Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 90 (2016) 175 – 181

Procedia Computer Science

International Conference On Medical Imaging Understanding and Analysis 2016, MIUA 2016, 6-8 July 2016, Loughborough, UK

Security of multi-frame DICOM images using XOR encryption approach

Q. N. Natsheh*, B. Li, A. G. Gale

Department of Computer Science, Loughborough University, Epinal Way, Loughborough, Leicestershire LE11 3TU, United Kingdom

Abstract

Transferring medical images using networks is subjected to a wide variety of security risks. Hence, there is a need of a robust and secure mechanism to exchange medical images over the Internet. The Digital Image and Communication in Medicine (DICOM) standard provides attributes for the header data confidentiality but not for the pixel image data. In this paper, a simple and effective encryption approach for pixel data is provided for multi-frame DICOM medical images. The main goal of the proposed approach is to reduce the encryption and decryption time of these images, using Advanced Encryption Standard (AES) where only one image is encrypted and XOR cipher for encrypting the remaining multi-frame DICOM images. The proposed algorithm is evaluated using computational time, normalized correlation, entropy, Peak-Signal-to-Noise-Ratio (PSNR) and histogram analysis. The results show that the proposed approach can reduce the encryption and decryption time and is able to ensure image confidentiality.

Peer-review under responsibility of the Organizing Committee of MIUA 2016

Keywords: DICOM; confidentiality; XOR cipher; AES; medical images encryption.

1. Introduction

The massive progress in network communications over the past decade has established a great demand for secure image transmission over networks. Medical imaging represents one important field where securing data transmission is crucial especially with the raise of eHealth and mHealth applications. To provide secure transmissions and communications, the DICOM standard was developed by the American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA) [1]. DICOM is a compatible framework that provides mechanisms for storing, retrieving and transmission of most types of medical images produced by medical imaging equipment from different manufactures.

* Corresponding author. *E-mail address:*q.natsheh@lboro.ac.uk

Peer-review under responsibility of the Organizing Committee of MIUA 2016
doi:10.1016/j.procs.2016.07.018

A DICOM file consists of two parts: a Header Data which is a textual data format that stores the patients' information and clinical data such as name, scan image type, pixel array attributes such as pixel depth, etc., and Pixel Data which can be an image, short video or audio. DICOM provides confidentiality mechanisms for header data but not for the image pixel data. Accordingly, many researchers have addressed DICOM security utilising approaches that guarantee security robustness and reduce computational time[2]. DICOM supports a wide variety of digital medical images, such as the magnetic resonance images (MRI) and Computed Tomography (CT), which demand a large storage capacity and transmission bandwidth if they are treated as textual data[3]. Moreover, encrypting and decrypting the medical images pixel data increases the required computational time. Hence; it is important to reduce the encryption and decryption computational time.

Encryption algorithms can be classified into several categories depending on different rules such as function (Naïve, selective), key (symmetric, asymmetric), and size (stream, block). Naïve and selective encryption approaches are the two classes of pixel-based encryption for medical image encryption [2, 4]. The Naïve approach is a simple approach that is used to encrypt all pixels of the image, while the selective approach is more complicated and it encrypts selected image parts depending on segmentation of the image density, e.g. a Region Of Interest (ROI). The selective approach has a better computational time than the Naïve approach but on the other hand the naïve approach is considered to be more robust[2].

Ou et al.[5] proposed two schemes of the selective approach to gain secure access for DICOM images. The first scheme relies on random scrambling of bits in a subset that belongs to a ROI. While the second scheme utilised AES to encrypt sub-regions in the images. Belazi et al.[6] proposed a selective encryption scheme utilising substitution box, Discrete Wavelet Transform (DWT) and chaotic permutation. In Mahmood et al.[2] a hybrid encryption method was implemented to reduce the computational time of the AES, the proposed method applied the AES on the ROI, while the Region Of Background (ROB) is encrypted using a coding method such as Gold Code (GC). Although this selective algorithm can reduce the processing time, it also degrades the level of robustness, due to its poor error tolerance. Identifying ROI and ROB requires feature extraction, template matching and sometimes a pre-knowledge about the problem (i.e. training data). Accordingly, those methods are more complicated and require some pre-knowledge. On the other hand, the integration of simple encryption approaches such as Chaos Maps with more sophisticated encryption algorithms has a good potential to reduce the computational time.

Nag et al.[7] used the affine transform technique with four 8-bit keys to reposition the image's pixels, and then encrypted each (2×2) pixel block of the transformed image with XOR operation in two stages. The overall size of the key is 64 bits which strengthens the security level[7]. According to Xiang et al.[8] and Yu et al.[9] a chaotic encryption approach was proposed in which a circular bit shift mechanism permutes the plaintext block, after which the XOR cipher was utilised to encrypt every block. Li et al.[10] criticised Xiang et al.[8] and Yu et al.[9] after performing a cryptanalytic test, and found that the two schemes cannot resist against the differential known-plaintext and chosen-plaintext attacks. Li et al.[10] proposed doing further enhancement to the two approaches to be efficient in a required high level of security. Accordingly; Xu et al.[11] enhanced Xiang et al.[8] and Yu et al.[9] approaches by replacing the random number sequence generator (logistic map) with Chen's Chaotic System (CCS), and the plaintext permuted byte by byte instead of block by block, and then the modified plaintext is XORed in the inverse order of the permutation, this step has been performed to overcome the differential known-plaintext attack. A disturbance given to the CCS by the last obtained encrypted byte has been done to overcome the chosen-plaintext attack. In other words, utilize XOR with small key block (static key) prone to differential known-plaintext and chosen-plaintext attacks and this problem can be overcome by introducing variation in the plaintext or the key. Moreover, François et al.[12] proposed an encryption algorithm based on XOR operation coupled with a linear chaotic function. The benefit of that method is its resistance to the brute force attack because of the large key space produced.

Recently, many approaches of image encryption have been introduced through random and chaotic processes functions. In this paper, a simple encryption approach using XOR cipher and AES with two different key variations is proposed for multi-frame DICOM images. The proposed approach aim to reduce the computational time of multi-frame DICOM images encryption and decryption. Statistical analysis of the proposed approach is performed on the cipher image to assess the encryption/decryption performance.

The rest of the paper is organised as follows. The proposed approach is described in section 2. Performance analysis and discussion of the proposed approach is presented in section 3. Finally, section 4 reports the conclusion and introduces the future work.

2. The proposed encryption approach

2.1. XOR cipher

The Exclusive OR (XOR) logical function can be applied to binary bits. Also, it is a fundamental encryption cipher that is well known for its simplicity. The XOR cipher is a symmetric encryption algorithm[13]. The basic idea of the XOR cipher is derived from Boolean algebra XOR function that returns 'true' when the two arguments have different values. In the encryption context, the strength of the XOR cipher depends on the length and the nature of the key. The XOR cipher with a lengthy random key can achieve better security performance[14]. Also, large XOR keys increase unpredictability and can confront brute-force attack[15].

2.2. XOR-AES based encryption

The approach adopted in this paper aims to reduce the encryption/decryption time using XOR cipher and AES. AES has a high reputation as a robust encryption algorithm. Moreover, it is adopted by the DICOM standard[16]. The proposed solution uses the first image in the multi-frame DICOM images as XOR key or a randomly generated key that has the same dimension as the unified frames size. Fig. 1 illustrates the proposed approach where the first image (image A) is used as XOR key to encrypt the rest of the images in the multi-frames (image B and image C), or a 16 bits grayscale random image, as XOR key, is generated based on the frame size to encrypt the multi-frame DICOM images. Fig. 2 illustrates the decryption process. The second step of the approach is to encrypt the key (first image in the multi-frame or the random generated image) using AES with Counter (CTR) mode of operation. Both approach key-variations are compared with the Naive encryption where all multi-frame DICOM images is encrypted using AES.

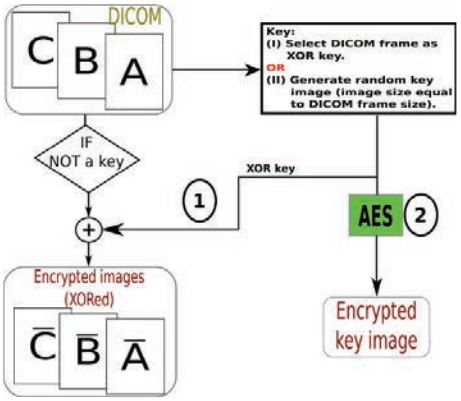

Fig. 1. Proposed approach (encryption)

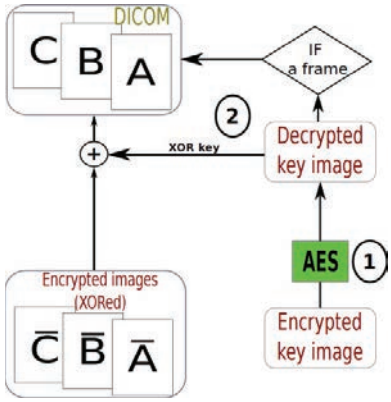

Fig. 2. Proposed approach (decryption)

The pseudocode of the XOR encryption with DICOM frame key is presented in Table 1, while Table 2 presents the pseudocode of the XOR encryption with random key. Each frame is converted into plaintext, while the key image will be segmented into 32 bytes (key block). Each key block will be used as a key to encrypt **N** plaintext block. In other words, if the length of the plaintext is 49152 bytes (after two stages of padding) and the length of the random image (key) is 1536 bytes, then the key image will be segmented into 32 bytes blocks where each key block will be used to encrypt 1024 bytes from the plaintext after two stages of padding as shown in pseudocode (Table 1 and Table 2).

3. Performance analysis and discussion

Experimental evaluation was performed over a benchmark set of 60 frames MRI Neoadjuvant Chemotherapy (NACT) breast cancer DICOM images, where each frame has 256×256 pixels with a depth of 16 bits[17]. The experiment was conducted using Python on Ubuntu machine (intel i5 at 2.27 GHz). The proposed approach was evaluated using performance metrics with regard to confidentiality requirement. Confidentiality efficiency is guaranteed if the cipher image is highly uncorrelated to the original image. Broadly speaking, the evaluation metrics can be classified into two groups. The first group estimates the substitution efficiency between the original and the encrypted image such as the PSNR, histogram, entropy, and correlation coefficients. Those measurements are used to evaluate the correlation between the cipher and plain image to ensure the confidentiality requirement. The second group estimates diffusion features of the image encryption algorithm such as the mean absolute error (MAE) [14].

The multi-frame MRI images are encrypted using a Naive approach, for comparison with the proposed approach, where all frames can be encrypted using AES cipher with different operational modes. However, most security experts recommended AES in CTR mode as it's suitable for large data size and it can be parallelised[18]. Consequently, the AES with CTR operational mode is utilized for the proposed approach.

Table 1. XOR encryption with DICOM frame key pseudocode.

Algorithm 1 XOR Encryption with DICOM Frame key

```
procedure MULTI-FRAME DICOM IMAGE ENCRYPTION
    M ← Number of Frames
Select first DICOM frame as XORKey
    KeyImage ← Select( DICOM frame)
    KeyByte ← ToByte( keyImage )
    Keylen ← length( keyByte )
XOR Encryption:
    for x = 1 To M do
        while Frame(x) ≠ Key do
            Pixels(matrix) ← PixelData( DICOM )
            width ← GetWidth( DICOM )
            height ← GetHeight( DICOM )
            Plaintextlen ← height × width
            XORkeylen = 32 Bytes
            Breakup PixelData into a single String:
            l = 0
            for i = 0 To width do
                for j = 0 To height do
                    Plaintext(l) ← Pixels(i , j)
                    l ← l + 1.
            Padding (for XOR block):
            while length(Plaintext)%16 ≠ 0 do
                Plaintext = Plaintext + 'n'
            N = Keylen/XORkeylen
            Padding (to match the XOR key (XORkeylen)):
            while length(Plaintext)%N ≠ 0 do
                Plaintext = Plaintext + 'n'
            Plaintextlen ← Length (Plaintext)
            Encryption
            for i = 0 To N do
                XorEncrypt(Plaintext(i*N:i*N+N), KeyByte(i*32:i*32+32))
Key Encryption:
        KeyEncryption(AES/CTR, KeyImage)
```

Table 2. XOR encryption with random key pseudocode.

Algorithm 2 XOR Encryption with Random key

```
procedure MULTI-FRAME DICOM IMAGE ENCRYPTION
    M ← Number of Frames
Generate Random KeyImage
    width ← GetWidth( DICOM )
    height ← GetHeight( DICOM )
    KeyImage ← GenerateImage( width, height)
    KeyByte ← ToByte( keyImage )
    Keylen ← length( keyByte )
XOR Encryption:
    for x = 1 To M do
        Pixels(matrix) ← PixelData( DICOM )
        width ← GetWidth( DICOM )
        height ← GetHeight( DICOM )
        Plaintextlen ← height × width
        XORkeylen = 32 Bytes
        Breakup PixelData into single String:
        l = 0
        for i = 0 To width do
            for j = 0 To height do
                Plaintext(l) ← Pixels(i , j)
                l ← l + 1.
        Padding (for XOR block):
        while length(Plaintext)%16 ≠ 0 do
            Plaintext = Plaintext + 'n'
        Padding (to match the XOR key (XORkeylen)):
        while length(Plaintext)%N ≠ 0 do
            Plaintext = Plaintext + 'n'
        Plaintextlen ← Length (Plaintext)
        Encryption
        for i = 0 To N do
            XorEncrypt(Plaintext(i*N:i*N+N), KeyByte(i*32:i*32+32))
Key Encryption:
        KeyEncryption(AES/CTR, KeyImage)
```

The following measurements are used to evaluate the correlation between the original and encrypted images:

PSNR: this measurement is used to evaluate how much the original and the encrypted images are similar. So a low value of PSNR attained as shown in Table 3 is (28.20 dB) using XOR with random key and it is (28.24 dB) with MRI frame as a key indicates that the two images are uncorrelated, and subsequently the confidentiality is accomplished.

Normalized correlation: this is the similarity degree measurement. If the correlation factor for the completely different images is very close to zero then this is an efficiency indicator of the encryption algorithm, but if the factor is equal to one, this indicates that the original and encrypted images are identical, and so indicates inefficiency[19].

The correlation ratios calculated between encrypted and plain images as shown in Table 3 using XOR with random key is (- 0.0000096) and it is (0.0000078) using XOR with MRI frame key indicate a weak correlation between encrypted and plain image.

Entropy: this is the randomness measurement by which confidentiality can be achieved on the encrypted image with a high degree of entropy[20]. The entropy obtained by the XOR with random key is (7.3687 bits/pixel) as shown in Table 3, and it is (7.4710 bits/pixel) for image encrypted with MRI frame XOR key, while the entropy of the encrypted image in the Naive approach is (7.3626 bits/pixel). This indicates a higher level of randomness achieved by the proposed approach in comparison to the Naive approach.

The best performance results were achieved by the proposed approach using random generated key from confidentiality perspectives. It requires shorter encryption/decryption time compared with the other approaches as shown in Table 3.

Table 3. Encryption/decryption time and confidentiality metrics for the proposed and Naive approach.

Key/ Metrics	**Encryption time (*sec*)***	**Decryption time (*sec*)***	**PSNR (*dB*)**	**Normalized correlation**	**Entropy (*bits/pixel*)**
MRI DICOM frame XOR key	101.065	86.365	28.24	0.0000078	7.4710
Random generated XOR key	90.14	88.88	28.20	- 0.0000096	7.3687
AES_CTR (Naive)	144.712	132.45	28.32	0.00047	7.3626

* The reported encryption/decryption time is an average value of 4 run times.

Histogram: this metric helps in distinguishing the correlation between the original and the encrypted images by showing each grey level probability. Subsequently, if the difference between the original and encrypted images is large; the images are highly uncorrelated. Moreover, if the grey level probabilities are distributed uniformly; the attacker cannot predict enough information to make statistical attack[21]. Fig. 3 (a) shows the plain image while Fig. 3 (d) shows its histogram. Fig. 3 (b) shows the encrypted image using MRI frame as XOR key, while Fig. 3 (e) indicates its histogram. Fig. 3 (c) shows the encrypted image using XOR with random key, while Fig. 3 (f) shows its histogram.

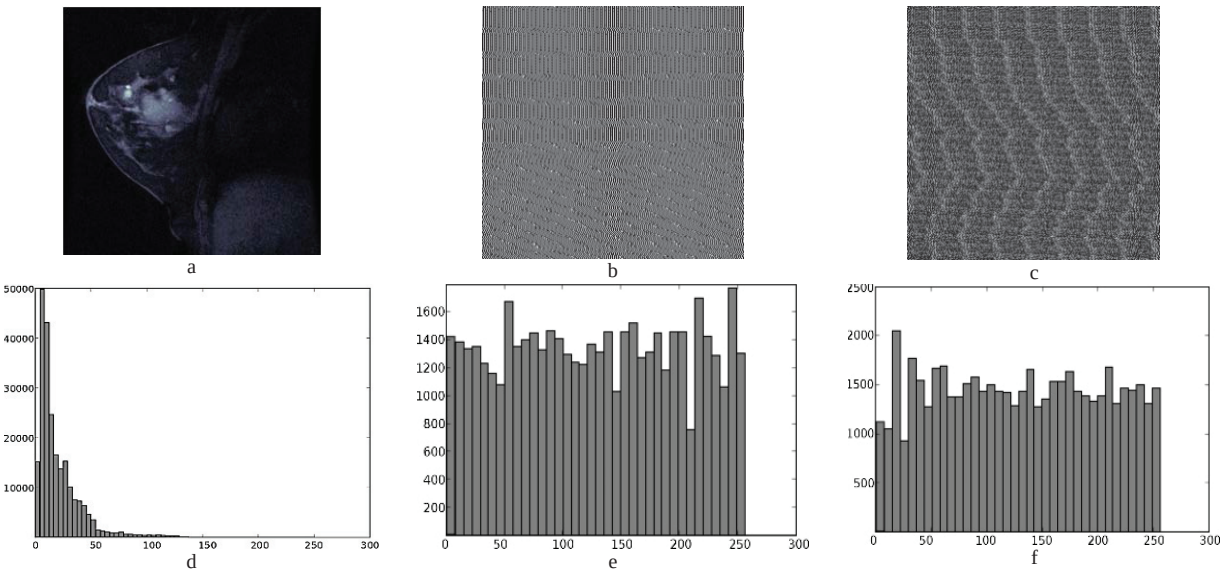

Fig. 3. (a) the original image; (b) the encrypted image (frame key); (c) the encrypted image (random key); (d) histogram of the original image; (e) histogram of the encrypted image (frame key); (f) histogram of the encrypted image (random key).

4. Conclusions and future work

The proposed approach provides confidentiality of pixel data of multi-frame DICOM images. These initial results in this study, evaluated by the correlation, PSNR, entropy and histogram analysis, illustrate the effectiveness of the proposed approach. Medical image confidentiality was achieved while reducing the encryption/decryption time. This goal was achieved by utilising the XOR cipher. The XORs' keys were generated randomly or by using one frame from the multi-frame medical images. The encryption approach based on a random key provides better performance and shorter encryption/decryption time than Naive approach. In future work, chaotic crypto-based algorithm will be utilized to permute images' pixel data of XOR encrypted images so as to ensure higher confidentiality by increasing the level of randomness. Moreover, level of variation in the proposed approach can be simply increased by randomly selecting a frame or combination of different random frames as the XOR key for the encryption process.

Acknowledgements

I would like to express my appreciation to Lamya Abdullah for her support and cooperation.

References

1. 'National Electrical Manufacturers Association, Digital imaging and communications in medicine (DICOM), NEMA Standards Publication, PS3.6-1993,', NEMA: Washington, 1993., Technical report, NEMA.
2. Mahmood, A.; Dony, R. & Areibi, S. (2013), An adaptive encryption based genetic algorithms for medical images, in '2013 IEEE International Workshop on Machine Learning for Signal Processing (MLSP)', pp. 1-6.
3. Hu, J. & Han, F. (2009), 'A pixel-based scrambling scheme for digital medical images protection', Journal of Network and Computer Applications 32(4), 788 - 794.
4. Jeyamala Chandrasekaran, S. J. T. (2015), 'Ensemble of Chaotic and Naive Approaches for Performance Enhancement in Video Encryption', The Scientific World Journal 2015, 11.
5. Ou, Y.; Sur, C. & Rhee, K. H.Preparata, F. P. & Fang, Q., ed., (2007), Frontiers in Algorithmics: First Annual International Workshop, FAW 2007, Lanzhou, China, August 1-3, 2007. Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, chapter Region-Based Selective Encryption for Medical Imaging, pp. 62--73.
6. Belazi, A.; El-Latif, A. A. A.; Rhouma, R. & Belghith, S. (2015), Selective image encryption scheme based on DWT, AES S-box and chaotic permutation, in '2015 International Wireless Communications and Mobile Computing Conference (IWCMC)', pp. 606-610.
7. Nag, A.; Singh, J. P.; Khan, S.; Ghosh, S.; Biswas, S.; Sarkar, D. & Sarkar, P. P. (2011), Image encryption using affine transform and XOR operation, in 'Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on', pp. 309-312.
8. Xiang, T.; Liao, X.; Tang, G.; Chen, Y. & wo Wong, K. (2006), 'A novel block cryptosystem based on iterating a chaotic map ', Physics Letters A 349(1вЂ“4), 109 - 115.
9. Yu, W. & Cao, J. (2006), 'Cryptography based on delayed chaotic neural networks', Physics Letters A 356, 333-338.
10. Li, C.; Li, S.; Alvarez, G.; Chen, G. & Lo, K.-T. (2007), 'Cryptanalysis of two chaotic encryption schemes based on circular bit shift and operations',
11. Xu, S.-J.; Chen, X.-B.; Zhang, R.; Yang, Y.-X. & Guo, Y.-C. (2012), 'An improved chaotic cryptosystem based on circular bit shift and operations',
12. François, M.; Grosges, T.; Barchiesi, D. & Erra, R. (2012), 'A new image encryption scheme based on a chaotic function', Signal Processing: Image Communication 27(3), 249 - 259.
13. Churchhouse, R. (2002), Codes and Ciphers: Julius Caesar, the Enigma and the Internet,, Cambridge: Cambridge University Press,ISBN 978-0-521-00890-7.
14. Abd El-Samie, F. E.; Ahmed, H. E. H.; Elashry, I. F.; Shahieen, M. H.; Faragallah, O. S.; El-Rabaie, E.-S. M. & Alshebeili, S. A. (2013), Image Encryption: A Communication Perspective, CRC Press, Inc., Boca Raton, FL, USA.
15. Kumar, A. and Ghose, M.K., 2011. Extended substitution–diffusion based image cipher using chaotic standard map. Communications in Nonlinear Science and Numerical Simulation, 16(1), pp.372-382. .
16. National Electrical Manufacturers Association, "Digital Imaging and Communications in Medicine (DICOM) Part 15 Security and System Management Profiles," http://medical.nema.org/dicom/2004/04 15PU.PDF, 2004.
17. David Newitt, Nola Hylton, "Single site breast DCE-MRI data and segmentations from patients undergoing neoadjuvant chemotherapy", The Cancer Imaging Archive (2016). doi:10.7937/K9/TCIA.2016.QHsyhJKy.
18. MULUALEM, G. M. (2015s), 'COMPRESSION AND ENCRYPTION FOR SATELLITE IMAGES: A COMPARISON BETWEEN SQUEEZE CIPHER AND SPATIAL SIMULATIONS', PhD thesis, Faculty of GeoInformation Science and Earth Observation of the University of Twente.

19. Borujeni, Shahram Etemadi, E. M. (2009), 'Chaotic image encryption design using Tompkins-Paige algorithm.', Mathematical Problems in Engineering 2009, Article ID 762652, 22 p.-Article ID 762652, 22 p..
20. Al-Haj, A., 2015. Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. Journal of digital imaging, 28(2), pp.179-187. .
21. Zhang, G. and Liu, Q., 2011. A novel image encryption method based on total shuffling scheme. Optics Communications, 284(12), pp.2775-2780..