Contribution to the Improvement of Cryptographic Protection Methods for Medical Images in DICOM Format through a Combination of Encryption Method

Maka Maka Ebenezer[1], Pauné Félix[2], Malong Yannick[3], Simo Ntso Pascal Junior[4], Nnemé Nnemé Léandre[5]
Department of Computer Engineering and Telecommunications,ENSPD,University of Douala[1,3,4]
Department of Computer Engineering,ENSET, University of Douala[2,5]

***Abstract*—This paper proposes a method for storing and securing medical images in DICOM format. Other methods offered affect the quality of the image. The solution proposed here is based on the AES256 algorithm in Galois/Counter Mode (GCM) which already integrates authentication and signature processes to ensure the integrity of the images manipulated. This solution is implemented by using the Phyton programming language under the DJANGO framework, libraries such as NUMPHY, PYDICOM, MYSQLCLIENT, and PYCRYPTODOME. The results obtained after experimental tests give us a good average encryption and decryption time. The difference in the mean value of time between encryption and decryption is quite small in view of the tests carried out. We obtain saving on storage space owing to the fact that the proposed solution directly stores the encrypted image. The manipulated image is not altered.**

Keywords*—Medical images; DICOM; advanced encryption standard (AES); GCM; authentication

I. Introduction

With the digital evolution, the consumption of intangible goods has significantly increased, resulting in the circulation of large amounts of data on computer networks, in particular on the internet. Distance communication between individuals is growing rapidly and this does not spare the professional field where documents and audio-visual flows are shared. This contributes to the development of services such as teleworking and telemedicine. In the health sector, according to [1], he indicates for example that multimedia Information and Communication Technology (ICT) are likely to provide doctors with decisive help in the search for a better quality of care. Then several other aspects of cybercrime can mar this help.

Questions relating to the protection of the data that is exchanged across the world are increasingly felt despite the security methods put in place. Whether it is Short Message Service (SMS), instant messaging (chat) or electronic messaging (email), this data must remain "Confidential", which means that only authorized people can consult it; "Integral because they must not undergo any modification by a third person other than the one having the authorization to do so and they must above all remain available. The particular case of the exchange of digital medical images which contain a great deal of information on patients and must imperatively be protected in order to guarantee medical secrecy regulated by Law. To provide solutions to this issue of digital medical images privacy, several protection methods have been developed to guarantee their Availability, Integrity and Confidentiality (AIC). Among these protection methods, cryptographic ones seem to be the most suitable.

In this paper, we will describe some methods of protecting medical images, and methods of storing medical images. We will propose a cryptography-based solution using a symmetric encryption algorithm combined with an authenticated encryption algorithm designed to provide both data integrity and authenticity, as well as confidentiality (Galois / Counter Mode). The proposed solution will thus improve the storage capacity of medical image backup systems. This will ensure the security of the medical image in Picture Archiving and Communication System (PACS) while ensuring the AIC criterion. We structure this paper into six sections. Section I introduces the methods of cryptographic protection. Section II gives the literature review on the protection of medical images. Section III describes the transmission of medical images. Section IV deals with securing medical image. Section V gives the methodology and results. Section VI concludes this work.

II. Protection of Medical Images

The protection of medical images is one of the top priority issues about digital image security. Several researchers have focused on work aimed at improving methods of securing the medical image. From the use of watermarking methods for shared medical images [2], in order to ensure the integrity and confidentiality of the data [3], through selective encryption [4] and the use of cryptography-based protection methods on the displacement of Red Green Blue (RGB) pixels [5], without forgetting the algorithms based on the encryption of flows with a function of nonlinear filtering [6].

The medical image has undergone very remarkable changes in recent years thanks to the development of physics. The medical image, by its nature, is supposed to carry a set of information on the patient. Many methods allowing the acquisition of medical images have emerged; for standard IT management of medical imaging data and to ensure interoperability between these different modalities, the DICOM standard has been adopted. DICOM stands for Digital Imaging and Communication in Medicine. The objective of the DICOM standard is to facilitate the transfer of medical images between machines from different manufacturers. It defines a file format for digital files created during medical imaging examinations as well as a data transmission protocol (based on TCP / IP) [7]. Several techniques are used to ensure the protection of medical images.

A. Cryptographic Protection

Cryptography is the first device to guarantee the security of electronic documents [8]. It allows sensitive information to be stored or transmitted over insecure networks (such as the Internet) so that it cannot be read by anyone other than the intended person. Data that can be read and understood without special measures is called clear text, and the process of hiding clear text so as to hide its substance is called encryption. The operation to recover the clear data from the encrypted data is called decryption. Encryption is usually done using an encryption key, while decryption also requires a decryption key. There are two types of keys, namely symmetric keys, that is to say keys used at the same time for encryption and decryption. This is referred to as symmetric encryption or secret key encryption; and asymmetric keys, which mean that the keys used for encryption and decryption are different, this is referred to as asymmetric encryption or public key encryption.

1) Symmetric key encryption or secret key cryptography: In this type of system, the same key is shared between the sender and the receiver to encrypt and decrypt information. The problem with this method resides in the secure distribution of the key to the recipient of the encrypted message. Several secret key encryption algorithms have emerged, these include the algorithms of continuous or stream cipher, which act on the clear text and on one bit at a time; block cipher algorithms, which operate on plain text in groups of bits called blocks. And of all these algorithms, according to [8] the most widely used symmetric encryption algorithm is AES. In order to secure the transfer of medical images, William Puech and Develay Morice jointly used the AES algorithm in stream mode and JPEG compression [4].

2) Asymmetric encryption or public key cryptography: Whitfield Diffie and Martin Hellman invented the concept of public key cryptography in 1976, with the aim of solving the key distribution problem posed by secret key cryptography. Numerous algorithms have emerged for this purpose, all based on sophisticated mathematical problems that are generally difficult to solve. In these algorithms, the encryption and decryption keys are distinct and cannot be deduced from each other. We can therefore make one of the two public while the other remains private. If the public key is used for encryption, anyone can encrypt a message which only the owner of the private key can decrypt. Some algorithms allow the private key to be used for encrii.

A hash function is a function that will calculate a unique fingerprint (or signature) from the data provided. A cryptographic hash function has some particular characteristics, unidirectional meaning being the most important of them. As a matter of fact, it is a function whose reverse is impossible to calculate, even by using a great computing power for a long period of time. The most famous according to [4] is Message Digest 5 (MD5) which is still widely used although in terms of security, it is recommended to upgrade to more robust versions because collision suites have been found; this function returns a 128-bit hash. The Secure Hash Algorithm 1 (SHA1) was the replacement function of MD5 because it produced 160-bit hashes with no possibility of finding collisions until 2004-2005, when attacks proved the possibility of generating collisions. Since that date it is no longer recommended to use the SHA1 function. But it is still widely used. We also have SHA256 and SHA512 which are two of the major standards in use today as there have been no attacks so far to detect security holes on these hash functions. They produce signatures of 256 bits and 512 bits, respectively.

B. Data Hiding

Data hiding refers to the insertion into a digital medium of a given quantity of secret binary information imperceptibly and more or less robust, depending on the intended application. The term "concealment" does not mean here that the information is visible but encoded, in this case it would be cryptography. Rather, it means that the presence of the information to be protected (called a useful message) is not perceptible because it is buried in other information (called a cover message). In the case of the protection of digital information, the useful message makes it possible to identify the owner of the cover message or its origin or to guarantee its integrity. Data concealment encompasses two techniques that are very similar to each other, but which do not have the same objectives or the same constraints. Depending on the context, a distinction is made between steganography where it must be impossible to distinguish whether the cover message contains a useful message or not. The most important constraint is then imperceptibility; and digital marking where the useful message is linked to the identity of the beneficiary of the cover document, and must therefore remain present even if the latter undergoes modifications. In this case the main constraint is then robustness [9].

1) Storage of medical images: The reception facilities for digital images are much more accessible in practical terms than those for analogue images [10]. Thanks to the digital storage of medical images, it is possible to comment, view and process them locally or remotely. Image archiving and communication systems PACS are set up for the management of medical images and their communication in the appropriate infrastructures. These systems include an archiving station for long-term storage of image data, and an examination station for displaying images based on received image data [11]. Depending on the needs of the institutions, the storage devices can be local as in the previous case or very often remote thanks to cloud-type infrastructures. In all cases, the short and long term security of the DICOM files for the studies provided from the imaging modalities must be guaranteed. A "study" consists of one or more series of images captured using an imaging modality.

III. Transmission of Medical Images

The medical image flow circulates between the source which constitutes the modality (scanner, OTP, CT, etc.) which allows the acquisition of the medical image or any other DICOM image source, then the backup server and archiving (PACS or other system) of imaging files and finally the radiologist's reading workstation.

The transmission of medical images must be done quickly, securely and reliably. This is done by ensuring that all data passing through the network is encrypted. In practice, a VPN / IPSec tunnel is built between the source and the recipient for the routing of data; thus, all transmissions are secure. It is also possible to transmit securely through the DICOM / TLS protocol provided by the DICOM standard, which has been used more and more in recent years; or on the web through SSL / TLS protocol.

As most modern modalities increasingly produce high quality images, this can impact the speed of data transmission which would be a problem for emergency requests. Compression methods are very often used to overcome this problem. DICOM supports lossy and lossless compression mechanisms, such as JPEG2000, RLE, and even JPEG-LS. Other techniques are used to overcome this problem such as parallel data transfer. However, the constant improvement of telecommunications networks and data networks makes it possible to solve this problem without any particular technique.

IV. Securing Medical Images

The deployment of PACS and electronic medical records requires to significantly increases the security of hospital and radiological information systems in order to ensure the protection of patient’s data. The security rules that govern this protection are based on three principles: confidentiality, reliability and availability [12].

Securing a DICOM file consists of four operations, namely: securing access to the file by defining access rights, securing the transmission of the file, digitally signing the file and securing the storage [13]. Assuming that a secure transmission has been established, we now need to ensure that stored medical images are protected and that processes and procedures are in place to ensure data security and availability only to authorized users. The proposed work fully contributes to the management of access control, digital signature and secure storage of files. It combines the Hash Message Authentication Code (HMAC), RSA and AES methods to ensure the confidentiality and integrity of images.

A. AES Algorithm

This algorithm was officially approved as a standard on December 6, 2001 [14]. It is a block cipher algorithm for encrypting a clear text consisting of 128 bits of data using a secret key consisting of 128,192 or 256 bits. Its operating principle consists in taking as input a block of 128 bits, the key being 128, 192 or 256 bits. The 128 input bits are "mixed" according to a previously defined table. These bytes are then placed in a 4x4 square matrix. Line items are rotated to the right. The increment for the rotation varies depending on the row number. A transformation is then applied to the matrix by an XOR with a key matrix. Finally, an XOR between the matrix and another matrix makes it possible to obtain an intermediate matrix. These different operations are repeated several times and define “one turn”. For a key of 128, 192 or 256, AES requires 10, 12 and 14 turns, respectively, depending on the size of the key.

B. Message Authentication Code

Better known by the acronym MAC, Message Authentication Code, these are cryptographic functions intended to verify the integrity of data and to authenticate its origin. These MACs work in a similar way as hash functions. They calculate from a message of arbitrary length a summary of fixed length (this summary is called a hash). But, unlike hash functions, this summary also depends on a secret key *K*.

A message authentication code is a function $h(M,K)$ where M is the message and K the key, which returns fixed-length text. The calculation of $h(M,K)$ must be done very quickly; and if we know examples of code calculated with the same key, say $h(M_1,K)$,…, $h(M_n,K)$ and if we have a new message M, but not the key K, we cannot calculate $h(M,K)$.

When communicating between individuals, MACs are used in the following way: a sender and recipient begin by agreeing on a secret key, through a secure channel. The sender, when he wants to send a message, calculates his MAC using the secret key, and jointly sends the message and his MAC code. On arrival, the recipient also calculates the MAC using its own secret, and compares it with the version sent. If the two coincide, he is sure of both who sent him the message and also that this message has not been modified. Otherwise, the integrity of the message is compromised.

C. RSA Algorithm

It is one of the most popular asymmetric encryption algorithms. Its principle is based on the problem of factoring large numbers. It is extremely difficult to set up a fast algorithm capable of finding two prime numbers whose product is a known number. This is even more difficult when the numbers used are very large. Suppose that an Entity A wishes to send a message to an Entity B. It makes a communication request to Entity B. The key creation step is the responsibility of Entity B. It does not intervene at each encryption because the keys can be reused. The first difficulty which encryption does not solve, is that Entity A is quite certain that the public key it holds is that of Entity B. The renewal of the keys only occurs if the private key is compromised, or as a precaution after a certain time (which can be counted in years). The principle of key creation is as follows:

1. *Choose p and q, two distinct prime numbers;*
2. calculate their product $n = p \times q$, called the encryption module;
3. calculate $\phi(n) = (p-1)(q-1)$ (it is the value of the indicatrix of Euler in n n);
4. choose a natural number e prime with $\varphi(n)$ and strictly less than $\varphi(n)$, called the encryption exponent;
5. calculate the natural number d, inverse of $e \equiv \varphi(n)$, and strictly less than φ(n), called the decryption exponent; d can be calculated efficiently by the extended Euclidean algorithm.

As e is prime with $\varphi(n)$, according to the Bachet-Bézout theorem there are two integers $d \text{ and } k$ such that $ed = 1 + k\varphi(n)$, that it to say that $ed \equiv 1[\varphi(n)]$ and e is actually invertible modulo $\varphi(n)$.

The pair (n, e) or (e, n)[15] is the public key of the encryption, while its private key is [16] the number d, knowing that the decryption operation requires only the private key d and the integer n, known to the public key (the private key is sometimes also defined as the pair (d, n)[15] or the triplet (p, q, d).

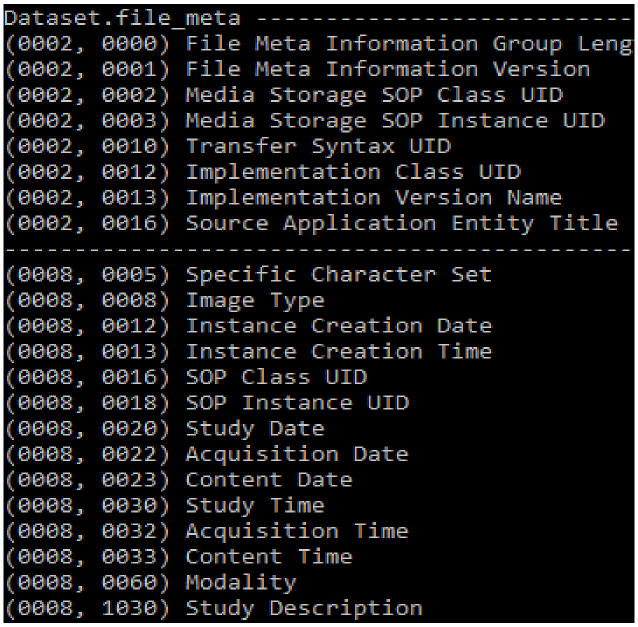
If M is a natural number strictly less than n representing a message, then the encrypted message will be represented by $M^e \equiv C[n]$ and the natural number C being chosen strictly less than n.

To decipher C, we use d, the inverse of $e \bmod (p-1)(q-1)$, and we find the plain message M by $M = C^d[n]$.

V. Methodology and Results

The solution implemented in this paper is based on a tool for sharing and archiving medical images. To carry out this work we used tools such as PYTHON which is an interpreter, multi-paradigm and multiplatform programming language. The python DJANGO framework is for the development of web applications. The NUMPY library of the Python programming language, intended to handle multidimensional matrices or arrays as well as mathematical functions operating on these arrays. The PYDICOM library of the Python language allowing the manipulation of DICOM files. The MYSQLCLIENT library of the Python language is for the connection to the MySQL database manager. The PYCRYPTODOME library of the stand-alone Python language of low-level cryptographic primitives and the Radian DICOM viewer-2 software is for viewing medical images.

DICOM files are made up of image details and patient details. These files are organized in tags referring to specific information. Fig. 1 shows an extract from the display of the tags of a DICOM file via the PYDICOM library from the command pydicom.dcmread('file name.dcm').



```
Dataset.file_meta -------------------------------
(0002, 0000) File Meta Information Group Leng
(0002, 0001) File Meta Information Version
(0002, 0002) Media Storage SOP Class UID
(0002, 0003) Media Storage SOP Instance UID
(0002, 0010) Transfer Syntax UID
(0002, 0012) Implementation Class UID
(0002, 0013) Implementation Version Name
(0002, 0016) Source Application Entity Title
-------------------------------------------------
(0008, 0005) Specific Character Set
(0008, 0008) Image Type
(0008, 0012) Instance Creation Date
(0008, 0013) Instance Creation Time
(0008, 0016) SOP Class UID
(0008, 0018) SOP Instance UID
(0008, 0020) Study Date
(0008, 0022) Acquisition Date
(0008, 0023) Content Date
(0008, 0030) Study Time
(0008, 0032) Acquisition Time
(0008, 0033) Content Time
(0008, 0060) Modality
(0008, 1030) Study Description
```

Fig. 1. Visualization of some DICOM Tags.

Fig. 2 and Fig. 3 respectively show the process of encryption and decryption of the proposed process.

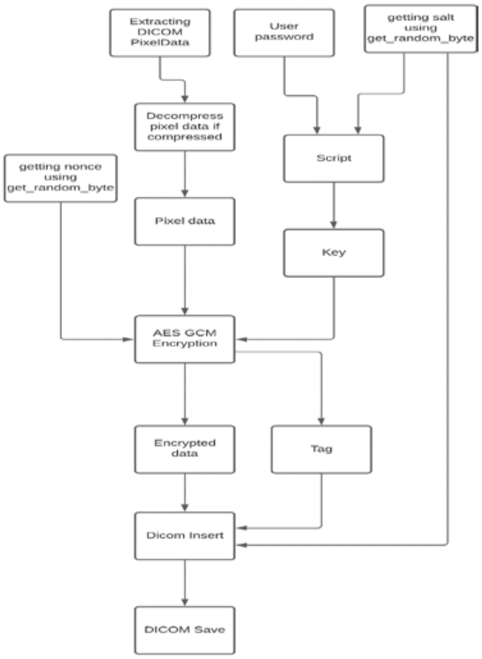

Extracting DICOM PixelData
User password
getting salt using get_random_byte
Decompress pixel data if compressed
getting nonce using get_random_byte
Script
Pixel data
Key
AES GCM Encryption
Encrypted data
Tag
Dicom Insert
DICOM Save

Fig. 2. Diagram of an Image Encrypting Process in DICOM Format.

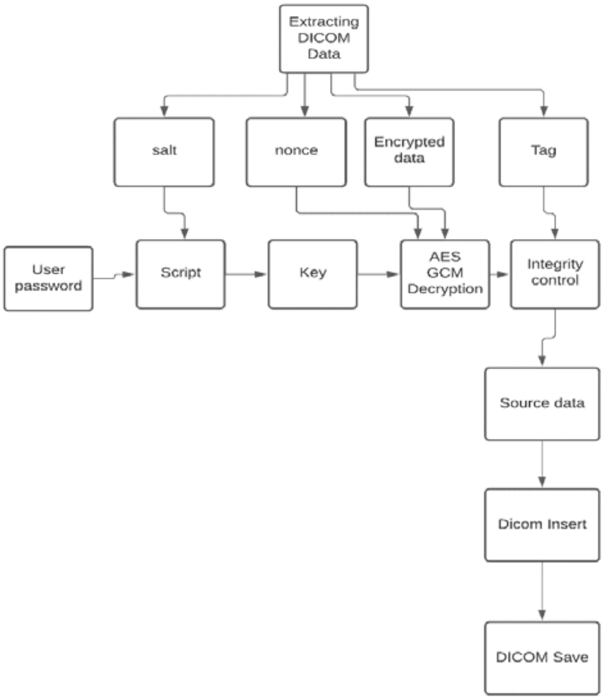
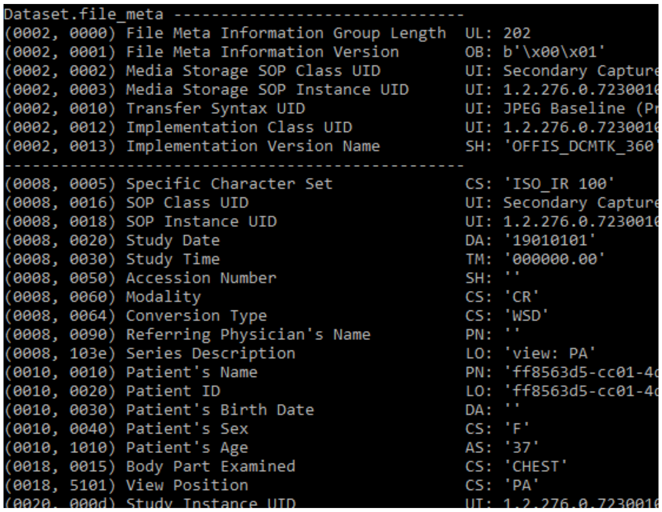


Fig. 3. Diagram of the Process of Deciphering a Cipher.

A. *Application of the Encryption Process for Medical Images with the AES Method in GCM Mode*

The encryption method adopted is to encrypt the entire contents of the file. A 32-byte encryption key is obtained by calculating the hash of a password from the script function. Then this key is used to initialize a cipher block from a 16-byte initialization vector. The chosen encryption mode is GCM.

Fig. 4 shows the extraction of DICOM tags before encryption. We can very well observe the corresponding values for each element concerning the patient.



```
Dataset.file_meta -------------------------------
(0002, 0000) File Meta Information Group Length  UL: 202
(0002, 0001) File Meta Information Version       OB: b'\x00\x01'
(0002, 0002) Media Storage SOP Class UID         UI: Secondary Captur
(0002, 0003) Media Storage SOP Instance UID      UI: 1.2.276.0.723001
(0002, 0010) Transfer Syntax UID                 UI: JPEG Baseline (P
(0002, 0012) Implementation Class UID            UI: 1.2.276.0.723001
(0002, 0013) Implementation Version Name         SH: 'OFFIS_DCMTK_360'
-------------------------------------------------
(0008, 0005) Specific Character Set              CS: 'ISO_IR 100'
(0008, 0016) SOP Class UID                       UI: Secondary Captur
(0008, 0018) SOP Instance UID                    UI: 1.2.276.0.723001
(0008, 0020) Study Date                          DA: '19010101'
(0008, 0030) Study Time                          TM: '000000.00'
(0008, 0050) Accession Number                    SH: ''
(0008, 0060) Modality                            CS: 'CR'
(0008, 0064) Conversion Type                     CS: 'WSD'
(0008, 0090) Referring Physician's Name          PN: ''
(0008, 103e) Series Description                  LO: 'view: PA'
(0010, 0010) Patient's Name                      PN: 'ff8563d5-cc01-4
(0010, 0020) Patient ID                          LO: 'ff8563d5-cc01-4
(0010, 0030) Patient's Birth Date                DA: ''
(0010, 0040) Patient's Sex                       CS: 'F'
(0010, 1010) Patient's Age                       AS: '37'
(0018, 0015) Body Part Examined                  CS: 'CHEST'
(0018, 5101) View Position                       CS: 'PA'
(0020, 000d) Study Instance UID                  UI: 1.2.276.0.723001
```

Fig. 4. Extract from DICOM tags before Encryption.

It should be remembered that bits as we have specified above, represent the content of the DICOM file. Fig. 5, Fig. 6 and Fig. 7 show on the first line (on the left the real image and on the right the corresponding histogram); on the second line, we have on the left the numbered image and on the right its corresponding histogram. This line clearly shows that the encryption process is indeed effective and its corresponding histogram sufficiently reflects the difference with the histogram of the real image. The third line reflects the result of the decryption process and we can observe the stability of these images compared to those of the first line.

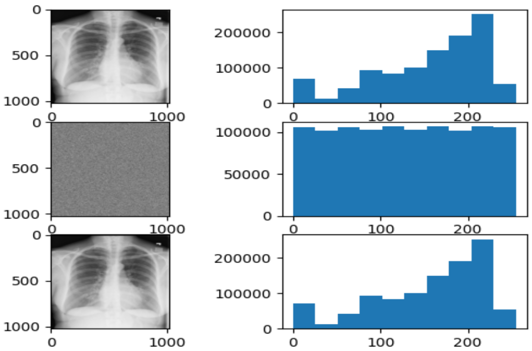


Fig. 5. Result of the Encryption and Decryption Process of a Radiology.

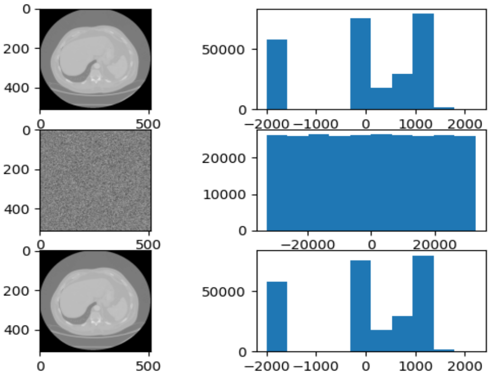


Fig. 6. Result of the Process of Encryption and Decryption of a Tomography.

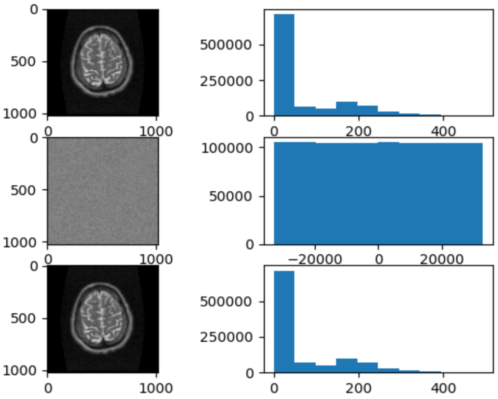


Fig. 7. Result of the Encryption and Decryption Process of an IRM.

B. Signature of the DICOM File

The owner of the image in the system has an RSA key pair. Image data such as: patient name, image pixels, patient ID; are combined and then compressed using the SHA256 function. The hash thus obtained is encrypted using the owner's private key and inserted into a tag in the DICOM file: the tag (0400,0120) or Signature.

To check the integrity of an image, the same data is extracted and the hash is recalculated. The signature is decrypted using the owner's public key accessible to everyone. The hashes thus obtained are compared. Since the hash functions are strict, the slightest change in the image will result in a drastic change in the hash. We can therefore say that the integrity of the image is preserved.

C. Evaluation of the Response Time of the Encryption and Decryption Process

The tests carried out on a radiology-type modality for a DICOM file of 4,739,280 bytes, i.e. 4.5MB, made it possible to obtain the Table I, which lists a set of 10 tests on the same medical image, thus making it possible to obtain each time the encryption and decryption time of said image.

Table I shows a variation of the encryption and decryption time. Note that the average encryption time for the tests performed is approximately 21.82 ms with a minimum time of 21.38 ms and a maximum time of 23.17 ms for a sample of 10 tests. Regarding the decryption, the average time is 22.12 ms for a minimum time of 21.09 ms (that is to say near to the minimum encryption time) and for a maximum time of 23.99 ms (near to the maximum encryption time). From the above results, we can attest to the speed of the encryption and decryption process of the AES algorithm in GCM mode.

TABLE I. EVALUATION OF THE ENCRYPTION AND DECRYPTION TIME OF THE PROCESS IMPLEMENTED IN A RADIOLOGY MODALITY

	Encryption Time (ms)	Decryption Time (ms)
T1	23,17	23,99
T2	21,53	21,33
T3	21,38	21,21
T4	21,53	21,48
T5	21,53	21,94
T6	21,58	21,91
T7	22,04	22,19
T8	21,83	21,09
T9	21,84	22,63
T10	21,81	22,50
MAX	23,17	23,99
MIN	21,38	21,09
AVG	21,82	22,12

VI. CONCLUSION

In this paper, we have proposed an efficient solution which is both, reliable and fast using a mechanism to reinforce the security of the contents of DICOM files in the PACS. To achieve this, we combined the AES symmetric encryption algorithm with the GCM authenticated encryption algorithm. As part of this work, the DICOM file is fully encrypted and then stored. The proposed solution requires less storage space in PACS because the content of the image is directly encrypted, the properties of the file remain the same. According to the experimental results, the image quality is not affected. The time required for encryption is on average 21.82 ms and that for decryption is 22.12 ms. Given these results, we can say that the minimum encryption time is equal to the average encryption time to the unit; the same is true for the decryption time. It should also be noted that the average difference in absolute value of the encryption and decryption time is of the order of 0.3 ms.

REFERENCES

[1] Alain Venot, “Security, legal and ethical aspects of computerized health data,” in Medical Informatics, e-Health, Paris, 2013.

[2] M. Karasad, “Tattooing Shared Medical Images,” p. 164.

[3] M. A. Hajjaji, H. Ridha, M. Abdellatif, and B. El-Bey, “Tattooing Medical Images for Data Integrity and Privacy,” Tunisia, nov. 2010, Accessed: Oct 24, 2020. [Online]. Available at: https://hal.archives-ouvertes.fr/hal-00822661.

[4] W. Puech, J. Rodrigues, and J.-E. Develay-Morice, “Secure Transfer of Medical Images by Joint Coding: Selective Encryption by AES in Stream Mode and JPEG Compression,” nov. 2006.

[5] Q.-A. Kester, “Image encryption based on the RGB PIXEL transposition and shuffling,” Int. J. Comput. Netw. Inf. Secur., vol. 5, p. 43-50, june 2013, doi: 10.5815/ijcnis.2013.07.05.

[6] Belmeguenaï Aïssa,Derouiche Nadir and Mansouri Khaled, “Security analysis of image cryptosystem using stream cipher algorithm with nonlinear filtering function,” International Journal of Advanced Computer Science and Applications(IJACSA),3(9),2012.

[7] Marie-Hélène Coste and Véronique Simon, “Journey to the Heart of Medical Imaging Networks,” Press kit, French Society of Radiology.

[8] E. Coumet, “Cryptography and numeration,” Ann. Hist. Sci. Soc., vol. 30, no 5, p. 1007-1027, 1975.

[9] Chikhi Samia Boucherkha, “Contribution to the Flexible Authentication of Digital Images Using Image Marking Techniques: Application to Medical Images,” oct. 2008.

[10] J.S. DELMOTTE and G. GAY, “Modern medical imaging applied to internal medicine, technical and practical aspects,” Lille, Nancy (France).

[11] R. E. C. Jr, M. G. Gaeta, D. M. Kaufman, et J. G. Henrici, “ Picture archiving and communication system,” US6574629B1, june 03, 2003.

[12] Romain Hérault, “Image tattooing and cryptography: To ensure the confidentiality, integrity and authentication of medical images and to insert confidential data,” DEA practical internship, August 20, 2004.

[13] P. Subhasri et D. A. Padmapriya, “Enhancing the security of dicom content using modified vigenere cipher,” vol. 10, p. 7, 2015.

[14] FIPS 197, “Advanced Encryption Standard (AES),” nov. 2001.

[15] « Rivest, Shamir et Adleman 1978, p. 122. » .

[16] « Menezes, van Oorschot et Vanstone 1996, chap. 8, p. 286 ; Schneier 1996, Applied Cryptography, p. 467. ».