Security Analysis of Medical Image Encryption using AES Modes for IoMT Systems

Zied Guitouni
Electronics & Microelectronics Laboratory, Faculty of Sciences of Monastir, Tunisia

Mohammed Ali Ghaieb
Higher Institute of Computer Science and Multimedia of Gabes, Tunisia

Mohsen Machhout
Electronics & Microelectronics Laboratory, Faculty of Sciences of Monastir, Tunisia

ABSTRACT
The Internet of Medical Things (IoMT) driven health is the most advantageous aspect of technology in the global healthcare industry. Securing medical images in IoMT systems is a great challenge to protecting medical privacy. Many cryptographic schemes that provide the confidentiality and integrity of these images over IoMT devices are proposed. The Advanced Encryption Standard (AES), is one of the most standards used in digital image security systems, it employs five encryption modes. In this paper, the security analysis of medical images encryption was described for IoMT Systems using the AES modes. For the evaluation and analysis of security performance, several tests were employed such as the quality of the encrypted images, the Peak Signal to Noise Ratio (PSNR), the histogram analysis, the correlation between the adjacent pixels, and the encryption/decryption times for the five modes.

Keywords
IoMT, AES, AES modes, image encryption, images analysis.

1. INTRODUCTION
The Internet of Medical Things (IoMT) is an ecosystem of connected sensors, wearable devices, medical devices, and clinical systems. It enables various healthcare applications to provide timely medical responses, reduce healthcare costs, and increase the quality of medical treatment.

The IoMT has become a strategic priority for future e-healthcare because of its ability to improve patient care and its scope to provide more reliable clinical data, increase efficiency and reduce costs [1].

Most hospitals and health centers use IoMT for the exchange of medical images, the security of these images cannot be granted to the patient's personality within these institutions. Therefore, securing medical images in IoMT systems is a great challenge for the protection of medical privacy.

The most basic step in securing IoMT begins with obtaining trusted visibility and classification of all IoMT devices across hospital networks, data centers, cloud environments, mobile assets, remote clinics and endpoints. By doing this, healthcare IT teams will be empowered to take a prevention-first instead of an alert-only approach to keeping medical devices safe from potential threats.

Various methods have been developed and studied to protect the data and privacy of patients. Encryption is one of the best ways to secure IoMT networks, to protect valuable information from unwanted readers.

For security reasons, there is a need for an encryption scheme that can easily encrypt biomedical data and it can be shared with other centers via the Internet without and privacy concerns.

Advanced Encryption Standard (AES) is one of the most widely used algorithms for encrypting digital images. It consumes little memory space, is less complicated, easier to implement, very fast, and has never been broken until today. It has five operations modes.

This work presents a security analysis of the AES operations modes in medical image encryption and decryption, a comparative study between these modes is conducted to select the most appropriate operating mode for IoMT applications.

This research is divided into the following sections: Section 2 provides an insight into IoMT and the related work, Section 3 describes the details of the AES algorithm and these modes, section 4 gives the implementation details of medical image encryption in IoMT systems and the security analysis, while section 5 concludes the paper.

2. IoMT AND RELATED WORK

2.1 IoMT
With the development of the Internet of Things (IoT) technologies, the IoMT adopts these technologies in the domain of medicine. It is an interdisciplinary filed, and many medical imaging types of equipment are widely connected and used to facilitate the process of treating and diagnosing for doctors, e.g., the computed tomography scan (CT), magnetic resonance imaging (MRI), ultrasound, and nuclear medicine imaging.

The medical images in IoMT are managed by a Picture Archiving and Communication System (PACS) [2]. When a patient is scanned by the medical imaging equipment, the generated medical images will be first stored in the PACS. When the doctor begins to examine the patient, the PACS will retrieve the needed images from the database and transfer the images in an intranet environment to the doctor’s workstation which works with the patient information from the Hospital Information System (HIS). The HIS modules are described in Figure. 1.

IoMT systems pose a risk to each other regarding integrity, confidentiality, and data availability. Information security in the storage, transfer, and review of medical images in these systems is a great challenge for sensitive patient privacy information protection. Encryption is one of the best schemes to secure IoMT systems. In the next subsection, insight into the related work in medical image encryption is described.

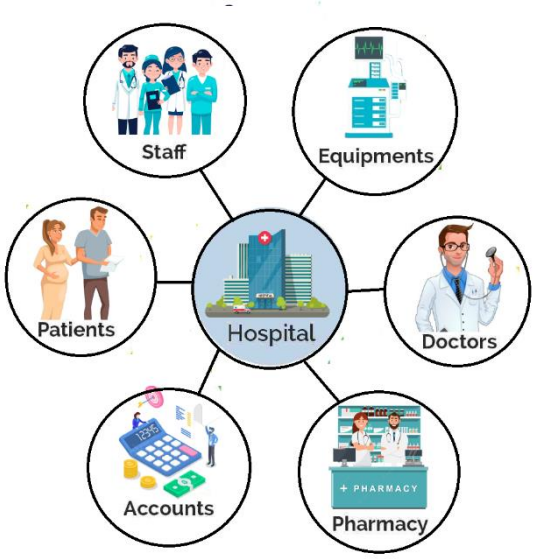


Fig 1: Hospital Information System

2.2 RELATED WORK

The protection of medical images has attracted a lot of attention lately, especially when these images are sent over unsecured networks. An image encryption method attempts to transform one image into another image that is difficult to achieve. The security mechanisms deployed in current methods of handling digital health images are mainly based on traditional encryption methods such as DES, AES, IDEA and RSA [3].

Mitra et al. [4] proposed a method for encrypting images using several random permutation approaches. This work describes a simple-to-implement yet effective solution for image encryption. The results of this work indicate that the combined method achieves the advantages of all the individual permutation techniques and overcomes the limitations of these methods.

Dai et al. proposed in [5] a chaotic picture encryption approach based on bit-plane decomposition The encrypted image is first split into an eight-bitmap, with the top four bits accounting for a significant amount of plain text. As a result, Arnold permutation on the high four-bit is used to correlate the time of permutation with the image order. After then, the scrambled images are combined to form a new scrambled image, which is then discussed.

In [6], H. Nematzadeh et al. proposed a medical image encryption method based on a hybrid model of the modified genetic algorithm (MGA) and coupled map lattices. First, the proposed method employs coupled map lattice to generate the number of secure cipher-images as initial population of MGA. Next, it applies the MGA to both increase the entropy of the cipher-images and decrease the algorithm computational time. Experimental results and computer simulations both indicate that the proposed method that includes a hybrid algorithm not only performs excellent encryption but also is able to resist to various typical attacks.

Çavuşoğlu et al. [7] developed a secure image encryption algorithm based on a new chaos-based RNG and S-BOX structure. A new S-Box design algorithm is developed to create the chaos based S-Box to be utilized in encryption algorithm and performance tests are made. According to tests results, the proposed algorithm is secure and speed for image encryption application.

Hongjun et. al. [8] have proposed an asymmetric program for the encryption and decryption of color pathological pictures according to the Dadras chaotic system. The system seems to have received great sensitivity to the key used and also a key size big enough to fight the brute force attack.

In [9], N. K. Pareek proposed a similar work to [8], the medical image encryption algorithm dependent on confusion and also diffusion operation carried out by using Arnold's transformation and 2 chaotic methods.

M. Mukhedkar [10] described an image encryption method using Blowfish Algorithm due to its excellent delivery and execution time. To provide substantial protection, a hybrid approach continues to be recommended that use a combination of image encryption plus image encryption plus image hiding.

In [11] Tauhid, A et. al, proposed a new method has been proposed which combines cryptography and steganography to ensure even more secure communication. The proposed method has two levels of security, it is a combination of both AES Cryptographic and DCT Steganographic methods which have proved to improve data security as well as the data secrecy. Using spatial domain to modify the images may cause suspicion to attackers due to its additive noise on the cover image.

3. ADVANCED ENCRYPTION STANDARD (AES)

In this work, we have used the symmetrical algorithm AES for the security analysis of medical image encryption in IoMT Systems. This section describes the details of the AES algorithm and these modes.

3.1 AES Algorithm

The Advanced Encryption Standard (AES) is a cryptographic symmetrical algorithm published by the National Institute of standard and Technology (NIST) in December 2001. The AES is a Non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It supports three different cryptographic keys of 128, 192, and 256 bits (16, 24 and 32 bytes). The cipher consists of specific rounds, where the number of rounds depends upon key length: 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key.
The AES algorithm works on 4 * 4 matrixes of bytes. It consists of four transformations: SubBytes, Shift Rows, MixColumns and AddRoundKey [11]. These transformations are reversible; it is easy to prove that decryption does recover the plain text or image. AES achieves a safer and more secure encryption scheme and higher encryption speed than other cryptographic algorithms [11]. In this work, we will study the performances analysis of medical image encryption using AES 128. The algorithm is described in figure. 2.
The AES rounds are governed by the following transformations:

- **SubBytes Transformation**: Is a nonlinear byte substitution, each byte in this round is replaced with reference to the bytes present in the lookup table.
- **ShiftRows transformation**: This is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.
- **MibColumns transformation**: This is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.
- **AddRoundkey transformation**: Is a simple XOR between the working state and the round key.

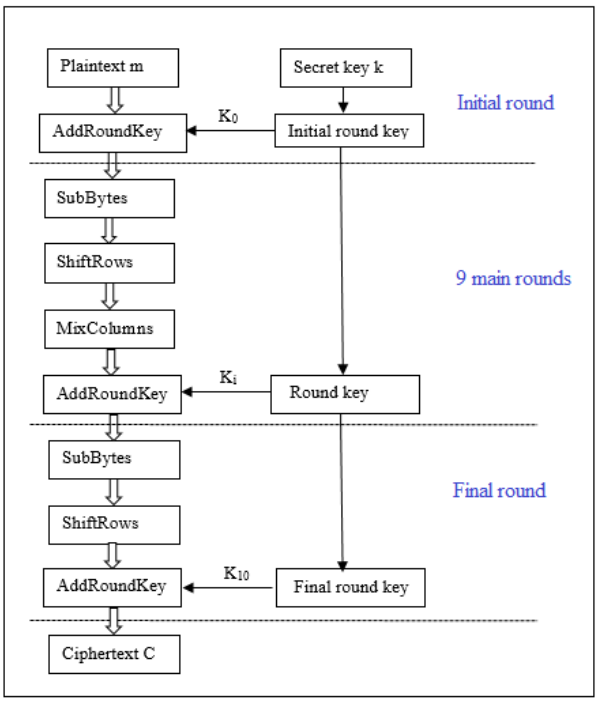


Fig 2: AES128 algorithm

3.2 AES Modes

AES algorithm has five modes of operation namely: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher FeedBack (CFB), Output FeedBack (OFB), and Counter (CTR) [12]. In this Sub-section, that will be described.

A. Electronic Code Book (ECB)

In the ECB mode, the plaintext is divided into blocks of 128 bits and padding is needed when the size of the message is not a multiple of the block size. It is the simpler and faster operational mode. As showed in Figure in Figure. 3, each block is encrypted with the same key, which in the case of existing two equal blocks, the result of the cipher text will be reflected [12].

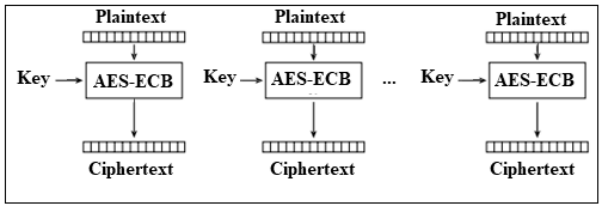


Fig 3: ECB encryption mode

B. Cipher Block Chaining (CBC)

The CBC mode implements a chain system based on a random number (initialization vector: IV). In the first interaction, the IV is used in an XOR operation ( ) with the plaintext, and the product of this operation that is subsequently encrypted with the key. The result of the encryption is used as an input of the next interaction for the XOR operation with the next plaintext block [12]. This mode is represented in give figure. 4.

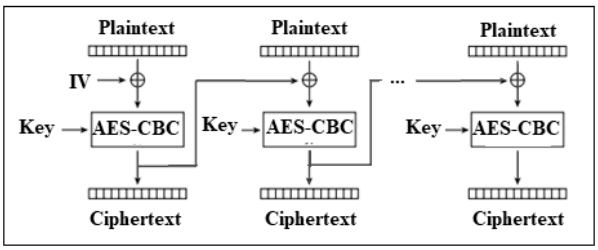


Figure 4. CBC encryption mode

C. Counter (CTR)

The CTR is a simple mode, shown in figure. 5, it creates a flow of pseudo-random numbers independent of the plain text. In this mode, the key flow is obtained by encrypting successive values of a counter (T) which is then exorited with a block of the message in clear to generate a block of the encrypted message [13].

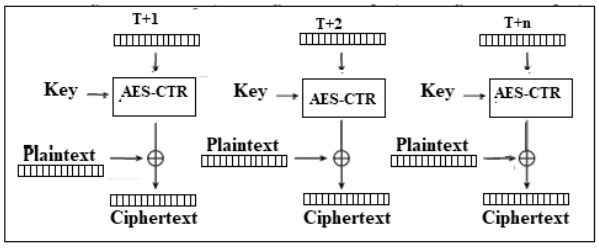


Fig 5: CBC encryption mode

D. Cipher FeedBack (CFB)

CFB mode implements a chain system based on an initialization vector (IV). In the first interaction, the encryption is performed by using an IV and an encryption key, and the result of this operation is used for an XOR operation with the plaintext block [12]. The scheme of this mode is given in figure. 6.

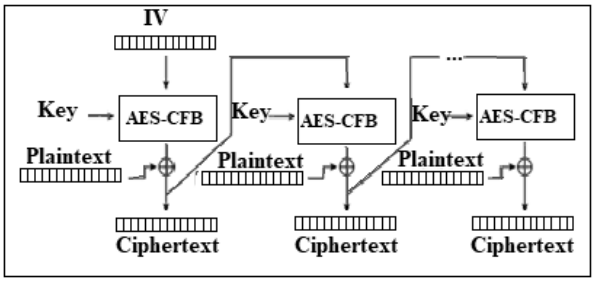


Fig 6: CFB encryption mode

E. Output Feedback (OFB)

The OFB mode has a similar operation to the previous mode CFB, it differs in the fact of carrying out successive encryptions to the initialization vector (IV) in each interaction. As shown in figure. 7.

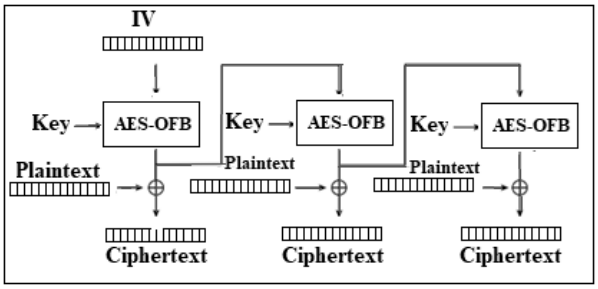


Fig 7: OFB encryption mode

4. IMAGE ENCRYPTION IN IoMT SYSTEMS

This section describes the proposed architecture design of the IoMT system and the security analysis of the AES modes for medical image encryption/ decryption.

4.1 Architecture of IoMT security

The proposed architecture for IoMT security using the AES algorithm is shown in Figure 8.

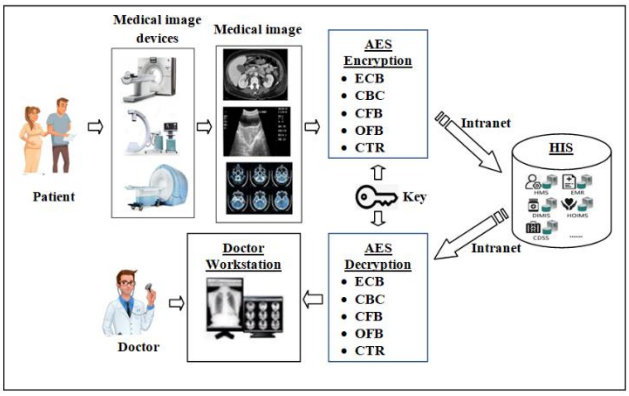


Fig 8: IoMT security architecture

The architecture consists of the following modules:

- Medical image acquisition: there are different types of medical imaging procedures, including X-ray, ultrasound, magnetic resonance imaging (MRI), touch imaging.....
- Encryption module: After acquisition, the original medical image is encrypted with the AES128 algorithm using one of five operating modes (ECB, CBC, CFB, OFB and CTR mode).
- The PACS retrieves the required images from the database and transfers them in an intranet environment to the physician's workstation, which works with the patient information from the HIS.
- The decryption module: the encrypted image will be decrypted each time by AES128 in one of five modes

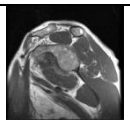
4.2 Security analysis

Several test metrics are employed to analyze the security performance of medical image encryption in IoMT systems. These metrics are based on the analysis of histograms of the encrypted images, the correlation between the adjacent pixels, the entropy of the encrypted image, and the PSNR between the original image and the decrypted one. Moreover, we exploit the analysis of encryption and decryption times for the five modes of the AES algorithm. In these metrics, we chose three tests images known as “ShoulderCR” image (1162 pixels x 684), “MR” image (512 pixels x 513) and “Ultrasound” image (895 pixels x 597).

4.2.1. Histograms of encrypted images

The proposed architecture for IoMT security using the AES algorithm is described using a python programming language. The simulation results of the ciphered images for the fives modes are shown in table 1.

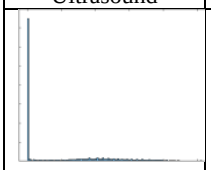
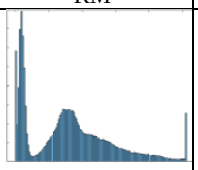
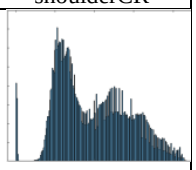
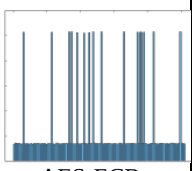
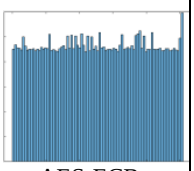
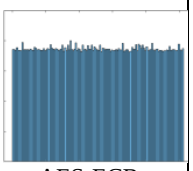
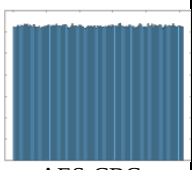
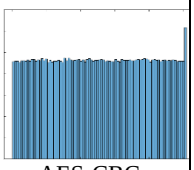
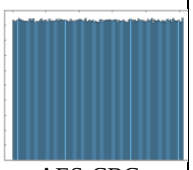
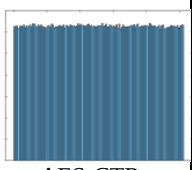
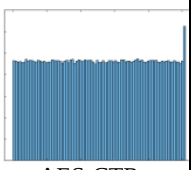
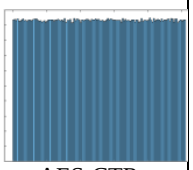
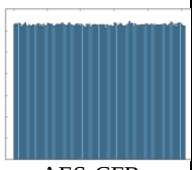
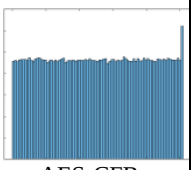
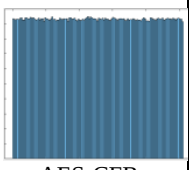
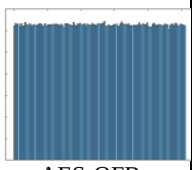
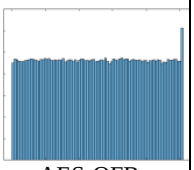
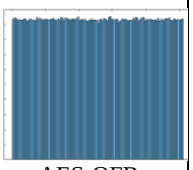
Table 1. Ciphered images with AES modes

Medical Images		
Ultrasound	RM	shoulderCR
		
Ciphered Images		
 AES-ECB	 AES-ECB	 AES-ECB
 AES-CBC	 AES-CBC	 AES-CBC
 AES-CTR	 AES-CTR	 AES-CTR
 AES-CFB	 AES-CFB	 AES-CFB
 AES-OFB	 AES-OFB	 AES-OFB

As expected, the ECB ciphered image still bears some resemblance to the original (Ultrasound), but the other modes appear simply as random data, with no trace of the original image. We calculated the histograms of the tree image for the five modes. The results are shown in table2.

According to table. 2,We can see that the histogram of the ciphered image with ECB mode is nonuniform. But, the histogram of the ciphered image with the other modes is fairly uniform and is significantly different from that of the ECB ciphered image. Therefore, it does not provide any indication of employing any statistical attack on the image under consideration. Moreover, there is no loss of image quality after performing the encryption/ decryption steps for the five modes.

Table 2. Histograms of encrypted images

Histograms of Medical Images		
Ultrasound	RM	shoulderCR
		
Histograms of Ciphered Images		
 AES-ECB	 AES-ECB	 AES-ECB
 AES-CBC	 AES-CBC	 AES-CBC
 AES-CTR	 AES-CTR	 AES-CTR
 AES-CFB	 AES-CFB	 AES-CFB
 AES-OFB	 AES-OFB	 AES-OFB

4.2.2. Correlation of two adjacent pixels

We tested the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in three ciphered images. First, we randomly selected n pairs of two adjacent pixels from an image. Then, we calculated the correlation coefficient of each pair by using the following formula.

$$Cov(x,y) = E((x - E(x))(y - E(y))). \quad (1)$$

Where x and y are grey-scale values of two adjacent pixels in the ciphered image. Table 3, present the variation of the correlation values of two horizontal (H) and vertical (V) adjacent pixels in function of the different modes

Table 3. Correlation coefficients of ciphered images

AES MODE	Correlation Coefficients					
	Ultrasound		RM		shoulderCR	
	V	H	V	H	V	H
ECB	0.154	0.372	0.041	0.028	0.154	0.370
CBC	0.031	0.016	0.033	0.019	0.031	0.016
CTR	0.032	0.015	0.035	0.020	0.032	0.016
CFB	0.032	0.015	0.033	0.021	0.032	0.015
OFB	0.032	0.015	0.034	0.019	0.032	0.015

In figure 9, we present the arithmetic average of the horizontal and vertical correlation for the different modes.

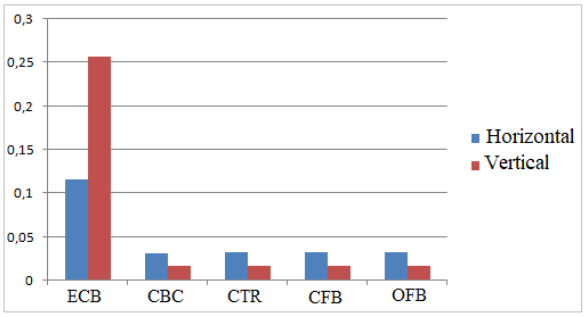


Fig 9: Arithmetic average correlation

According to figure 9, we can see that the arithmetic average of the correlation of two vertically adjacent pixels is about 0.116 for the ECB encrypted images, and the arithmetic average of the correlation of two horizontally adjacent pixels is about 0.256. There are the highest values compared with others modes. For the CBC, CTR, CFB, and OFB are low values of the correlation about 0.032 for the vertical adjacent pixels and 0.017 for the horizontal adjacent pixels.

4.2.3. Information entropy test

The information entropy expresses the uniform distribution of the pixel value. For a random image, the ideal entropy should be equal to 8. Therefore, the ideal information entropy of an encrypted image should be in the order of 8, which proves that the information is completely random and confirms the robustness of the proposed encryption algorithm.

The information entropy H(s) of a message source s can be calculated as:

$$H(s) = \sum_{i=0}^{2^N-1} p(s_i) log_2 \frac{1}{p(s_i)} \quad (2)$$

Where p(si) represents the probability of symbol si. In Table 4, the entropy variation for the three images with different AES modes has been presented, which reveals that the encrypted images in all cases reached an entropy value closer to the expected theoretical value of 8 except for the ultrasound image with the ECB modes the entropy value is about 6.78.

Table 4. Information entropy variation

AES MODE	Entropy Variation		
	Ultrasound	RM	shoulderCR
AES-ECB	7.9311	7.9236	6.7870
AES-CBC	7.9316	7.9297	7.9320
AES-CTR	7.9320	7.9305	7.9320
AES-CFB	7.9323	7.9324	7.9344
AES-OFB	7.9315	7.9305	7.9299

4.2.4. PSNR test

The Peak Signal-to-Noise Ratio (PSNR) represents the ratio between the original image and the encrypted image. The higher value of the PSNR, the closer the encrypted image is to the original. In general, a higher PSNR value should correlate to a higher-quality image. For a good encryption scheme, the PSNR should be as low as possible [15]. Table 5 shows, the PSNR variation for the three images with different AES modes.

Table 5. PSNR variation

AES MODE	PSNR Values		
	Ultrasound	RM	shoulderCR
AES-ECB	10.820	8.751	7.069
AES-CBC	10.817	8.801	7.362
AES-CTR	10.826	8.807	7.369
AES-CFB	10.819	8.803	7.359
AES-ECB	10.820	8.751	7.069

The low PSNR values, presented in Table 5 reflect the difficulty in retrieving the plain image from the cipher image, without the knowledge of secret key.

4.3 Encryption and decryption time

This subsection describes the evaluation and analysis of the encryption (E) and decryption (D) times for the different AES modes. Table 6 shows the average time required to encrypt and decrypt of the three medical images.

Table 6. Encryption and decryption times

AES MODE	Encryption and decryption time (s)					
	Ultrasound		RM		shoulderCR	
	E	D	E	D	E	D
ECB	0.015	0.031	0.015	0.031	0.031	0.124
CBC	0.015	0.046	0.031	0.078	0.015	0.046
CTR	0.031	0.031	0.015	0.031	0.031	0.046
CFB	0.218	0.218	0.110	0.174	0.312	0.374
OFB	0.031	0.046	0.015	0.031	0.031	0.046

According to Table 6, the CFB mode has a high encryption and decryption time for the different images, the average encryption time being about 213 s and the average decryption time about 253 s. The encryption/decryption times of the ECB, CBC, CTR, and OFB modes are very low.

5. CONCLUSIONS

In this study, a comparison of five encryption modes (ECB, CBC, OFB, CFB, and CTR) of the AES algorithm is conducted to select the most appropriate mode that best meets the safety requirements of medical images in IoMT applications. For the analysis of encrypted images, we assessed several metrics based on the analysis of histograms of the encrypted images, the correlation between the adjacent pixels, the entropy of the encrypted image, and the PSNR between the original image and the decrypted one. Moreover, we exploit the analysis of encryption and decryption times for the five modes. This paper demonstrates that the most favorable modes for the encryption of medical images are CBC, OFB, and CTR modes. The CFB mode has good test results but the encryption and decryption time is very high compared to the other modes.

6. REFERENCES

[1] R. Hireche, H. Mansouri and A. K. Pathan,"Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis", Journal of Cybersecurity an Privacy. 2022, 2, 640–661.

[2] B. Liu, H. Huang, “Picture archiving and communication systems and electronic medical records for the healthcare enterprise,” Biomedical Information Technology, Academic Press, pp. 105-164, 2020.

[3] Y. Wan, S. Gu, and B. Du, “A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding,” Entropy, vol. 22, no. 2. 2020.

[4] A. Mitra, Y. S. Rao, and S. Prasanna, “A new image encryption approach using combinational permutation techniques,” International Journal of Computer Science, vol. 1, no. 2, pp. 127-131, 2006.

[5] Y. Dai, H. Wang, and Y. Wang, “Chaotic medical image encryption algorithm based on bit-plane decomposition,” International Journal of Pattern Recognition and Artificial Intelligence, vol. 30, no. 4, p. 1657001, 2016.

[6] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, “Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices,” Optics and Lasers in Engineering, vol. 110, pp. 24-32, 2018.

[7] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, “Secure image encryption algorithm design using a novel chaos based S-Box,” Chaos, Solitons & Fractals, vol. 95, pp. 92-101, 2017.

[8] Hongjun Liu, A. Kadir, ” Asymmetric color image encryption scheme using 2D discrete-time map”, Signal processing journal, Volume 113, August 2015, Pages 104-112

[9] N. K. Pareek and V. Patidar, “Medical image protection using genetic algorithm operations,” Soft Comput., vol. 20, no. 2, pp. 763–772, 2016.

[10] M. Mukhedkar, P. Powar, and P. Gaikwad,” Secure non real time image encryption algorithm development using cryptography & steganography”, 2015 Annual IEEE India Conference (INDICON)

[11] Tauhid, A. , Tasnim, M. , Noor, S. , Faruqui, N. and Yousuf, M. (2019) A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform. Journal of Information Security, 10, 117-129.

[12] D. Aruna kumari M. Chandrika and B. Surekha Ratnam Bharadwaj,“Magnified Cipher Block Chaining Mode using DES to Ensure Data Security in Cloud Computing”, Indian Journal of Science and Technology, Vol 9,mar 2016.

[13] D. Blazhevski, A. Bozhinovski, B. Stojchevska, and V. Pachovski, “The 10 th Conference for Informatics and Information Technology (CIIT2013) MODES OF OPERATION OF THE AES ALGORITHM.” Accessed: Feb. 19, 2021.

[14] Stavroulakis, P., & Stamp. M, "Handbook of information and communication security, " Springer Science & Business Media, 2010.

[15] N. Set, S. Vijay, “Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique”, Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013).