

Crypto-based algorithms for secured medical image transmission

ISSN 1751-8709

Received on 15th May 2014

Revised on 2nd February 2015

Accepted on 11th March 2015

doi: 10.1049/iet-ifs.2014.0245

www.ietdl.org

Ali Al-Haj¹ ✉, Gheith Abandah², Noor Hussein³

¹Computer Engineering, Princess Sumaya University, Amman 11941, Jordan

²Computer Engineering, University of Jordan, Amman, Jordan

³Computer Engineering, Balqa Applied University, Salt, Jordan

✉ E-mail: ali@psut.edu.jo

Abstract: Booming telemedicine applications makes it deemed necessary to provide security services for such applications. The algorithms proposed in this field can be grouped into three classes: watermarking-based algorithms, crypto-based algorithms and hybrid algorithms. In this study, the authors propose two crypto-based algorithms capable of providing confidentiality, authenticity and integrity services to medical images exchanged in telemedicine applications. Strong cryptographic functions with internally generated symmetric keys and hash codes are used. The advanced encryption standard-Galois counter mode is used with the whirlpool hash function to provide confidentiality and authenticity, and the elliptic curve digital signature algorithm is used to provide authenticity and integrity. The proposed algorithms are based on the digital imaging and communication in medicine (DICOM) standard; however, unlike the standard, the algorithms provide confidentiality, authenticity and integrity for the header data, as well as for the pixel data of the DICOM images. Effectiveness of the proposed algorithms is evaluated and demonstrated through extensive experimentation using a benchmark set of DICOM images.

1 Introduction

Telemedicine is a modern medical care practice facilitated by the deployment of communication and information systems into the healthcare infrastructure. Numerous benefits are gained by telemedicine applications such as remote diagnosis and consultation among physicians, access to centralised medical archives and medical remote-distance learning [1, 2]. With these benefits, however, there are concomitant risks for medical data circulating in open networks, and thus being easily accessible by intruders [3, 4]. Therefore professionals working in the medical field have expressed their urgent need for secured schemes and methods capable of providing safe exchange of medical images and records.

The importance of a secured exchange of medical images has paved the way for international healthcare organisations to publish special standards that deal with medical data security issues. One such standard is the digital imaging and communication in medicine (DICOM) standard [5, 6]. The standard provides guidelines and mechanisms to healthcare professionals and entities to achieve three telemedicine security services: confidentiality, authenticity and integrity [7]. The confidentiality service is necessary to prevent illegal access to the transmitted images, whereas the integrity and authenticity services are needed to verify ownership and detect tampering of the received images. Currently, cryptography and digital watermarking technologies are used to implement schemes and algorithms capable of providing the required security services to telemedicine applications.

The crypto-based approach for achieving security in the medical information exchange systems is based on the application of cryptographic functions such as symmetric encryption, hashing and digital signatures [8]. Symmetric encryption provides confidentiality for the transmitted images using block ciphers and stream ciphers, whereas hashing and digital signatures verify authenticity and strict integrity of the received images. On the other hand, digital image watermarking is the practice of hiding secret data into digital medical images [9, 10].

Confidentiality is achieved by embedding the patient's private data as robust watermarks, whereas authenticity and integrity are achieved by hiding robust and fragile watermarks into the medical images [11]. Although the embedded watermarks are almost imperceptible to the human eye, the very idea of embedding, and thus degrading the medical image, may induce severe resistance to its adoption by medical standards and professionals.

In this paper, we propose two crypto-based algorithms capable of providing confidentiality and verifying authenticity and integrity of DICOM images. Unlike the DICOM standard and other crypto-based schemes, the proposed algorithms provide confidentiality, authenticity and integrity for both constitutes of the DICOM images: the header data and the pixel data. Strong cryptographic functions with externally and internally generated symmetric keys and hash codes are used in the implementation of the algorithms. The remaining of the paper is organised as follows. Section 2 describes recent secured telemedicine schemes and algorithms relevant to the proposed algorithms. The cryptographic functions used in the implementation of the algorithms are described in Section 3. The proposed algorithms are described in Section 4, and their performance results are presented and analysed in Section 5. Discussion and conclusions are given in Section 6.

2 Related work

Despite the booming applications of telemedicine, and the immediate need for providing security services for such applications, only recently research in this field has started to attract attention. The algorithms proposed in this field have been categorised under different classifications, however, in this paper we adopt our own classification which groups the methods into watermarking-based algorithms, crypto-based algorithms and hybrid algorithms. In this section, we briefly touch on related work in this field by describing representative algorithms under each class.

2.1 Watermarking-based algorithms

Three types of watermarking methods have been proposed for medical image watermarking: irreversible methods, reversible methods and region-based methods [12, 13]. Irreversible watermarking methods are not acceptable in the medical field since the distortion caused to the images by the watermarking process involves non-invertible operations such as bit replacement, truncation or quantisation [14, 15]. Reversible watermarking methods, on the other hand, allow the medical image to be restored to its original pixel values. Hence, original images can be used in the medical diagnosis process [16–20]. However, most reversible watermarking algorithms lack the tamper localisation capability which is desired in the integrity verification of medical images. The region-based methods involve segmenting the original medical image into two separate areas: region-of-interest (ROI) and region-of-non-interest (RONI). The two regions have different characteristics and thus different watermarks can be embedded to achieve different functionality. Most importantly, region-based methods possess the tamper localisation capability which provides content-based integrity for exchanged medical images [21–23]. However, segmenting the medical images into ROI and RONI regions is dependent on many factors and thus it may not always be accurate or even practical. Regardless of which of the three watermarking methods is acceptable, watermarking by its very essence introduces image degradation, and this may prevent it from possible future adoption by medical security standards and professionals.

2.2 Crypto-based algorithms

The crypto-based approach for achieving security in healthcare information systems is based on the application of cryptographic functions such as symmetric encryption, hashing and digital signatures [24–27]. The best known crypto-based method is the DICOM standard which provides different mechanisms to achieve security for exchanged medical images. The standard is described below along with its security limitations. The limitations were partially treated by Kobayashi *et al.* [24] as described later in this sub-section.

2.2.1 DICOM standard: DICOM is the worldwide accepted standard of reference for the exchange of medical images. The standard provides mechanisms for application entities to securely authenticate each other and detect any tampering with the exchanged medical data. The DICOM standard makes use of unique identifiers to uniquely identify DICOM objects such as images. The Health Insurance Portability and Accountability Act (HIPAA) security requirements have been projected in part 15 of the DICOM standard by defining a whole set of security and management profiles [28, 29].

A DICOM image has two constituents: header data and pixel data. Authenticity and integrity of the pixel data are addressed by the digital signature profiles, however, confidentiality of the pixel data is not addressed by the basic application level confidentiality profile [30, 31]. This is a major limitation in the standard because an image transmitted in plain may always get tampered with, rendered, or edited. In fact, with any good image editor, one can edit anatomy features to completely alter the diagnostic result of the image. Any editing of the image will not be detected if its digital signature gets deleted or lost from the header data. As for the security of the header data, the DICOM standard addresses header confidentiality according to the basic application level confidentiality profile, however, header's authenticity and integrity are not addressed. This is also a major limitation of the standard since the security of the header is of a vital importance because it contains sensitive patients' and security data. Other limitations of the DICOM standard are described in [32].

2.2.2 Kobayashi scheme: Owing to the limitations cited above, not all commercial implementations of DICOM's 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 constituents of the DICOM file: the pixel data and the header data. Kobayashi *et al.* [24] proposed a novel scheme that addresses the security limitations of DICOM's proposal supplement's (PS) 3.15 profiles. The scheme is based on data encryption and takes advantage of the data structures of the DICOM standard. It provides confidentiality for the pixel data by allowing an encrypted version of the image to be transmitted. However, since the keys of the encryption algorithm are stored without encryption in the header, the confidentiality provided for the pixel data may not be guaranteed. Authenticity and integrity are provided for the pixel data using digital signatures with internally generated keys. However, the proposed scheme does not provide confidentiality, authenticity and integrity for the header data.

2.2.3 Proposed crypto-based algorithms: The crypto-based algorithms we propose in this paper solve the security limitations of the DICOM standard and the Kobayashi scheme [24]. The algorithms provide confidentiality, authenticity and integrity for the pixel data as well as for the header data of DICOM images. Detailed description of the proposed algorithms and their performance evaluation results are given in the following sections.

2.3 Hybrid algorithms

To utilise the combined benefits of the two approaches, many crypto-watermarking algorithms have been proposed in literature that address the security requirements of telemedicine applications [33–36]. In the hybrid approach, watermarking is used as the implementation platform, and the integrity and authenticity watermarks are implemented as cryptographic primitives such as hash codes, cyclic redundancy codes (CRCs) and digital signatures. The cryptographic watermarks are embedded as robust or fragile watermarks depending on the required security service. In general, hash codes are used to provide strict integrity of the medical image, whereas CRCs are more appropriately used to detect tampered areas in the received image. However, hybrid algorithms suffer from being computation intensive. Moreover, a 1 bit change in a CRC or a hash code will lead to false authenticity and inaccurate integrity verification.

3 Cryptographic functions

The two proposed algorithms provide confidentiality, integrity and authenticity for the header and pixel data of DICOM images through the use of three effective cryptographic functions. The three functions are the advanced encryption standard-Galois counter mode (AES-GCM), the whirlpool hash function and the elliptic curve digital signature algorithm. The functions and their selection criteria are described in this section.

3.1 Advanced encryption standard-Galois counter mode

AES-GCM is an authenticated encryption function which is primarily used in applications demanding confidentiality, authenticity and integrity. The operation of AES-GCM is based on a universal hashing over a binary Galois field to provide authenticated encryption which produces cipher output for confidentiality, and authentication tag for authenticity and integrity verification. To operate properly, AES-GCM needs three inputs: the data to be encrypted or decrypted, a 256 bits encryption key and a 256 bits initial vector. The produced outputs are the encrypted or decrypted data and a 256 bits authentication tag [37].

The choice of AES-GCM has been based on the fact that it offers symmetric encryption and authentication at the same time. Such an authenticated encryption functionality outperforms the conventional sequential encryption and authentication, and thus improves the overall security of crypto-based applications. Moreover, it has been shown recently that AES-GCM is faster than many National Institute of Standards and Technology (NIST)

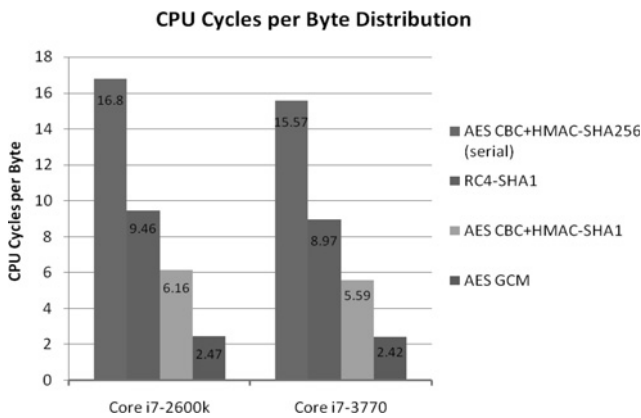


Fig. 1 Some authenticated encryption performance [38]

standardised authenticated encryption algorithms such as AES CBC + HMAC – SHA1, AES CBC + HMAC – SHA256 and RC4 – SHA1, as illustrated in Fig. 1 [38].

3.2 Whirlpool hash function

Whirlpool is a hash function that was developed in the New European Schemes for Signatures, Integrity and Encryption project, and standardised by International Standards Organisation [39]. The function operates on messages $<2^{256}$ bits in length to produce a hash code of 512 bits. The code is divided in our implementation of the proposed algorithms into two parts: 256 bits for encryption keys and 256 bits for initialisation vectors. The whirlpool hash is a strong function when compared with other hash functions such as MD5, SHA-1, SHA-224, SHA-256 and SHA-384. A similarly strong hash function is the SHA-512 hash, however, we have chosen to use the whirlpool hash function because of the fact that no attacks have been reported on earlier versions of the function.

3.3 Elliptic curve digital signature algorithm

The elliptic curve digital signature algorithm (ECDSA) is a variant of the digital signature algorithm (DSA). Both algorithms are based on public key cryptography, however, ECDSA uses elliptic curve cryptography (ECC) to produce shorter signatures than the original DSA, while maintaining the same security levels [40]. This property is of a particular importance for our proposed algorithms since the 256 bits digital signatures produced by ECDSA can be easily stored in the DICOM header, as will be explained in the proposed algorithms section. Furthermore, ECDSA reduces the computational requirements while maintaining the same level of security afforded by other public key schemes with correspondingly larger keys. Table 1 shows that a 256 bits ECC provides the same security level a 3072 bits Diffie–Hellman scheme offers, at much lower computation cost [41].

Table 1 Relative computation costs of Diffie–Hellman and elliptic curves [41]

Diffie–Hellman key size, bits	ECC key size, bits	Cost ratio between Diffie–Hellman and ECC
1024	160	3:1
2048	224	6:1
3072	256	10:1
7680	384	32:1
15 360	512	64:1

4 Proposed algorithms

Two algorithms are proposed, each of which consists of two procedures: the encryption and signature creation procedure, and the decryption and signature verification procedure. The first algorithm uses AEC-GCM, the whirlpool hash function and ECDSA, whereas the second algorithm uses AEC-GCM and ECDSA only. A description of the two algorithms is given in this section.

4.1 First algorithm

This algorithm uses symmetric encryption, hashing and digital signatures to provide confidentiality, integrity and authenticity for the header and pixel data of DICOM images. The pixel data and confidential attributes of the header data are encrypted using AES-GCM which produces the cipher pixel data and an authentication tag simultaneously. The encryption keys and initialisation vectors are produced internally using the whirlpool hash function. The authentication tag is then signed by ECDSA. The encryption and signature creation procedure, and the decryption and signature verification procedure are described below.

4.1.1 Encryption and signature creation procedure: This procedure takes the pixel data and the confidential attributes of the header data as its inputs, and outputs fully encrypted pixel data and partially encrypted DICOM header. Operational steps of the procedure are illustrated in Fig. 2.

1. **Header data confidentiality:** To conform to the basic application level confidentiality profile described in DICOM PS 3.15, the procedure reads all confidential attributes of the header, encrypts their original values using AES-GCE and stores the result in the ‘modified attributes sequence (0400, 0550)’ while replacing the values in the original locations with dummy ones. An additional output of AES-GCE is the authentication tag of the header which will be used in the next step. The encryption key and initialisation vector used by AES-GCE to encrypt the header data are taken from the hash code produced by applying the whirlpool hash function on the pixel data. The hash code is then encrypted by AES and stored in the DICOM header for later use at the receiver’s side. Generating the encryption key and initialisation vector from the hash code 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 with or corrupted. Moreover, different DICOM files have different confidential header attributes, and thus the encryption key and initialisation vector vary from one image to

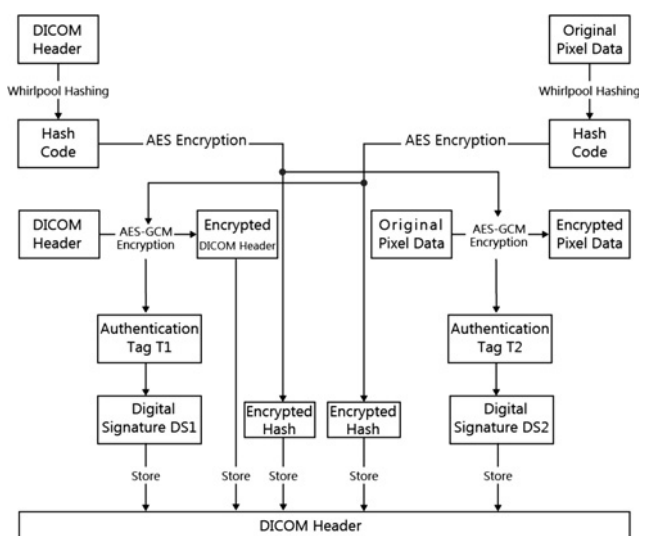


Fig. 2 Encryption and signature creation procedure of the first algorithm

another. This reduces security risks and avoids introducing a potential vulnerability in the encryption process.

2. *Header data authenticity and integrity*: The authentication tag produced by AES-GCE in the previous step is signed with the private key of the sending entity using ECDSA. The generated digital signature is stored in the DICOM header. Authenticity and integrity of the header data are not addressed in part 15 of the DICOM standard.

3. *Pixel data confidentiality*: The pixel data is encrypted with AES-GCE: the same encryption algorithm used to encrypt the header data. However, the encryption key and initialisation vector are the hash code produced by applying the whirlpool hash function on the confidential attributes of the header. The hash code (encryption key and initialisation vector) is then encrypted by AES and stored in the DICOM header for later use at the receiver's side. An additional output of AES-GCE is the authentication tag of the pixel data which will be used in the next step. Encryption, and thus confidentiality, of the pixel data is not addressed in part 15 of the DICOM standard.

4. *Pixel data authenticity and integrity*: The authentication tag produced by AES-GCE in the previous step is signed with the private key of the sending entity, generating a digital signature of the pixel data. The signature is stored in the DICOM header according to the digital signatures profiles described in part PS 3.15 of the DICOM standard.

4.1.2 Decryption and signature verification procedure:

This procedure decrypts the partially encrypted DICOM header and the encrypted pixel data, and verifies their authenticity and integrity as shown in Figs. 3 and 4 and described hereafter.

1. *Pixel data confidentiality*: Retrieve the encrypted hash code of the header's confidential attributes from the DICOM header and decrypt it using the AES standard. The 512 bits output is used by AES-GCM as a decryption key and an initialisation vector to decrypt the pixel data. Other than the pixel data, AES-GCM produces an authentication tag of the pixel data.

2. *Pixel data authenticity and integrity*: Retrieve the digital signature of the pixel data from the header and extract its authentication tag using the public key of the sending entity. Compare the extracted tag with the authentication tag generated by AES-GCE in the previous step. If a match exists between the two tags, authenticity and integrity of the pixel data are verified.

3. *Header data confidentiality*: Retrieve the encrypted hash code of the pixel data and decrypt it using the AES standard. The 512 bits output is used by AES-GCM as a decryption key and initialisation vector to decrypt the confidential attributes of the header. Other than the decrypted header's attributes, AES-GCM produces an authentication tag of the attributes.

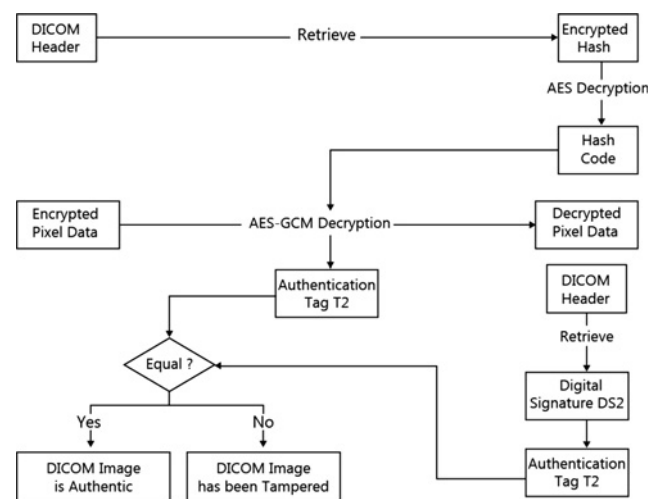


Fig. 3 Pixel data decryption and signature verification procedure

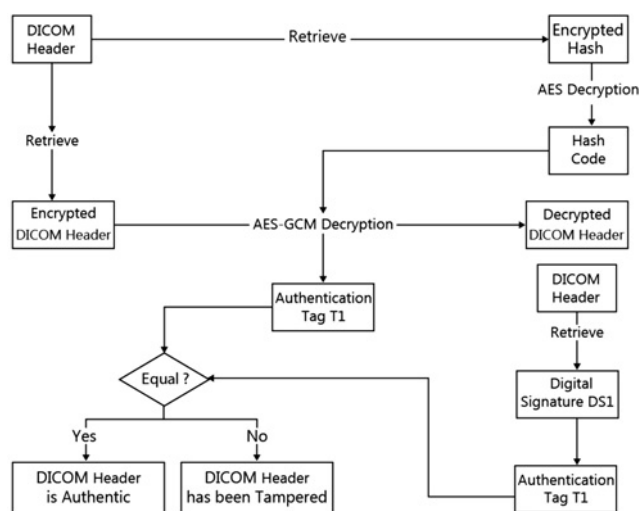


Fig. 4 Header data decryption and signature verification procedure

4. *Header data authenticity and integrity*: Retrieve the digital signature of the header data from the DICOM header and extract its authentication tag using the public key of the sending entity. Compare the extracted tag with the authentication tag generated by AES-GCE in the previous step. If a match exists between the two tags, authenticity and integrity of the confidential header attributes are verified.

4.2 Second algorithm

In the first algorithm described above, the encryption keys and initialisation vectors used by AES-GCM are generated internally by hashing the pixel data and the confidential attributes of the header. This enhances security of the algorithm by establishing a strong bond between the header data, pixel data and the generated security data. However, hashing the pixel data and the confidential attributes of the header to generate the keys and initialisation vectors may cause computational overhead, since hashing, by its very nature, is a computation-intensive process. Therefore the second algorithm described here eliminates such an overhead by providing the encryption keys and initialisation vectors externally. The keys can be supplied using traditional methods such as key distribution centres or public-key methods such as the Diffie-Hellman key exchange. Another option for the exchange of external keys and initialisation vectors is to store them encrypted in the DICOM header at the sender's side, and decrypt them at the receiver's side.

4.2.1 *Encryption and signature creation procedure*: This procedure takes the pixel data and the confidential attributes of the header data as its inputs, and produces fully encrypted pixel data and partially encrypted DICOM header. Operational steps of the procedure are illustrated in Fig. 5 and described in detail below.

1. *Header data confidentiality*: Read all confidential attributes of the header, encrypt their original values with AES-GCE, and store the encrypted attributes in the 'modified attributes sequence (0400, 0550)', while replacing the values in the original locations with dummy ones. The AES-GCE encryption process uses an externally supplied encryption key and an initialisation vector. Other than the encrypted header data, AES-GCM outputs an authentication tag of the confidential attributes of the header.

2. *Header data authenticity and integrity*: Sign the authentication tag produced by AES-GCE with the private key of the sending entity using ECDSA. This is followed by storing the generated digital signature of the header in the DICOM header according to the digital signatures profiles described in part PS 3.15 of the DICOM standard.

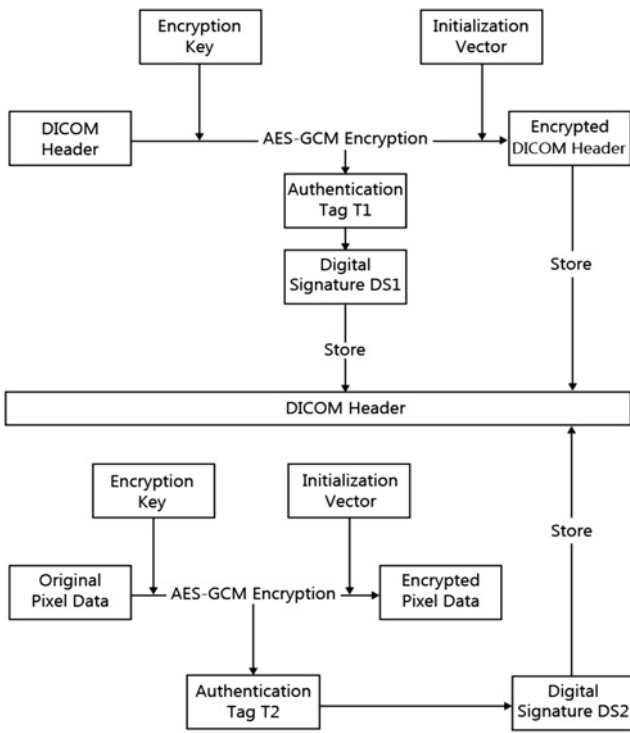


Fig. 5 Encryption and signature creation procedure of the second algorithm

3. *Pixel data confidentiality*: Encrypt the pixel data with AES-GCE using the same encryption algorithm, encryption key and initialisation vector used to encrypt the header data. In addition to the encrypted data, AES-GCM outputs an authentication tag of the pixel data.

4. *Pixel data authenticity and integrity*: Sign the authentication tag generated by AES-GCE with the private key of the sending entity. The generated digital signature of the pixel data is stored in the DICOM header according to the digital signatures profiles described in part PS 3.15 of the DICOM standard.

4.2.2 Decryption and signature verification procedure:

This procedure decrypts the received DICOM header and pixel data, and verifies their authenticity and integrity as shown in Figs. 6 and 7 and described below.

1. *Pixel data confidentiality*: Using the decryption key and initialisation vector used by the sending entity, apply AES-GCE to produce the pixel data and the corresponding authentication tag.

2. *Pixel data authenticity and integrity*: Retrieve the digital signature of the pixel data from the header and extract its authentication tag using the public key of the sending entity. Compare the extracted tag with the authentication tag generated by AES-GCE in the previous step. If a match exists between the two tags, authenticity and integrity of the pixel data are verified.

3. *Header data confidentiality*: Using the decryption key and initialisation vector used by the sending entity, apply AES-GCE to produce the decrypted header data and the corresponding authentication tag.

4. *Header data authenticity and integrity*: Retrieve the digital signature of the header data from the DICOM header and extract its authentication tag using the public key of the sending entity. Compare the extracted tag with the authentication tag generated by AES-GCE in the previous step. If a match exists between the two tags, authenticity and integrity of the confidential header attributes are verified.

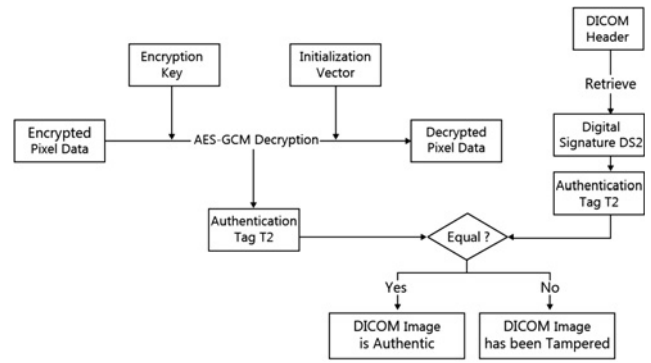


Fig. 6 Pixel data decryption and signature verification procedure

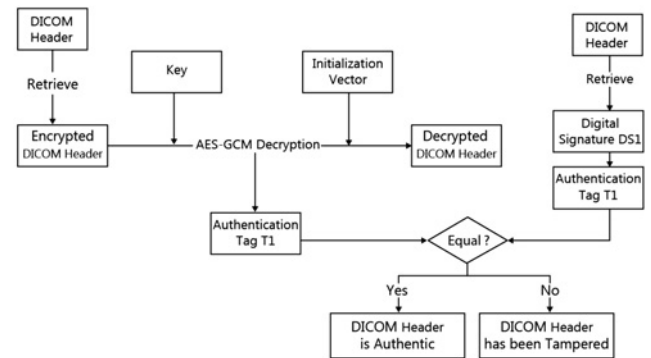


Fig. 7 Header data decryption and signature verification procedure

5 Performance analysis

Extensive experimentation has been done using a benchmark set of 20 MRI DICOM brain images to evaluate performance of the proposed algorithms with regard to their achievements of the preset security requirements. The size of each DICOM image is 256 × 256 pixels with a depth of 16 bits. The experiments were conducted in a graphical user interface (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 Windows XP operating system).

Confidentiality is ensured if the encrypted image is highly uncorrelated to the original plain image. To measure correlation between the plain and encrypted images produced by the two algorithms, the following set of performance analyses are used: similarity analysis, entropy analysis and histogram analysis. Strict integrity analysis has also been conducted to demonstrate authenticity and integrity of the algorithms. Finally, time analysis is conducted to evaluate the computational requirements of the two algorithms.

Proposed Algorithm	Original Image	Cipher Image	Correlation Factor	PSNR (dB)
Algorithm I			0.0081	11.1309
Algorithm II			0.0081	11.3778

Fig. 8 Correlation and PSNR values between the original and cipher images

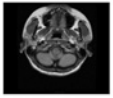

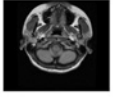

Proposed Algorithm	Original Image	Entropy of Original Image (bits/pixel)	Cipher Image	Entropy of Cipher Image (bits/pixel)
Algorithm I		5.8739		7.8909
Algorithm II		5.8739		7.9969

Fig. 9 Entropy values for the original and cipher images

5.1 Similarity analysis

Normalised correlation is a performance metric used to measure the degree of similarity between two digital objects. In the context of the proposed algorithms, if the plain and cipher images are completely different, then their normalised correlation factor will be very low or very close to zero. The correlation factors we measured between the plain and cipher images are given in Fig. 8. The low correlation values indicate that the encryption procedures we used are able to hide all attributes of the transmitted image, thus achieving the required confidentiality. Peak signal-to-noise ratio (PSNR) is another metric that measures the similarity between the plain and the cipher images. The PSNR values achieved by the proposed algorithms are given in the same figure. The low values prove that the two images are uncorrelated, and thus confidentiality is achieved.

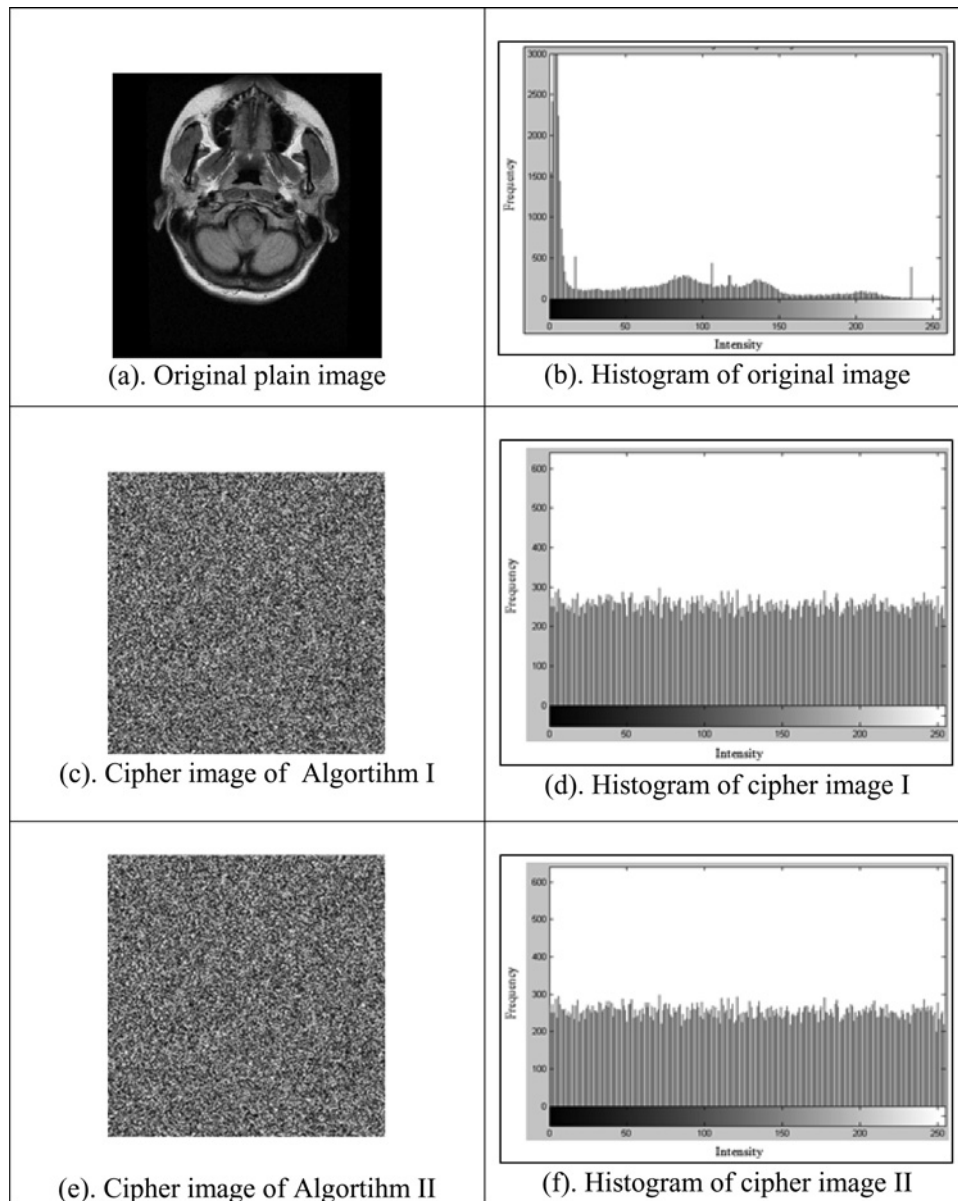


Fig. 10 Plain and cipher images and their corresponding histograms

- a Original plain image
- b Histogram of original image
- c Cipher image of algorithm I
- d Histogram of cipher image I
- e Cipher image of algorithm II
- f Histogram of cipher image II


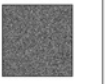
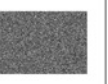
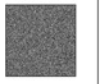

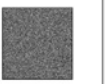
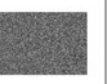
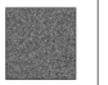
Proposed Algorithm	Noisy Cipher Image	Deciphered Image	Compressed Cipher Image	Deciphered Image
Algorithm I				
Algorithm II				

Fig. 11 Attacks showing the strict integrity of the proposed algorithms

5.2 Entropy analysis

Entropy is used to measure the 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 theoretical entropy for a grey scale image is 8 bits/pixel, the entropy values obtained for the proposed algorithms are given in Fig. 9. The achieved entropy values of the cipher images are close to 8 bits/pixel which demonstrate the effectiveness of the proposed algorithms in hiding the details of the original images. The entropy value of the original plain image is given in the figure for comparison.

5.3 Histogram analysis

Image histogram analysis aids in visualising correlation between the plain and cipher images by giving the probability of appearance of each grey level. Fig. 10 shows the histograms for the plain and cipher images for the two algorithms. The large difference between the histograms of the plain and cipher images shown in the figure indicates that the images are highly uncorrelated. Furthermore, the histograms of the cipher images show that the probabilities of appearance of the grey levels are equitably distributed, and thus little amount of information can be predicted from the cipher images.

5.4 Strict integrity analysis

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 images to simulate different manipulation scenarios. These attacks include additive Gaussian noise, JPEG compression, rotation, cropping, among others. Fig. 11 shows the result of two attacks on the cipher images: the Gaussian noise and JPEG compression. As shown in the figure, the decryption process fails to produce the correct original images if the cipher images are tampered with by a Gaussian noise or a JPEG compression attack. This result emphasises the strict integrity property of the proposed algorithms which states that the receiver's side can only view the originally transmitted plain image, if and only if, the image is received intact without any manipulations.

Table 2 Encryption quality and runtime comparison with Kobayashi scheme

Algorithm	Normalised correlation	PSNR, dB	Entropy, bits/pixel	Encryption time, s	Decryption time, s
algorithm I	0.0081	11.1309	7.8909	811.7	861.1
algorithm II	0.0081	11.3778	7.9969	484.8	552.7
Kobayashi [24]	0.0242	11.4760	7.4764	876.2	904.2

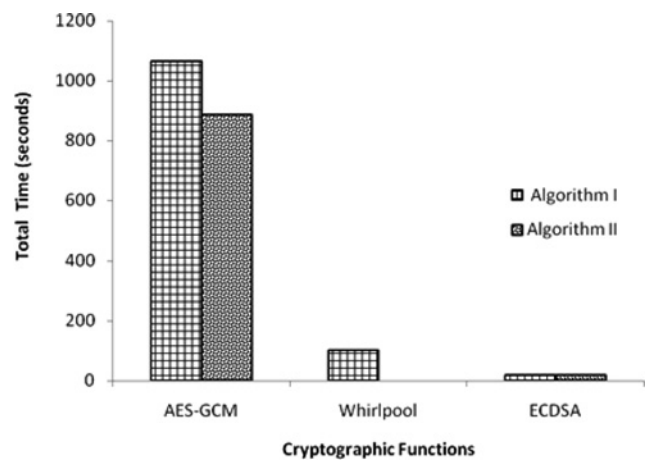


Fig. 12 Total processing time distribution for the cryptographic functions

5.5 Time analysis

The total encryption and decryption times, for both algorithms, have been measured and illustrated in Fig. 12. For the first algorithm, the encryption and decryption times were 811.7 and 861.1 s, respectively. The second algorithm required a lesser amount of computation since the encryption keys and initialisation vectors were supplied externally, and not generated internally. The total encryption and decryption times for the second algorithm were 484.8 and 552.7 s, respectively.

For a better understanding of the computational requirements of the three cryptographic functions, Fig. 12 shows a breakdown of the total encryption and decryption times elapsed by each function. As shown in the figure, the two algorithms spend most of their time in executing the AEC-GCM encryption and decryption procedures. The whirlpool is only executed in the first algorithm to generate the private keys and initial vectors for AEC-GCM, and ECDSA requires the least processing time for the two algorithms.

AEC-GCM encryption and decryption times could be greatly reduced if only a subset of the confidential DICOM header attributes are encrypted, instead of encrypting all attributes as proposed by the DICOM standard. Further reduction in the encryption and decryption times can also be achieved using specialised hardware such as graphic processors in addition to parallel programming methods.

5.6 Performance comparison

Authenticated encryption has been used by our proposed algorithms to provide confidentiality, authenticity and integrity, however, it was used by Kobayashi *et al.* [24] to provide authenticity and integrity only. For the sake of completion, we compare in Table 2 the performance of the two proposed algorithms with the performance of Kobayashi scheme [24]. Comparison is done with regard to the normalised correlation, PSNR, entropy and processing times. As shown in the table, our proposed algorithms achieve better encryption performance, and require less encryption and decryption times.

Table 3 Security services achieved by different crypto-based algorithms

Algorithm	Confidentiality	Authenticity	Integrity
the DICOM standard	header data only	pixel data only	pixel data only
Kobayashi scheme [24]	pixel data only	pixel data only	pixel data only
algorithm [42]	—	header and pixel data	header and pixel data
algorithm I	header and pixel data	header and pixel data	header and pixel data
algorithm II	header and pixel data	header and pixel data	header and pixel data

6 Discussion and conclusions

The proposed algorithms, as described throughout the paper, provide confidentiality, authenticity and integrity, for both the header and pixel data of DICOM images. This is a significant improvement that can be extended to the security profiles of the DICOM standard. That is, the standard provides confidentiality for a selected subset of header attributes through the mechanisms specified in the PS 3.15 basic application level confidentiality profile. However, it provides no mechanisms to achieve confidentiality of the pixel data. Similarly, the standard provides authenticity and integrity for the pixel data through its base digital signature profiles, however, it provides no authenticity and integrity mechanisms for the header data.

On the other hand, the DICOM-based algorithm proposed by Kobayashi *et al.* [24] provides authenticity and integrity for the pixel data, but not for the header data. As for confidentiality, encryption of the pixel data provides confidentiality, however, since the symmetric key is stored in the unprotected plain header, the privacy of the pixel data will be violated if the symmetric key is retrieved by intruders. Moreover, the algorithm does not provide confidentiality for the header data. Despite these limitations, a major contribution of the algorithm proposed by Kobayashi *et al.* [24] is the strong bond established between the pixel data and its security data. A summary of the comparison made above is shown in Table 3. The two proposed algorithms behave similarly in terms of achieving required security services.

Finally, it is worthwhile mentioning that an attempt to achieve the three security services for DICOM images has been reported by one of the authors in a crypto-based algorithm in [42]. The algorithm relies on the three cryptographic functions which have been used in the two proposed algorithms. A block diagram of the algorithm's encryption and signature creation procedure is shown in Fig. 13. The procedure adopts a closed-loop approach to generate the security data. The loop starts with the plain pixel data

and ends up with the encrypted pixel data. As shown in the figure, the procedure starts by hashing the pixel data to generate the encryption key and initialisation vector for the AES-GCM function to encrypt the confidential attributes of the header. This loop continues with hashing the encrypted header in order to generate the encryption key and the initialisation vector for the AES-GCM function. The loop is closed by encrypting the pixel data and generating the corresponding authentication tag. The encrypted hash codes are not stored in the DICOM header.

Compared with the algorithms presented in this paper, the algorithm [42] offers a stronger bond between the different entities of the algorithm and requires less storage space in the DICOM header. However, a thorough analysis of the algorithm has revealed a serious security flaw that leads to a complete loss of confidentiality for both the header and pixel data. The cause of the flaw is that the internally generated keys and initialisation vectors were sent in the DICOM header in clear (not encrypted). Therefore compared with the algorithms proposed in this paper, the algorithm reported in [42] achieves authentication and integrity of the header and pixel data of the DICOM images, whereas confidentiality is not achieved. The algorithm is compared with the DICOM standard and Kobayashi scheme in Table 3.

To conclude, two proposed crypto-based algorithms have been developed to provide confidentiality, authenticity and integrity for DICOM files exchanged between medical entities. Unlike the DICOM standard, and other DICOM-based cryptographic algorithms, the proposed algorithms provide the required security services for the pixel data as well as for the header data. Providing security services for the header is important since it contains confidential data which must be protected during transmission and verified at the receiving end before being used for diagnostic purposes. The algorithms were implemented using strong cryptographic primitives: AES-GCM, the whirlpool hash function and the ECDSA. Effective performance of the algorithms has been achieved as reflected by the results obtained for correlation, entropy, PSNR, histogram analysis and robustness against signal processing attacks.

As an ongoing research, we are currently working on extending the proposed algorithms to deal with multi-slice and multi-frame DICOM medical images. For the future, we will incorporate a tamper localisation scheme to allow for content-based integrity rather than the strict-integrity functionality implemented by the current algorithms. Tamper localisation is a useful functionality because integrity control based on the exact preservation of all parts of the image may be unnecessarily strict as distortions on the image may also be due to noise originating from the transmission process.

7 References

- Craig, J., Patterson, V.: 'Introduction to the practice of telemedicine', *J. Telemed. Telecare*, 2005, **11**, pp. 3–9
- Raghupathi, W., Tan, J.: 'Strategic IT applications in health care', *Commun. ACM*, 2002, **45**, (12), pp. 56–61
- Ashley, R.: 'Telemedicine: legal, ethical and liability considerations', *J. Am. Diet. Assoc.*, 2002, **102**, (2), pp. 267–269
- McEvoy, F., Svalastoga, E.: 'Security of patient and study data associated with DICOM images when transferred using compact disc media', *J. Digit. Imaging*, 2009, **22**, (1), pp. 65–70
- Pianykh, O.: 'Digital imaging and communications in medicine (DICOM)' (Springer-Verlag, Berlin Heidelberg, 2012)
- 'Digital imaging and communications in medicine (DICOM) standard, DICOM', 2006. Available at <http://medical.nema.org/dicom/2006/>
- 'Digital imaging and communications in medicine (DICOM), part 15: security profiles ed.', National Electrical Manufacturers Association (NEMA), 2001, PS 3.15–2001
- Buchmann, J.: 'Introduction to cryptography' (Springer-Verlag, New York, 2001)
- Cox, I.J., Miller, M.L., Bloom, J.A.: 'Digital watermarking' (Morgan Kaufmann, San Francisco, CA, 2002), pp. 26–36
- Hartung, F., Kutter, M.: 'Multimedia watermarking techniques'. Proc. of IEEE, July 2006, vol. 87, no. 7, pp. 1069–1107
- Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R.: 'Relevance of watermarking in medical imaging'. Proc. of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, Arlington, USA, November 2000, pp. 250–255

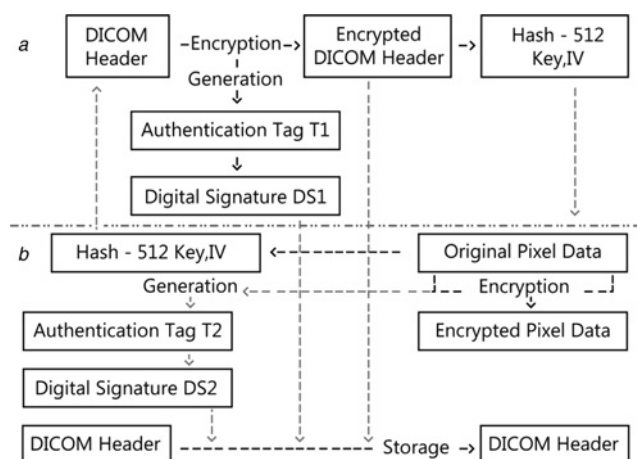


Fig. 13 Encryption and signature creation procedure of algorithm [42]

- 12 Coatrieux, G., Lecornu, L., Sankur, B., Roux, Ch.: 'A review of image watermarking applications in healthcare'. Proc. of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, New York, USA, 2006, pp. 4691–4694
- 13 Coatrieux, G., Maitre, H., Sankur, B.: 'Strict integrity control of biomedical images'. Proc. of SPIE Security Watermarking Multimedia Contents III, SPIE 2001, San Jose, CA, January 2001, vol. 4314, pp. 229–240
- 14 Giakoumaki, A., Pavlopoulos, S., Koutsouris, D.: 'Multiple image watermarking applied to health information management', *IEEE Trans. Inf. Technol. Biomed.*, 2006, **10**, (4), pp. 722–732
- 15 Giakoumaki, A., Pavlopoulos, S., Koutsouris, D.: 'Secure and efficient health data management through multiple watermarking on medical images', *Med. Biol. Eng. Comput.*, 2006, **44**, (8), pp. 619–631
- 16 Thodi, D., Rodriguez, J.: 'Expansion embedding techniques for reversible watermarking', *IEEE Trans. Image Process.*, 2007, **16**, (3), pp. 721–730
- 17 Celik, M., Sharma, G., Tekalp, M., Saber, E.: 'Lossless generalized-LSB data embedding', *IEEE Trans. Image Process.*, 2005, **14**, (2), pp. 253–266
- 18 Celik, M.U., Sharma, G., Tekalp, A.M.: 'Lossless watermarking for image authentication: a new framework and an implementation', *IEEE Trans. Image Process.*, 2006, **15**, (4), pp. 1042–1049
- 19 Liew, S., Zain, J.: 'Tamper localization and lossless recovery watermarking scheme', *Commun. Comput. Inf. Sci.*, 2011, **179**, (1), pp. 555–566
- 20 Guo, X., Zhuang, T.: 'Lossless watermarking for verifying the integrity of medical images with tamper localization', *J. Digit. Imaging*, 2009, **22**, (6), pp. 620–628
- 21 Osamah, M., Khoo, B.: 'Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images', *J. Digit. Imaging*, 2011, **24**, (1), pp. 114–125
- 22 Guo, X., Zhuang, T.: 'A region-based lossless watermarking scheme for enhancing security of medical data', *J. Digit. Imaging*, 2009, **22**, (1), pp. 53–64
- 23 Su, P.C., Wang, H.J., Kuo, C.C.J.: 'Digital image watermarking in regions of interest'. Proc. of the IS&T Conf. on Image Processing, Image Quality, Image Capture Systems, Savannah, GA, 1999, pp. 295–300
- 24 Kobayashi, L., Furuie, S., Barreto, P.: 'Providing integrity and authenticity in DICOM images: a novel approach', *IEEE Trans. Inf. Technol. Biomed.*, 2009, **13**, (4), pp. 582–589
- 25 Kobayashi, L., Furuie, S.: 'Proposal for DICOM multiframe medical image integrity and authenticity', *J. Digit. Imaging*, 2011, **24**, (1), pp. 114–125
- 26 Bernarding, J., Thiel, A., Grzesik, A.: 'A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption', *Int. J. Med. Inf.*, 2001, **64**, pp. 429–438
- 27 Acharya, U.R., Bhat, P.S., Kumar, S., Min, L.C.: 'Transmission and storage of medical images with patient information', *Comput. Biol. Med.*, 2003, **33**, pp. 303–210
- 28 'The Health Insurance Portability and Accountability Act (HIPAA), March 2009'. Available at <http://www.hhs.gov/ocr/privacy/index.html>
- 29 'Security and privacy: an introduction to HIPAA, privacy and security committee, medical imaging informatics section', NEMA. Available at <http://medical.nema.org/privacy/privacy.html>
- 30 'Digital imaging and communications in medicine (DICOM) supplement 55: attribute level confidentiality DICOM standards committee', Rosslyn, VA, 5 September 2002 Security Supplement. Available at <http://medical.nema.org/>
- 31 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)
- 32 Bendel, M.: 'Hackers describe PS3 security as epic fail, gain unrestricted access', Exophase.com, 2010
- 33 Shiguo, L., Zhongxuan, L., Zhen, R., Haila, W.: 'Commutative encryption and watermarking in video compression', *IEEE Trans. Circuits Syst. Video Technol.*, 2007, **17**, (6), pp. 774–778
- 34 Puech, W., Rodrigues, J.M.: 'A new crypto-watermarking method for medical images safe transfer'. Proc. of 12th European Signal Processing Conf., Vienna, Austria, September 2004, pp. 1481–1484
- 35 Zhou, X.Q., Huang, H.K., Lou, S.L.: 'Authenticity and integrity of digital mammography images', *IEEE Trans. Med. Imaging*, 2001, **20**, (8), pp. 784–791
- 36 Chao, H., Hsu, C., Miaou, S.: 'A data-hiding technique with authentication, integration, and confidentiality for electronic patient records', *IEEE Trans. Inf. Technol. Biomed.*, 2002, **6**, (1), pp. 46–53
- 37 Dworki, M.: 'Recommendation for block cipher modes of operation: Galois/countermode (GCM) and GMAC' (NIST Special Publication, 800–38D, 2007)
- 38 Gueron, S.: 'AES-GCM for efficient authenticated encryption – ending the reign of HMAC-SHA-1?'. Workshop on Real-World Cryptography, Stanford University, USA, 2013
- 39 Barreto, P., Rijmen, V.: 'The WHIRLPOOL Hashing Function', Available at <http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip>, 2003
- 40 Caelli, W., Dawson, E., Rea, S.: 'Elliptic curve cryptography, and digital signatures', *Comput. Sec.*, 1999, **18**, (1), pp. 47–66
- 41 Prabhadevi, S., Natarajan, A.: 'A comparative study on digital signatures based on elliptic curves in high speed ad hoc networks', *Aust. J. Basic Appl. Sci.*, 2014, **8**, (2), pp. 1–6
- 42 Al-Haj, A.: 'Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM Images', *J. Digit. Imaging*, 2015, **28**, (2), pp. 179–187, doi: 10.1007/s10278-014-9734-8