. Env. Res. Risk. Assess.* **2022**, 1–21. [CrossRef]
28. Rotating Keys, Cloud kms Documentation, Google Cloud 2022. 2022. Available online: https://cloud.google.com/kms/docs/key-rotation (accessed on 3 March 2022).
29. Rotating AWS KMS keys-AWS Key Management Service. Available online: https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html (accessed on 3 March 2022).
30. Cannière, C.D.; Preneel, B. Trivium. In *New Stream Cipher Designs*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 244–266.
31. Chen, S.; Wang, R.; Wang, X.; Zhang, K. Side-channel leaks in web applications: A reality today, a challenge tomorrow. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 191–206.
32. Oswald, E.; Mangard, S.; Pramstaller, N.; Rijmen, V. A side-channel analysis resistant description of the AES S-box. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 413–423.
33. Renauld, M.; Standaert, F.X.; Veyrat-Charvillon, N. Algebraic side-channel attacks on the AES: Why time also matters in DPA. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 97–111.
34. Bogdanov, A. Improved side-channel collision attacks on AES. In *International Workshop on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 84–95.
35. Neve, M.; Seifert, J.P.; Wang, Z. A refined look at Bernstein's AES side-channel analysis. In Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, Taipei, Taiwan, 21–24 March 2006; p. 369.
36. Chevallier-Mames, B.; Ciet, M.; Joye, M. Low-cost solutions for preventing simple side-channel analysis: Side-channel atomicity. *IEEE Trans. Comput.* **2004**, *53*, 760–768. [CrossRef]
37. Izu, T.; Takagi, T. A fast parallel Elliptic curve multiplication resistant against side channel attacks. In *International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 280–296.
38. Joye, M.; Yen, S.M. The Montgomery powering ladder. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 291–302.