J Digit Imaging (2015) 28:179–187
DOI 10.1007/s10278-014-9734-8

Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images

Ali Al-Haj

Published online: 30 September 2014

Abstract Exchange of medical images over public networks is subjected to different types of security threats. This has triggered persisting demands for secured telemedicine implementations that will provide confidentiality, authenticity, and integrity for the transmitted images. The medical image exchange standard (DICOM) offers mechanisms to provide confidentiality for the header data of the image but not for the pixel data. On the other hand, it offers mechanisms to achieve authenticity and integrity for the pixel data but not for the header data. In this paper, we propose a crypto-based algorithm that provides confidentially, authenticity, and integrity for the pixel data, as well as for the header data. This is achieved by applying strong cryptographic primitives utilizing internally generated security data, such as encryption keys, hashing codes, and digital signatures. The security data are generated internally from the header and the pixel data, thus a strong bond is established between the DICOM data and the corresponding security data. The proposed algorithm has been evaluated extensively using DICOM images of different modalities. Simulation experiments show that confidentiality, authenticity, and integrity have been achieved as reflected by the results we obtained for normalized correlation, entropy, PSNR, histogram analysis, and robustness.

Keywords Cryptography · Telemedicine · DICOM · Confidentiality · Integrity · Authenticity

A. Al-Haj (✉)
Department of Computer Engineering, King Abdullah II Faculty of Engineering, Princess Sumaya University for Technology, Al-Jubeiha, PO Box 1438, Amman 11941, Jordan
e-mail: ali@psut.edu.jo

Introduction

Medical images are important to clinical diagnosis, treatment, surgery, and research, and thus they are considered a major constituent of electronic patients' records. In recent years, the exchange of medical images between hospitals and medical professionals boosted a number of telemedicine applications, such as teleconsulting, telediagnosis, telesurgery, among others [1, 2]. However, due to the increased risk of unauthorized manipulation and misappropriation of exchanged medical records caused by open communication environments, the underlying medical data transfer process must be protected and well-secured [3].

Ensuring security of exchanged medical records has been mandated by governments in the form of legislatives rules such as the Health Insurance Portability and Accountability Act (HIPAA) [4]. Such rules require any secured implementation of telemedicine applications to provide three security services: confidentiality, authenticity, and integrity. Confidentiality is required to prevent illegal access to the transmitted image and authenticity and integrity to detect any tampering or manipulation in the received image. Currently, digital watermarking and cryptography are the two major technologies adopted by the medical research community to provide telemedicine security services.

Digital watermarking has been recently proposed as a convenient platform to implement security in telemedicine systems [5–7]. Confidentiality is achieved by embedding the patient's record into the image as robust watermarks, whereas authenticity and integrity are achieved by embedding fragile or cryptographic watermarks into the image. Irreversible and reversible watermarking techniques have been used for embedding the different watermarks in the spatial domain and frequency domains. However, irreversible watermarking is not acceptable in the medical field since the distortion caused to the watermarked image involves noninvertible operations

such as bit replacement, truncation, or quantization [8, 9]. Reversible watermarking, on the other hand, allows the medical image to be restored to its original pixel values, however, it introduces computational overhead to restore the watermarked image back to its original state [10–14]. Generally speaking, watermarking, by its very essence, introduces image degradation, and thus it has not been adopted yet by medical standards and professionals.

Cryptography enforces telemedicine security using standard symmetric encryption algorithms to provide confidentiality and hashing functions and digital signatures to provide authenticity and integrity. The best known crypto-based telemedicine standard is the digital imaging and communications in medicine (DICOM) [15, 16]. The standard defines a technical framework for application entities involved in the exchange of medical images. Moreover, the standard offers a set security profiles and mechanisms to achieve the required telemedicine security [17].

From a practical point of view, the confidentially, integrity, and authenticity requirements must be enforced on both the medical image (pixel data) and the accompanying medical report (header data). This is a valid requirement since a medical image is of no use if it is not accompanied with a relevant informative medical report. However, the DICOM standard achieves confidentiality for the header data, but not for the pixel data. On the other hand, it offers authenticity and integrity for the pixel data but not for the header data. To address these security limitations of the standard, Kobayashi [18] proposed a crypto-based scheme based on the data structures of the DICOM standard. However, the proposed scheme provides confidentiality, authenticity, and integrity for the pixel data, but none of these security services is provided for the header data. This is a serious limitation of the scheme since the header contains sensitive patient's data in addition to security data such as encryption keys and digital signatures.

In this paper, we propose a crypto-based algorithm that provides confidentially, authenticity, and integrity for the header and pixel data of DICOM images. Strong cryptographic primitives, utilizing internally generated encryption keys and digital signatures, are used to provide the required security services. The keys and signatures are generated from the header and pixel data, thus a strong bond is established between the medical and security data used in the algorithm. Effective performance of the proposed algorithm is verified by the results we obtained for normalized correlation, entropy, peak signal-to-noise ratio (PSNR), histogram analysis, and robustness.

The remaining of the paper is organized as follows. "The DICOM Standard—Overview and Limitations" gives an overview of the DICOM standard and pinpoints its limitations. The proposed algorithm and the cryptographic primitives used in its implementation are described in "The Proposed Algorithm." Performance results are presented in "Performance Evaluation Results," and performance analysis is discussed in the "Discusssion." Concluding remarks are given in the "Conclusions."

The DICOM Standard—Overview and Limitations

The DICOM standard defines a technical framework for application entities involved in the exchange of medical data. Today, virtually all modalities that are used in radiology, such as CT, magnetic resonance imaging (MRI), and ultrasound, support the DICOM standard. For each modality, the standard defines attributes which contain image-related information such as patient's data and imaging procedure information. The standard also provides security mechanisms for application entities to authenticate each other and to detect any tampering with the messages exchanged. In what follows, an overview of the security profiles set by the DICOM standard is described and their limitations are outlined.

Security Profiles

The Health Insurance Portability and Accountability Act (HIPAA), issued by the federal government in the US, requires health providers to protect patient's privacy [19]. The HIPPA requirements have been projected in part 15 of the DICOM standard by defining a whole set of security and management profiles. The confidentiality of exchanged images is addressed by DICOM's basic application level confidentiality profile. The profile adopts current data encryption techniques, such as AES and Triple-DES, to convert selected header data into a protected format [20]. An application conforming to this profile may take all instances of the encrypted attributes, encrypt their original values, store the encrypted result in the tag (0400 and 0550) modified attributes sequence, and finally replace original values with dummy ones. The authenticity and integrity of the exchanged images are addressed by DICOM's digital signature profiles. These profiles adopt digital signature algorithms, such as DSA, to verify the authenticity and integrity of the pixel data [21]. The pixel data are digitally signed and the signature is stored in the DICOM's header according to the norms of the standard.

Limitations

Authenticity and integrity of the pixel data (image) are addressed by the digital signature profiles; however, its confidentiality is not addressed by the basic application level confidentiality profile. This is a major limitation in the standard because an image transmitted in plain may always get tampered, rendered, or edited. In fact, with any good image editor, one can edit anatomy features to completely alter the diagnostic result of the image.

As for the security of the header data, the DICOM standard addresses header's confidentiality according to the basic application level confidentiality profile. However, header's authenticity and integrity are not addressed, even though selected attributes are used by the digital signature profiles to provide authenticity and integrity for the pixel data. This is also a major limitation of the standard since the security of the header is of a vital importance because it contains sensitive patient's and security data. Other limitations are described in [22].

It could be argued that the overall security of DICOM's header and pixel data can be achieved using DICOM's secure transport connection profiles for network transporting DICOM data, and media storage security profiles for storing and storing DICOM objects as files. However, with current networking technologies, it is fairly easy for malicious adversary to intercept and tamper the DICOM data when the public network is used for telemedicine applications. Moreover, the DICOM data transmitted between medical centers using compact disc digital media is extremely vulnerable to alteration.

Proposed Improvement

Due to the limitations cited above, not all commercial implementations of DICOM security profiles declare their compliance to part 15 of the standard. Therefore, a wider acceptance of the standard requires improvements in the security profiles in terms of providing confidentiality, authenticity, and integrity to both constitutes of the DICOM image, the pixel and the header data. Kobayashi [18] proposed a novel scheme that addresses the security limitations of DICOM's PS 3.15 profiles. The scheme is based on data encryption, and it takes advantage of the data structures of the DICOM standard. The scheme addresses the confidentiality of the pixel data by allowing an encrypted version of the image to be transmitted. As for authenticity and integrity of pixel data, the scheme uses digital signatures with internally generated keys as shown in Fig. 1.

Looking at the security provided by the Kobayashi scheme to the header data, confidentiality is not provided since all attributes of the header are sent in plain text. Similarly, authenticity and integrity of the header data are not provided in a direct and straightforward manner. Instead, header data is indirectly protected since any modification of the header becomes perceptible by means of the digital signature included in the header. That is, if the header is tampered with, then the original and received encryption/decryption keys will differ, thus leading to a scrambled decrypted image. An obvious flaw of the indirect protection of the header data is the inability to trace the cause of a scrambled decrypted image, as whether the cause was by tamped header data or tampered pixel data (image).

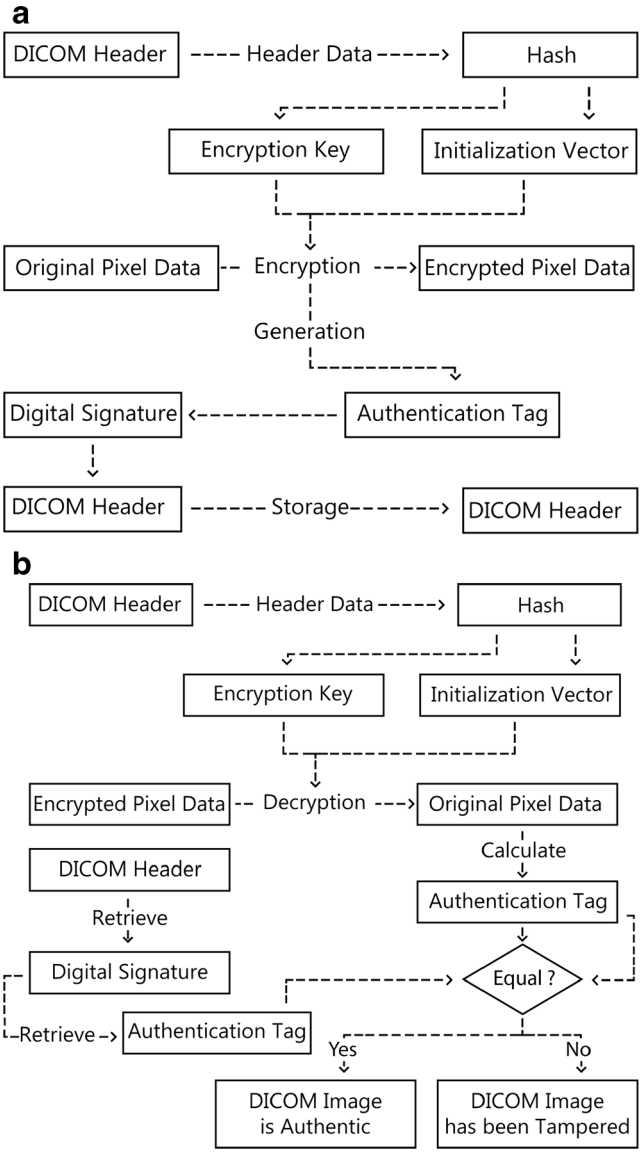


Fig. 1 Scheme proposed by Kobayashi [18]. **a** Encryption flow at the sender's side. **b** Decryption flow at the receiver's side

The Proposed Algorithm

The proposed algorithm is based on symmetric and asymmetric data encryption to provide confidentiality, integrity, and authenticity for the header and pixel data of DICOM images [23]. To achieve confidentiality, the pixel data is totally encrypted, whereas only confidential attributes of the header are encrypted. On the other hand, authenticity and integrity are achieved using digital signatures. The algorithm consists of two procedures; an encryption and signature creation procedure and a decryption and signature verification procedure. A detailed description of the two procedures is given in this section after briefly describing three cryptographic primitives employed in the procedures.

Cryptographic Primitives

Authenticated encryption improves the overall efficiency of information security systems compared with the conventional sequential encryption and authentication. *The Advanced Encryption Standard-Galois Counter Mode (AES-GCM)* is the best performing standard among the NIST-standardized authenticated encryption algorithms [24]. One merit of AES-GCM is that the computation cost of multiplication under the finite field *GF* (2^w) is less than integer multiplication [25]. AES-GCM takes as inputs the plain or cipher data, the encryption key, and the initialization vector, and outputs the cipher or plain data and an authentication tag.

The Whirlpool hashing function is a strong hashing function proposed in the New European Schemes for Signatures, Integrity and Encryption (NESSIE) Project. The Whirlpool hashing function produces a hash code of 512 bits [26]. *The elliptic curve digital signature algorithm (ECDSA)* is based upon elliptic curves and can offer levels of security with small keys comparable to RSA and other methods. ECDSA takes a hash input of 256 bits and outputs a digital signature of 256 bits using a private key [27].

Encryption and Signature Creation Procedure

The encryption and signature creation procedure is shown in Fig. 2, and it is described in details hereafter for the header and pixel data.

Header Data Encryption Process

Step 1 *(Encryption key generation)* Using the Whirlpool hashing function, hash the pixel data and divide the 512-bit output into two parts for use by the AES-GCE in the next step. The first part is used as the encryption key, and the second part as the initialization vector. Generating the encryption key and initialization vector from the hash value of the pixel data creates a strong link between the pixel, header, and security data. Thus, the user will not be able to see the correct header attributes if the pixel data gets tampered or corrupted. Moreover, Different DICOM files have different confidential header attributes, and thus the encryption key and initialization vector vary from one image to another. This reduces security risks and avoids introducing a potential vulnerability in the encryption process.

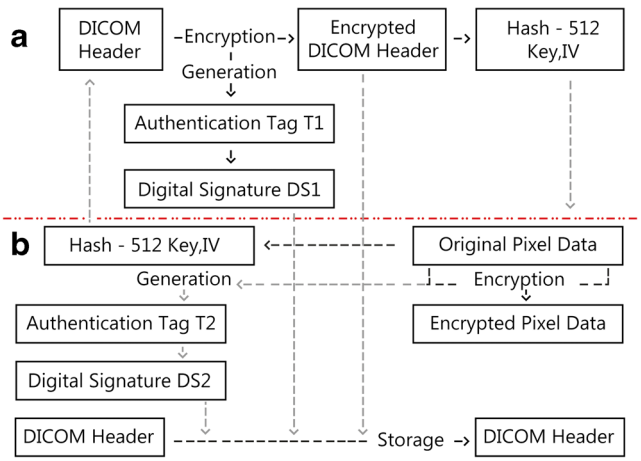


Fig. 2 Encryption and signature creation procedure: **a** for the header data and **b** for the pixel data

Step 2 (*Header data encryption*) Using the encryption key and initialization vector from the previous step, encrypt the confidential attributes of the header using AES-GCM. Store the encrypted attributes in the header's (0400 and 0550) modified attributes sequence, while replacing their original values with dummy ones. Other than the encrypted attributes, AES-GCM produces an authentication tag (AT) representing the hash value of the attributes.

Step 3 (*Digital signature generation*) Using the ECDSA, sign the authentication tag of the header with the private key of the sending entity and store the output digital signature in the header.

Pixel Data Encryption Process

Step 1 (*Encryption key generation*) Hash the encrypted header attributes using the Whirlpool hashing function and divide the 512-bit hash output into two parts for use by AES-GCE in the next step. The first part is used as the encryption key, and the second part as the initialization vector.

Step 2 (*Pixel data encryption*) Using the encryption key and initialization vector from the previous step, encrypt the pixel data using AES-GCM. Other than the encrypted pixel data, AES-GCM outputs an authentication tag representing its hash value.

Step 3 (*Digital signature generation*) Using the ECDSA, sign the authentication tag of the pixel data with the private key of the sending entity. The digital signature is stored in the header's digital signature sequence according to the digital signatures profiles described in part PS 3.15 of the DICOM standard.

Decryption and Signature Verification Procedure

The decryption and signature verification procedure is shown in Fig. 3 and described in details hereafter for the header and pixel data.

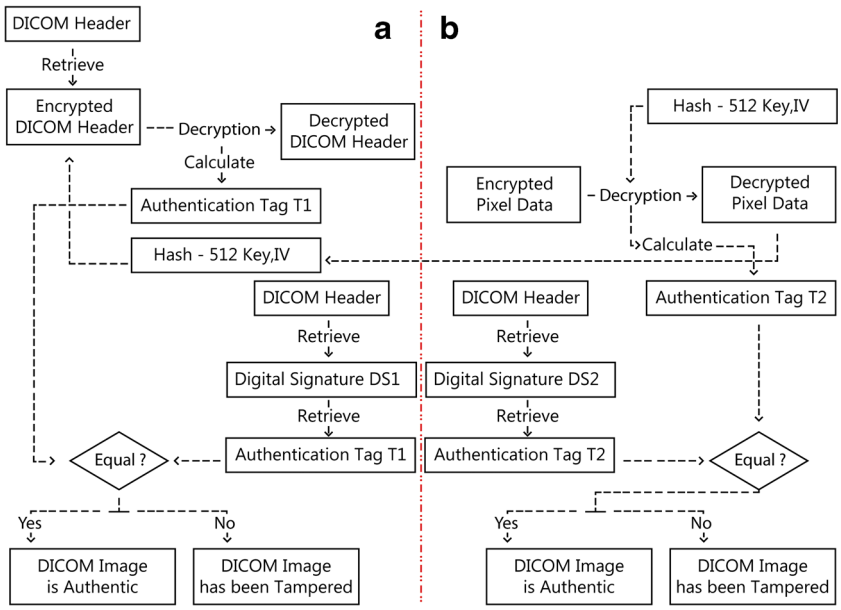


Fig. 3 Decryption and signature verification procedure: **a** for the header data and **b** for the pixel data

Pixel Data Decryption Process

Step 1 (*Encryption Key Generation*) Retrieve the encrypted part of the DICOM header, and hash it the using the Whirlpool hashing function. Divide the 512-bit hash output into two parts for use by AES-GCE in the next step.

Step 2 (*Pixel data decryption*) Using the decryption key and initialization vector, decrypt the pixel data using AES-GCM. Other than the decrypted header, AES-GCM produces an authentication tag representing its hash value.

Step 3 (*Authentication tag extraction*) Retrieve the digital signature of the pixel data from the DICOM header and extract its authentication tag using the public key of the sending entity.

Step 4 (*Authenticity and integrity verification*) Verify authenticity and integrity of the pixel data by comparing the authentication tag generated by the AES-GCM decryption process with the authentication tag extracted from the header's digital signature. If a match exists, the authenticity and integrity of the pixel data are verified.

Header Decryption Process

Step 1 (*Encryption keys generation*) Hash the decrypted pixel data using the Whirlpool hashing function and divide the output into two parts for use by AES-GCE in the next step. The first part is used as an encryption key, and the second part is used as the initialization vector.

Step 2 (*Header data decryption*) Using the decryption key and initialization vector, decrypt the encrypted part of the DICOM header using AES-GCM. Other than the decrypted header, AES-GCM produces an authentication tag representing hash value of the encrypted header.

Step 3 (*Authentication tag extraction*) Retrieve the digital signature of the encrypted header from the DICOM header and extract its authentication tag using the public key of the sending entity.

Step 4 (*Authenticity and integrity verification*) Verify authenticity and integrity of the header by comparing the authentication tag generated by the AES-GCM decryption process with the authentication tag extracted from the header's digital signature. If a match exists, the authenticity and integrity of the header is verified.

Performance Evaluation Results

In this section, we present performance results of the proposed algorithm. Extensive experimentation has been done using a benchmark set of 20 MRI DICOM brain images. The size of each image is 256× 256 pixels with a depth of 16 bits. The experiments were conducted in a GUI-based MATLAB environment running on a Dell N5010 machine (Intel Core TM, 4.00 GB RAM and M 350 at 2.27 GHz with Microsoft

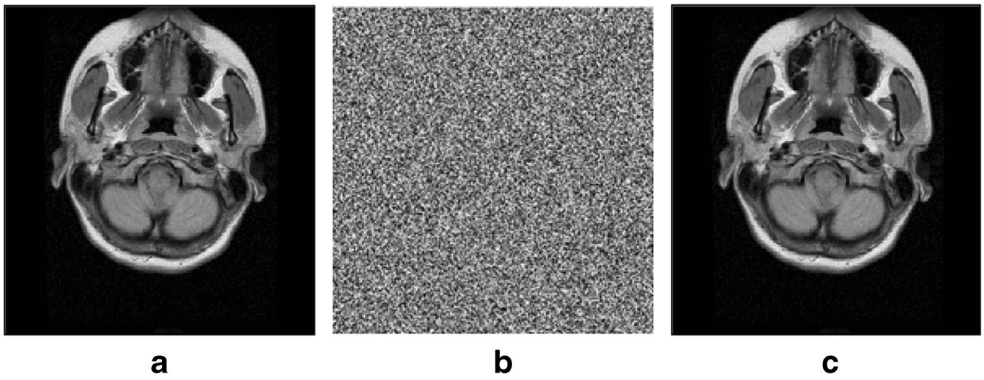


Fig. 4 **a** Original plain image. **b** Ciphered image. **c** Deciphered image

Windows XP operating system). The performance of the proposed encryption-based algorithm is evaluated with regard to its achievement of the required security services: confidentiality, authenticity, and integrity.

Confidentiality Performance Results

Confidentially is ensured if the encrypted image is highly uncorrelated to the original plain image. To measure correlation between the plain and encrypted images, shown in Fig. 4, the following sets of metric have been used: normalized correlation, PSNR, entropy, and histogram analysis.

Normalized correlation is a performance metric used to measure the degree of similarity between two objects. In the context of the proposed algorithm, if the cipher image and plain image are completely different, then their correlation factor will be very low or very close to zero. On the other hand, if the correlation factor is equal to one, then the two images are identical and the encryption method is completely ineffective. The correlation factor we measured between the plain and cipher images is 0.0047. This indicates that the encryption algorithm is able to hide all attributes of the transmitted image, thus achieving the required confidentiality.

The peak signal-to-noise ratio is another metric that measures the similarity between the original plain image and the cipher image. The low PSNR value achieved by the proposed algorithm (11.2941) proves that the two images are uncorrelated, and thus confidentiality is achieved.

Entropy is used to measure uncertainty present in the cipher image. The higher the entropy of the cipher image is, the higher the degree of randomness and confidentiality the image has. Given that the maximum theatrical entropy for a gray-scale image is 8 bits/pixel, the entropy obtained by the proposed algorithm is 7.9101 bits/pixel. For comparison, the entropy of the plain original image is 5.8739 bits/pixel indicating highly related pixels making up a meaningful image.

Image histogram analysis aids in visualizing correlation between the plain and cipher images by giving the probability of appearance of each gray level. Figure 5 shows histograms for the plain and cipher MR images. The large difference between the histograms of the two images indicates clearly that the images are highly uncorrelated. Furthermore, the histogram of the cipher image shown in Fig. 5b shows that the probabilities of appearance of the gray levels are equitably distributed, and thus little amount of information can be predicted from the cipher image.

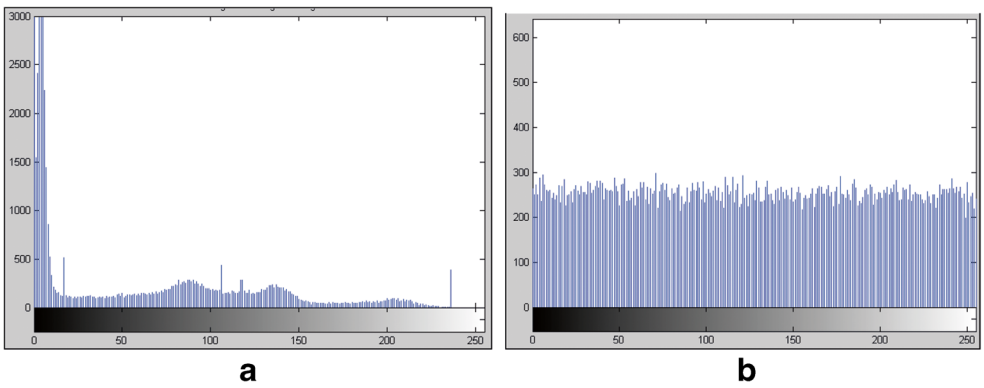


Fig. 5 Histograms of **a** the original plain image and **b** the cipher image

Authenticity and Integrity Performance Results

Authenticity and integrity of the received image is ensured, if and only if, the receiver's side is able to decrypt the image into its original form. Any manipulation of the cipher image must produce meaningless output data. Several signal processing attacks have been applied to the cipher image to simulate different manipulation scenarios. These attacks include additive Gaussian noise, JPEG compression, rotation, cropping, and dithering. Table 1 shows the attacked cipher image and the image produced by the decryption process. As shown in the table, the decryption process fails to produce the correct original image if the cipher image gets manipulated or tampered. This result emphasizes the strict-integrity property of the proposed algorithm which states that the receiver's side can only view the transmitted image, if and only if, the image is received intact without any manipulations. Similarly, the decryption process at the receiver's side will produce meaningless output data if the symmetric key gets manipulated or tampered. It is instructive to point out here that since the key is derived from the hash code of the encrypted header, then any manipulation of the header data will naturally lead to meaningless output pixel data as well.

Table 2 Encryption and decryption times for the header and pixel data

Header encryption time (s)	Pixel data encryption time (s)	Header decryption time (s)	Pixel data decryption time (s)	Total encryption time (s)	Total decryption time (s)
135.2	620.7	161.7	677.3	755.9	839.0

Time Performance Results

The time performance of the proposed algorithm is of a vital importance especially if the algorithm is to be deployed in a

Table 1 Robustness against statistical attacks

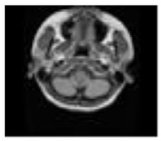
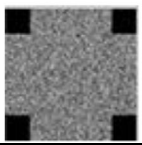
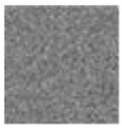
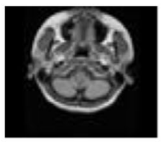
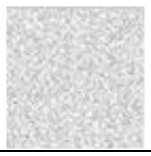
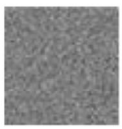
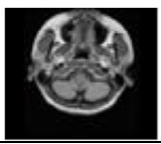
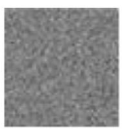
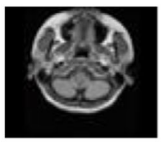
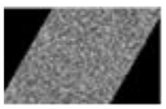
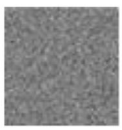
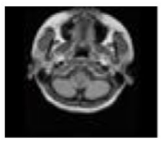
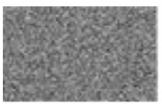
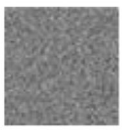
Attack Type	Original Image	Attacked Cipher Image	Deciphered Image
Cropping			
Additive Gaussian noise			
JPEG Compression			
Rotation			
Dithering			

Table 3 Comparing achievements of confidentiality, authentication, and integrity

Algorithm	Confidentiality (header)	Confidentiality (pixels)	Authenticity (header)	Authenticity (pixels)	Integrity (header)	Integrity (pixels)
DICOM standard	√			√		√
Kobayashi [18]		√		√		√
Proposed algorithm	√	√	√	√	√	√

hospital information system. The average encryption and decryption times, for both the header and pixel data, have been measured and recorded in Table 2. It is to be noted here that we encrypted all confidential attributes of the header, as proposed by the DICOM standard, to provide the required confidentially. Therefore, encryption and decryption times of the header could be greatly reduced if only a subset of the confidential attributes is encrypted. Further reduction in the encryption and decryption times can be achieved using specialized graphic processors or external graphics cards [28]. Optimized programming and parallelization techniques can also be used to enhance the overall time performance.

Discussion

Despite the importance of providing secure schemes for the exchange of medical images between healthcare entities, little research work has been reported. In this paper, we proposed a novel crypto-based algorithm that achieves confidentially, authenticity, and integrity for the header and pixel data of transmitted DICOM images. In this section, we compare our algorithm with the DICOM standard and with the crypto-based algorithm proposed by Kobayashi [18].

A DICOM file has two constitutes: header and pixel data. The DICOM standard achieves confidentiality of a selected subset of header's attributes through the mechanism specified in the PS 3.15 basic application-level confidentiality profile. However, the standard does not provide mechanisms to provide confidentiality for the pixel data. Similarly, the standard offers, through its base digital signature profiles, mechanisms to achieve authenticity and integrity of the pixel data, however, it provides no authenticity and integrity mechanisms for the header data. As for the algorithm proposed by Kobayashi [18], it operates on DICOM images and does not provide confidentiality for the header data. Encryption of the pixel data may provide it with confidentiality, however, the privacy of the pixel data will be violated if the symmetric key is retrieved by intruders, since the symmetric key is stored in the unprotected plain header. On the other hand, the algorithm provides authenticity and integrity for the pixel data but not for the header. Despite these limitations, a major contribution of the algorithm is the strong bond established between the pixel data and its security data. Finally, our proposed algorithm, as described throughout the paper, provides confidentiality, authenticity, and integrity, for both the header and the pixel data. A summary of the comparison made above is shown is Table 3.

Encryption of the pixel data is used by the proposed algorithm to provide confidentiality, authenticity, and integrity; however, it has been used by Kobayashi et al. [18] to provide authenticity and integrity only. Thus, and for completion, we compare their performance with regard to encryption quality by comparing their plain and cipher images using the metrics: normalized correlation, PSNR, and entropy. As show in Table 4, our proposed algorithm achieves better encryption performance and requires less encryption and decryption times.

Conclusions

The proposed algorithm provides confidentially, authenticity, and integrity to the header and pixel data of DICOM images exchanged between medical entities. Strong cryptographic primitives are used by the algorithm to provide the three security requirements by establishing strong bonds between the header and the pixel data, and their symmetric keys and hashing codes. Effective performance of the algorithm has been achieved as reflected by the results which we have obtained for correlation, entropy, PSNR, histogram analysis, and robustness. One direction of our ongoing research is to incorporate a tamper localization scheme into the algorithm to allow for content-based integrity, rather than the strict-

Table 4 Comparing encryption quality in terms of entropy, PSNR, correlation, and time

Algorithm	Entropy (bits/pixels)	PSNR (dB)	Normalized correlation	Encryption time (s)	Decryption
Proposed algorithm	7.9101	11.2941	0.0047	755.9	839.0
Kobayashi [18]	7.4764	11.4760	0.0242	876.2	904.2

integrity implemented by the current algorithm. Tamper localization is a useful functionality because integrity control based on the exact preservation of all parts of the image maybe unnecessarily strict. Tamper localization will also avoid unnecessary requests for retransmission between hospitals. Another future research direction is to extend the proposed algorithm to deal with multislice and multiframe DICOM images.

References

1. Raghupathi W, Tan J: Strategic IT applications in health care. Commun ACM 45(12):56–61, 2002
2. Huang H: PACS—Basic principles and applications. Wiley, New York, 1999, pp 116–119
3. Ashley R: Telemedicine: Legal, ethical and liability considerations. J Am Diet Assoc 102: no.2, 2002.
4. The Health Insurance Portability and Accountability Act (HIPAA), March 2009. [Online]. Available at http://www.hhs.gov/ocr/ privacy/ index.html
5. Chao H, Hsu C, Miaou S: A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Trans Inf Technol Biomed 6:46–53, 2002
6. Coatrieux G, Maitre H, Sankur B, Rolland Y, Collorec R: Relevance of watermarking in medical imaging. In: Proceedings of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, Arlington, USA, Nov. 2000, pp. 250–255
7. Coatrieux G, Lecornu L, Sankur B, Roux Ch: A review of image watermarking applications in healthcare. In: Porc. of IEEE-EMBC Conf., New York, USA, 2006, pp. 4691–4694
8. Giakoumaki A, Pavlopoulos S, Koutsouris D: Multiple image watermarking applied to health information management. IEEE Trans Inf Technol Biomed 10(4):722–732, 2006
9. Zhou XQ, Huang HK, Lou SL: Authenticity and integrity of digital mammography images. IEEE Trans Med Imaging 20(8):784–791, 2001
10. Guo X, Zhuang T: Lossless watermarking for verifying the integrity of medical images with tamper localization. J Digit Imaging 22(6): 620–628, 2009
11. Thodi D, Rodríguez J: Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730, 2007
12. Celik M, MU G, Sharma A, Tekalp: Lossless watermarking for image authentication: A new framework and an implementation. IEEE Trans Image Process 15(4):1042–1049, 2006
13. Liew S, Zain J: Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication. J Digit Imaging 24:114–125, 2011
14. Osamah M, Khoo B: Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. J Digit Imaging 24(1):114–125, 2011
15. Pianykh O: Digital Imaging and Communications in Medicine (DICOM). Springer, Berlin Heidelberg, 2012
16. Digital Imaging and Communications in Medicine (DICOM) Standard, DICOM. (2006). [Online]. Available at http://medical.nema.org/dicom/2006/
17. Digital Imaging and Communications in Medicine (DICOM), part 15: Security profiles ed., National Electrical Manufacturers Association (NEMA), 2001, PS 3.15–2001
18. Kobayashi L, Furuie S, Barreto P: Providing integrity and authenticity in DICOM images: A novel approach. IEEE Trans Inf Technol Biomed 13(4):582–589, 2009
19. Security and Privacy: An Introduction to HIPAA, Privacy and Security Committee, Medical Imaging Informatics Section, NEMA [Online]. Available at http://medical.nema.org/privacy/privacy.html
20. Digital Imaging and Communications in Medicine (DICOM) Supplement 55: Attribute Level Confidentiality DICOM Standards Committee, Working Group 14 Security 1300 N. 17th Street, Suite 1847 Rosslyn, Virginia 22209 USA VERSION: Final Text (Draft), 5 Sept. 2002 Security Supplement. Available at http://medical.nema.org/
21. NEMA Standards Publication, Digital Imaging and Communications in Medicine (DICOM) Supplement 142: Clinical Trial De-Identification Profiles, Version 3, National Electrical Manufacturers Association, Washington, 2008
22. Bendel and Mike: Hackers describe PS3 security as epic fail, gain unrestricted access. *Exophase.com*, 2010
23. Elbirt J: Understanding and Applying Cryptography and Data Security. CRC Press, USA, 2009
24. Dworki M: Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC. *NIST Special Publication,* 800-38D, 2007
25. Gueron and Shay: AES-GCM for efficient authenticated encryption—ending the reign of HMAC-SHA-1? In: Workshop on Real-World Cryptography, Stanford, USA, 2013
26. Barreto P, Rijmen V, The WHIRLPOOL hashing function [online]. Available at http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip. 2003
27. Caelli W, Dawson E, Rea S: Elliptic curve cryptography, and digital signatures. Comput Secur 18(1):47–66, 1999
28. Cook D, Ioannidis J, Keromytis A, Luck J: CryptoGraphics: Secret key cryptography using graphics cards. In: Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 2005, pp. 1–18. The paper is published in the series Lecture Notes in Computer Science Volume 3376, 2005, pp 334–350