Enhancing Security Mechanisms In DICOM Images Using AES Algorithm In Python

Mrs. S. Poonkodi[1], Ms.P.Gayathri[2]
[1, 2] Assistant Professor, Dept of Computer Science & Engineering
[1, 2] Karpaga Vinayaga College of Engineering & Technology, Kanchipuram Dt, Tamil Nadu, India

Abstract- *In our day to day life, health and its issues play a vital role. Nowadays most of the health care institution has to improving the patient diagnosis report in secure manner. The increased adoption of information system may lead to inefficient security. To overcome this inefficiency, the security level should be optimized. Health care institution categorized the clinical data into three types such as, demographic data, images and textual data (e.g. Report). Medical imaging is the process of using technology to view the human body for diagnosing, monitoring, and treating medical problems, therefore it is vital to take measures in order to prevent tampering and determine their provenance. Existing work provides information integrity and authenticity for medical images by the use of metadata and watermarking. However, still there are limitations for both approaches that must be properly addressed. This paper uses the cryptographic techniques of Advanced Encryption Standard (AES) algorithm for encryption and decryption in Python and DICOM standard to provide the information integrity, authenticity, and confidentiality for medical images.*

Keywords- Integrity, Authenticity, Confidentiality, Medical Images, Security, AES, Python, Digital Imaging and Communication in Medicine (DICOM)

I. INTRODUCTION

Health is one of the most basic needs of human. The introduction of information technology in the medical field has boosted the evolution of healthcare, replacing inefficient paper records to their digital counterparts, leading to the creation of electronic patient record / electronic health record (EPR / EHR).Digital information management involves standardization, ethics, privacy and security.

Due to lack of proper controls, procedures, and policies may tempt unauthorized users to access and use patient information in an inadequate fashion, weakening the credibility of healthcare information systems, and placing accuracy in diagnosis, treatment, and research into risk. Therefore, security is increasingly playing a relevant role in the healthcare field in order to provide services like information integrity, authenticity, confidentiality, and accountability.

Medical images are of paramount importance, given their importance to clinical diagnosis, treatment, and research. Therefore, there is a need for an infrastructure to ensure correct storage, processing, and visualization of medical images. The Digital Imaging and Communications in Medicine (DICOM) standard is world-wide accepted standard for medical images and Security.

This paper proposes the work deals with the medical images to facilitate information integrity, authenticity, and confidentiality using basic cryptographic techniques and Digital Imaging and Communication in Medicine (DICOM standard).

II. INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security shares the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. There are three points that should be taken into account when dealing with information security.

1. Security is not a strictly technological issue: The best security systems may be easily rendered useless by a legitimate, but a nonethical user. It can be said that security is ultimately about people, not technology [1].
2. There are no means to ensure total security: It is important to remember that the security level achieved depends on the trust assumed on the organizational, personal, and technological levels [2].
3. Security is an evolving process: Therefore, changes in the business rules and the technological advances require continuous updates of the security processes.

A. Security for Medical Images:

Integrity is the most important security asset for medical images. A degraded or tampered image is a potential source for mistakes in diagnosis, treatment, or research. The sender and receiver of a message may have a need for confidence that the message has not been altered during transmission it is called as integrity. [3]

Image integrity is closely related to its authenticity. The fidelity of information in a medical record is essential; this naturally demands means to identify the provenance and authorship of the information [4]. Confidentiality is preventing an opponent from extracting information from a communication channel. Confidentiality is achieved by using encryption and decryption process and reliable transmission.

III. THE DICOM STANDARD

There has been an enormous increase in the use of digital systems in the medical field. Nowadays, it is common in hospitals and other medical institutions to store, manage, exchange and retrieval medical images in a networked environment in so-called Picture Archiving and Communication Systems (PACS). PACS specify some agents, or nodes, that interact between them, allowing acquisition, visualization, archiving, retrieving, communication and general handling not only of the medical images themselves but also their related information. It follows then that in such a system there is a need for a common standardized ‖language‖ to which all nodes adhere so that effortless communication and collaboration is possible. This needed standardization is given by the Digital Imaging and COmmunication in Medicine (DICOM) standard.

DICOM mainly covers two main aspects: communication and data structures for storage. The communication aspect covers the definition of a protocol between PACS nodes based on the TCP/IP networking protocol and hence enables the agents to exchange information in a uniform and ordered manner. The data structure aspect defines the structure and formats of medical images and related information and is the part that we need to evaluate for its compatibility with thermal imaging.

IV. EXISTING APPROACH

In the existing method, there are two major approaches to provide authenticity and integrity: the use of metadata (e.g., header) and the use of watermarking.

A. Metadata:

Metadata are data attached to the information. For image security, usually the digital signature is the metadata, which is stored along with the medical image. This best approach is addressed in part 15 of the DICOM Std, where the digital signature information is stored in its header. The metadata approach has also been used to provide confidentiality, using DICOM header data to encrypt the images.

B. Watermarking:

Watermarking is a technique that embeds information into its own data. This method was proposed to improve medical image security. Zhou and Huang presented a method employing digital envelopes, i.e., encrypted digital signatures to add integrity and authenticity.

Limitations of Existing Work:

1. Metadata Approaches do not offer a strong bind between the medical image and its security metadata. So, it is relatively easy to weaken the metadata, making the image untrustworthy.
2. Watermarking Degrades image integrity, because the watermarked image resembles the original image. And, even if the adulteration is imperceptible to the human eye, the very notion of altering the image elicits resistance among the physicians.
3. Watermarking Has not been accepted by the DICOM standard yet, though there is a number of works involving watermarking DICOM images.

V. PROPOSED APPROACH

The proposed approach uses data encryption to provide integrity and authenticity of medical images. Therefore, an encrypted version of the image is stored, instead of the original data. This method takes advantage of the data structures proposed in the DICOM standard, making it a possible extension for the standard.

A. Basic Algorithm:

For this paper, a basic algorithm has been proposed and implemented, using a straightforward approach to encryption. The algorithm uses the DICOM header data as source to calculate the key and nonce [or initialization vector (IV)] of the encryption process. This complete process generates a stream of encrypted pixel data and an authentication tag, containing the information about the integrity of the pixel data.

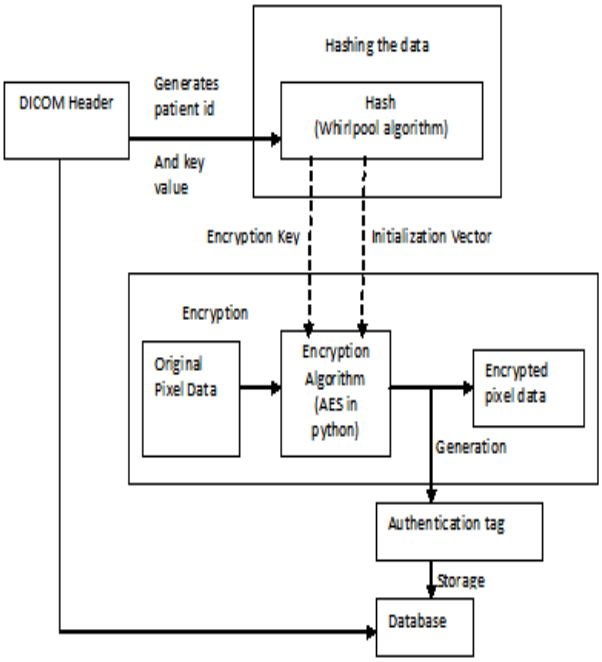

Fig. 1: Encryption Process

The encryption flow of the proposed algorithm is as follows (Fig.1): first, the header (or part of it) is hashed, generating an output of fixed size of bits representing its integrity. Then, a fixed portion of the output is used as the key and another portion, as the IV of the encryption algorithm. These will be the security data for image encryption, and the algorithm has to be sufficiently quick to provide an adequate performance. The AES GCM algorithm is used for encryption of the Medical image. It requires a secret key, initialization vector (IV), image and additional authenticated data for encryption process.

The authenticated encryption operation is defined by the following equations:

$$H = E(K, 0^{128})$$

$$Y_0 = \begin{cases} IV \,\|\, 0^{31}1 & \text{if } len(IV) = 96 \\ GHASH(H, \{\}, IV) & \text{otherwise.} \end{cases}$$

$$Y_i = incr(Y_{i-1}) \quad \text{for } i = 1, \ldots, n\,(1)$$

$$C_i = P_i \text{ xor } E(K, Y_i) \quad \text{for } i = 1, \ldots, n-1$$

$$C^*_n = P^*_n \text{ xor } MSB_u(E(K, Y_n))$$

$$T = MSB_s(GHASH(H, A, C) \text{ xor } E(K, Y_0))$$

At end of the encryption algorithm encrypted pixel data and authentication tag is generated, that information is stored on the database.

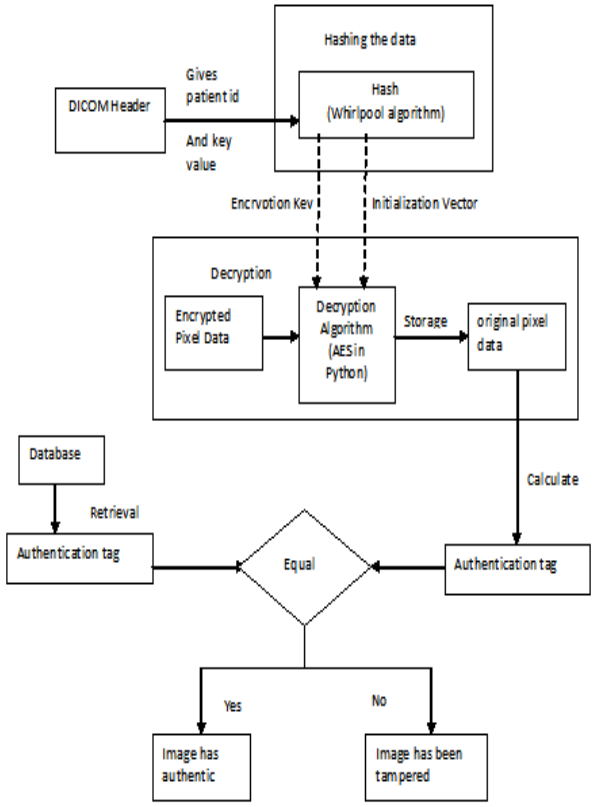

Fig. 2: Decryption and Verification Process

The decryption and security verification of the proposed algorithm are presented in Fig. 2 : first, the same header parts used in the encryption are retrieved and hashed to generate the key and the IV, in the same fashion of the encryption procedure. Then, the original pixel data are recovered from the encrypted data, as well as its authentication tag. This tag is matched against the data stored in the header, verifying the confidentiality, integrity and authenticity of the image.

The AES GCM algorithm is used for decryption of the Medical image. The authenticated decryption operation is similar to the encrypt operation, but with the order of the hash step and encrypt step reversed. More formally, it is defined by the following equations:

$$H = E(K, 0^{128})$$

$$Y_0 = \begin{cases} IV \,\|\, 0^{31}1 & \text{if len}(IV) = 96 \\ GHASH(H, \{\}, IV) & \text{otherwise.} \end{cases}$$

$$T' = MSB_s(GHASH(H, A, C)) \text{ xor } E(K, Y_0))$$

$$Y_i = incr(Y_{i-1}) \quad \text{for } i = 1, \ldots, n\,(1)$$

$$P_i = C_i \text{ xor } E(K, Y_i) \quad \text{for } i = 1, \ldots, n-1$$

$$P^*_n = C^*_n \text{ xor } MSB_u(E(K, Y_n))$$

The tag T' that is computed by the decryption operation is compared to the tag T associated with the ciphertext C. If the two tags match in both length and value, then the cipher text is returned. Otherwise, the special symbol **FAIL** is returned.

VI. IMPLEMENTATION AND EVALUATION OF THE BASIC ALGORITHM

A Python pycrypto was used for implementing the Advanced Encryption Standard algorithm proposed.

First, data were extracted from the DICOM header hashed using Whirlpool algorithm. This is a recent algorithm, proposed in the New European Schemes for Signatures, Integrity and Encryption (NESSIE) Project as a strong hash function, with a 512-bit output [7].

For this implementation, only the SOP instance UID and patient name were chosen to be hashed. The header hash was used as key for encrypting pixel data.

For data encryption, the algorithm of choice was Advanced Encryption Standard (AES) in Galois Counter Mode with a key size of 256 bits and an IV of 96 bits. This algorithm uses universal hashing over a binary Galois field to provide authenticated encryption, generating both the ciphertext and the authentication tag for integrity verification. It has been standardized by National Institutes of Standards and Technology (NIST) [8].

The encryption result is such that the processed pixel data hold no visual relation to the original image (Fig. 3). However, if the key and the image have not been tampered with, then it is possible to assert that the decrypted pixel data are exactly the same as the original image. This is a major difference to the existing watermarking approaches, since the user will only be able to see a meaningful image if it has not been altered in any way, be it perceptible or not.

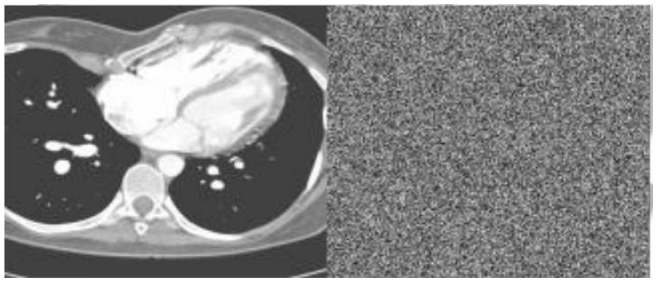

Fig. 3: Original Image (Left) and the Result of Its Encryption (Right)

Visually speaking, it is fairly obvious that the original image holds little or no relation to its ciphered counterpart. However, it is interesting to measure how related they are. Therefore, correlation was calculated for different modalities (Fig. 4).

Modality	Correlation
XA	$\|corr\| < 0.001$
MR	$\|corr\| < 0.001$
NM	$\|corr\| < 0.01$
US	$\|corr\| < 0.001$
CT	$\|corr\| < 0.01$

Fig. 4: Correlation between the Original Image and the Encrypted Image for Each Modality

Modality	Correlation frames i – (i-1)
XA	$\|corr\| < 0.001$
MR	$\|corr\| < 0.001$
NM	$\|corr\| < 0.01$
US	$\|corr\| < 0.001$
CT	$\|corr\| < 0.001$

Fig. 5: Correlation between consecutive frames of the encrypted image for each modality

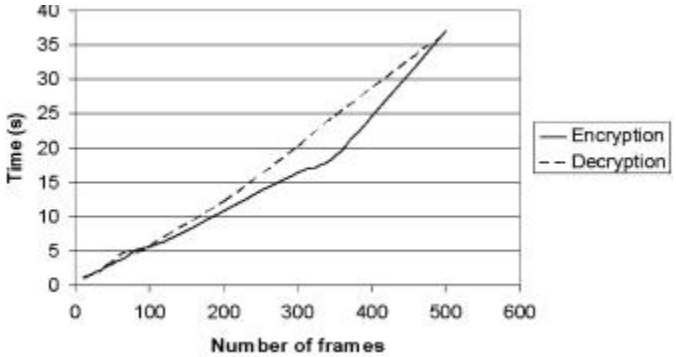

Fig. 6: Performance of Algorithm for IVUS Multiframe Images.

Correlation was also calculated between consecutive ciphered frames (Fig. 5). High correlation between frames could be a potential security weakness, since it could be exploited to retrieve useful information. Low correlation values are further evidences of the strength of the algorithm. For multiframe performance testing, intravascular ultrasound (IVUS) images were used. This modality was chosen because its number of frames may vary significantly, a convenient characteristic to evaluate the performance of the algorithm. Each IVUS frame has a size of 480 ×480 pixels, with a depth of 8 bits. The result of the test (Fig. 6) shows an approximately linear relationship between the number of frames and the time spent for encryption/decryption. Not having an exponential relation is positive, since it is possible to have IVUS images of more than 1000 frames.

VII. CONCLUSION

This paper proposes a new approach for medical image security. This method is distinct from the previous two approaches of watermarking and metadata, providing stronger trustworthiness of the medical images without compromising their quality.

This method has the advantage of using several structures and specifications from the DICOM standard, making it easier to be deployed. This paper allows the end user to see all images, tampered or not. This approach is achieved by symmetric encryption: the slightest modification in the data will affect the decryption process and the user will see only meaningless noise.

In the long run, the goal is to provide means to ensure information security in all levels of healthcare infrastructure, both intra institutional and inter institutional. To achieve this, it is vital to devise means to ensure security services like confidentiality, integrity and authenticity, and part of that effort to deliver better healthcare services to all involved parties.

REFERENCES

[1] J. Niinimaki, M. Savolainen, and J. J. Forsstrom, ―Methodology for security development of an electronic prescription system,‖ in Proc. AMIA Symp., 1998, pp. 245–249.

[2] A.Pfitzmann and B. Pfitzmann, ―Technical aspects of data protection in health care informatics, Adv. Med. Inf., pp. 368–386, 1992.

[3] D. L.Hamilton, ―Identification and evaluation of the security requirements in medical applications, in Proc. 5th Annu. IEEE Symp. Comput.-Based Med. Syst., Session 2B: Pictural Archival Commun. Syst., 1992, pp. 129–137.

[4] L. Rector, W. A. Nolan, and S. Kay, ―Foundations for an electronic medical record, Methods Inf. Med., vol. 30, pp. 179–186, 1991.

[5] Stallings, Cryptography and Network Security Principles and Practice. Englewood Cliffs, NJ: Prentice-Hall, 1999.

[6] Digital Imaging and Communications in Medicine (DICOM) Standard, DICOM. (2006). [Online]. Available: http://medical.nema.org/dicom/ 2006/

[7] P. S. L. M. Barreto and V. Rijmen. (2003). The WHIRLPOOL Hashing Function [Online]. Available: http://planeta.terra.com.br/informatica/ paulobarreto/whirlpool.zip.

[8] D. A. McGrew and J. Viega, ―The Galois/counter mode of operation (GCM), NIST Comput. Security Div., Comput. Security Resour. Center, Gaithersburg, MD, Tech. Rep., 2005