An Efficient Solution to Secure Embedded Information in DICOM Images for Telemedicine

Tuan T. Nguyen, Luan M. Tran, Ngoc C. Nguyen, and Thuong T. Le

Abstract

Digital Imaging and Communications in Medicine (DICOM) is an international data standard used worldwide to store and transmit various medical images. In addition to the image pixel data, DICOM files also consist of private information and other important information for diagnosis. However, they are easily modified, and alterations are not detectable with current DICOM file format. Consequently, the security of this kind of data over the Internet arises more challenges. This paper presents an efficient solution to secure embedded information in DICOM images by exploiting different techniques of data encoding, encryption and watermarking. Firstly, the proposed method encodes personal information, encrypts it and then embeds it into the DICOM images by two secret keys to increase the security. After that, personal information is removed from the DICOM images. As a result, medical images are still handled in both normal mode and secure mode without leakage of personal information. Finally, the experimental results on different medical images demonstrate the imperceptibility, capacity and efficiency of the proposed design to discuss its use in telemedicine.

Keywords

Embedded information • Encryption • Watermarking • DICOM • Telemedicine

1 Introduction

The terminology "telemedicine" was defined as the delivery of healthcare services from a distance using information and communication technologies. These technologies have facilitated the exchange of digital data and images between patients and medical staff through remote connection devices [1]. Meanwhile, DICOM, which stands for Digital Imaging and Communications in Medicine, is a set of industrial standards progressing in the demand of connecting, storing, exchanging and printing medical images. Various modalities such as CT (Computed Tomography), MR (Magnetic Resonance), US (Ultra Sound), DX (Digital Radiography), and so on are accompanied by a table that meets the DICOM standards to clarify the service classes that these devices support. DICOM has gradually gained widespread acceptance in hospitals and clinics. Nowadays, the management of this standard system belongs to DICOM Standards Committee consisting of many large companies operating in manufacturing medical devices and health organizations in North America, Japan and Europe. DICOM is also ISO 12052:2006 standard.

A DICOM file is not only a type of image data but also contains information relating to patients and modalities that create the images. It has a.dcm extension and consists of a number of information attributes with different data types and one special attribute containing image pixel data up to 65,536 (16 bits) grayscales for excellent image quality [2].

The rapid progress of digital imaging technique and Internet brings convenience to remote medical treatment, diagnosis and academic exchange, and effectively solves the problem of uneven distribution of medical resources. However, the individualized medical information sharing over public networks may violate the privacy of the patient. In order to improve information security, many different kinds of solutions have been developed so far, but mostly for non-DICOM images. Hence, the paper focuses on information security in DICOM medical images. It means that the embedded image is still compatible with the DICOM standard. The rest of this paper is organized as follows. Literature review in various technologies used to maintain medical image security, such as encryption and watermarking is included in Sect. 2. In Sect. 3, the new solution to secure embedded information in DICOM images is introduced and

T. T. Nguyen (✉) · L. M. Tran · N. C. Nguyen · T. T. Le
Ho Chi Minh City University of Technology (VNU-HCM),
268 Ly Thuong Kiet, Dist. 10, Ho Chi Minh City, Vietnam
e-mail: nttuan@hcmut.edu.vn

V. Van Toi et al. (eds.), *7th International Conference on the Development of Biomedical Engineering in Vietnam (BME7)*, IFMBE Proceedings 69, https://doi.org/10.1007/978-981-13-5859-3_76

analyzed. Experimental results are implemented on various medical images to evaluate the imperceptibility, capacity and efficiency of the proposed method. Section 4 summarizes and concludes the paper.

2 Literature Review

Patient information such as name, age, sex, date of birth, identification information, and so on is formatted in some DICOM common tags, specifically in group "0010". Data may or may not be displayed on the screen, but anyone can also extract this kind of private information from those tags when accessing to the DICOM file. A simple and easy method to secure patient information is to convert and export the DICOM file into common image formats such as PNG (Portable Network Graphics), TIFF (Tagged Image File Format) or JPEG (Joint Photographic Experts Group). However, all additional information excluding image data from original DICOM file will be lost. Moreover, the quality of resulting image may be degraded significantly due to the limitation of bit depth or the lossy compression of these image formats. Another solution is removing or replacing all patient information with "anonymization". It obtains the same quality of the resulting image due to keeping the DICOM format. However, private information is still not reconstructed from the resulting image so that it is only suitable for training purposes [3].

Therefore, some authors exploited the cryptography to obtain security with DICOM file such as Advanced Encryption Standard (AES). AES has a fixed block size, which has three levels of 128, 192 or 256 bits. It works on data managed in the form of matrices in the order of 4 × 4 byte principal column, called state. This technique is based on the combination of both substitutions and permutations as shown in Fig. 1, which has a great advantage in implementing both software and hardware [4].

However, applying encryption for whole DICOM file is not efficient because its size is extremely large. By contrast, encryption solution for only personal information in DICOM file may have latent errors because encrypted data can overlap with the control characters such as Patient Name (PN) tag and most DICOM patient information tags only support text characters as shown in Table 1. Moreover, encrypted data is completely not protected after decryption and easy to be realized, thus it may be hacked or simply removed by attackers.

Fig. 1 AES encryption and decryption algorithm

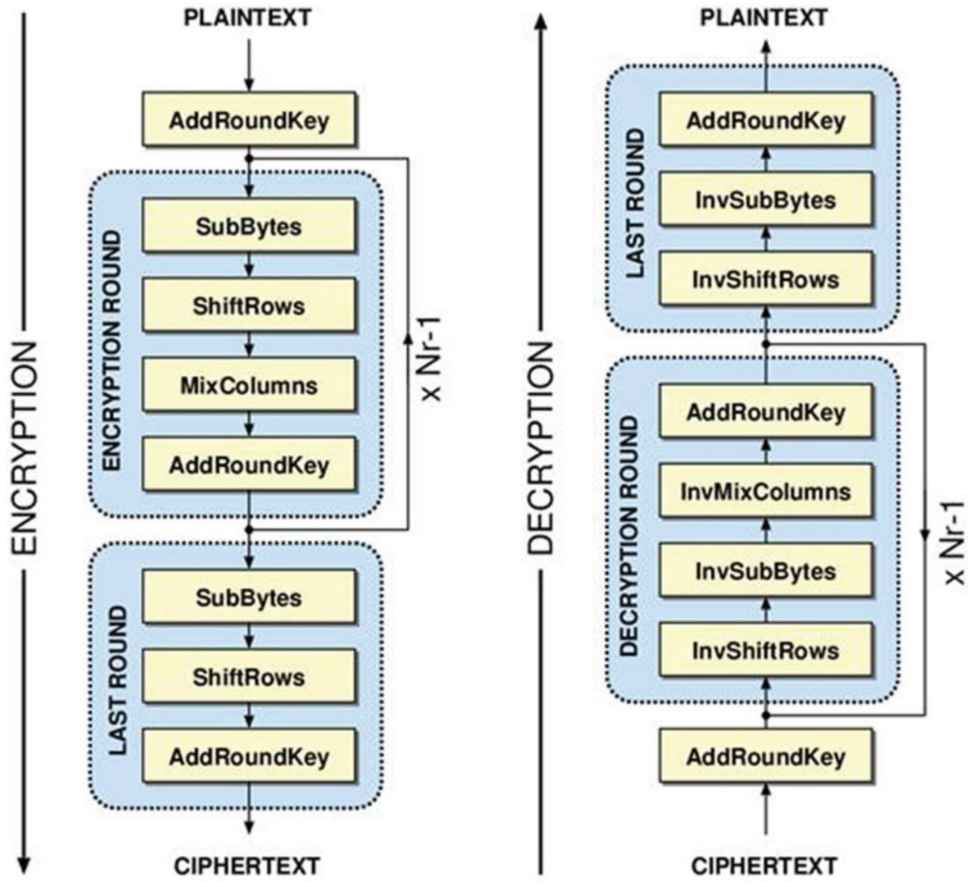


Table 1 Several patient information attributes

Tag	Name	VR	Character repertoire	Value
(0010, 0010)	Patient Name	PN	Excluding Control Characters LF, FF, and CR	64 chars maximum
(0010, 0020)	Patient ID	LO	Excluding Control Characters Except for ESC	64 chars maximum
(0010, 0030)	Patient's Birth Date	DA	YYYYMMDD: "0"–"9"	8 bytes fixed
(0010, 0032)	Patient's Birth Time	TM	HHMMSS.FFFFFF: Uppercase characters, "0"–"9", the SPACE character, and underscore "_"	16 bytes maximum
(0010, 0040)	Patient's Sex	CS	Uppercase characters, "0"–"9", the SPACE character, and underscore "_"	16 bytes maximum

To solve this problem, watermarking has recently been applied in the field of medicine for hiding information in medical image to increase usability. The advantage of watermarking technology is that it supports enhanced security, which cryptography simply cannot meet the need for secure medical data. By using digital watermarking with invisibility characteristics, the patient information as the watermark is hidden in medical images in order to ensure the transmission security on the Internet, and thus plays a role in protecting patient privacy [5–7].

Usually, medical image watermarking is to use traditional watermarking techniques to embed patient information in spatial domain [8] or transform domain [9]. Due to their simplicity and high capacity, Least Significant Bit (LSB) algorithms are the most studied in watermarking [10]. However, these methods are not secure, because no encryption technique is used for embedding information in images. In order to improve the security, some solutions exploit a private key from a pseudo random number generator to determine the pixels used for embedding [11]. Unfortunately, most proposed methods are applied for non-DICOM images. To overcome the above issues, our research on design of a new solution to secure embedded information in DICOM images for telemedicine applications by exploiting different techniques of data encoding, encryption and watermarking. Especially, the resulting image is fully compatible with DICOM standard.

3 Proposed Method

The main steps of the proposed method for embedding personal information are presented as below:

Table 2 Implicit VR encoding

Group number	Element number	Value length	Value
2-byte	2-byte	4-byte L	L bytes

Step 1 Binary encoding personal information based DICOM data structure as shown in Table 2. It is implicit encoding where each data element consists of a tag that identifies the attribute, includes Group Number (2 bytes) and Element Number (2 bytes) and a Value Representation (VR) that describes the data type and format of the attribute value [2].

Step 2 AES encryption of binary data from step 1 with a secret key as shown in Fig. 1.

Step 3 Insertion of encrypted data into original image through LSB planes by another key. The LSB bits of each pixel in original image are replaced by bitstream of encrypted data. In this way, the embedded image is obtained as shown in Table 3. Finally, personal information is removed completely from DICOM tags.

Correspondingly, the extraction process is also implemented in three main steps:

Step 1 Extraction of encrypted data from embedded image through LSB planes by the same embedded key.

Step 2 AES decryption of binary data from step 1 with the same secret key in encryption as shown in Fig. 1.

Step 3 Decoding personal information based DICOM data structure as shown in Table 2.

As a result, with our method, in the normal mode, any physician can also view medical images with full support of DICOM standard without leakage of personal information, even if one key is known, while in the secure mode, personal information can only be extracted and decrypted to the user having the rights to access patient's complete data.

To measure the amount of visual quality degradation between original image $\boldsymbol{x}$ and embedded image $\boldsymbol{s}$, this paper uses the mean squared error (MSE) and the peak signal-to-noise ratio (PSNR), as shown in Eqs. (1) and (2), where b is bit depth of original image with $M \times N$ size.

Table 3 LSB watermarking algorithm

Original image (pixels)				Bitstream of data	Embedded image (pixels)			
				1 | 1 | 0 | 0 | …				
			LSB					LSB
…	1	0	1		…	1	0	1
…	0	0	0		…	0	0	1
…	1	1	1		…	1	1	0
…	0	1	0		…	0	1	0
…	…	…	…		…	…	…	…

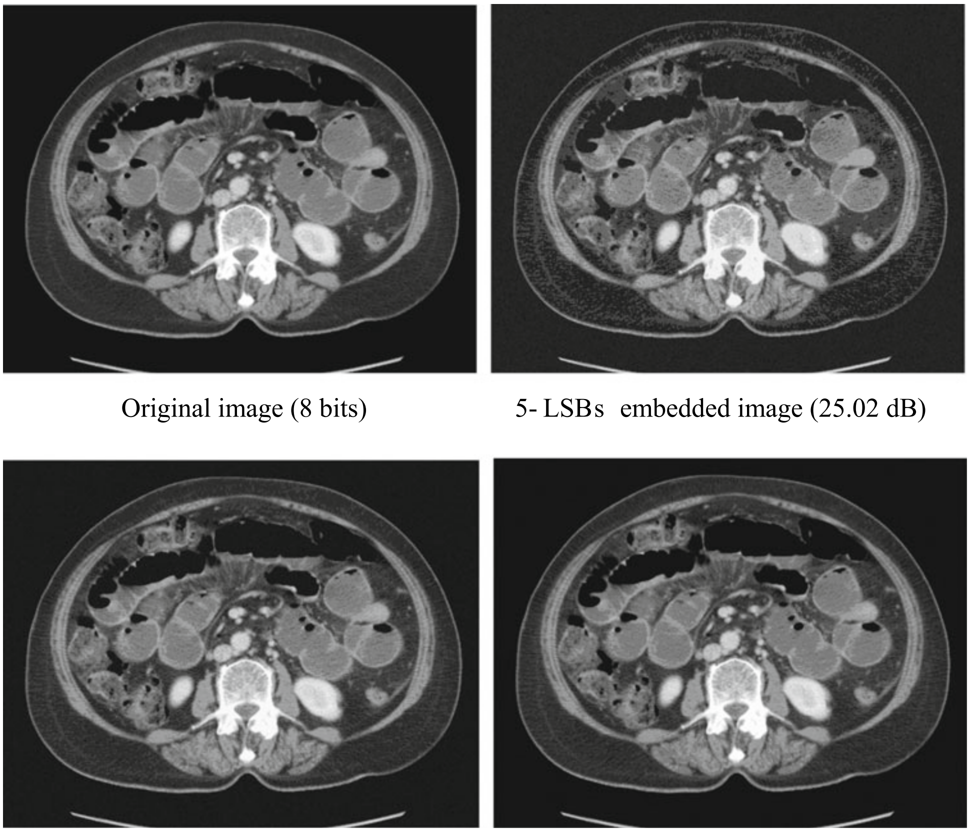
These measures are popular because they are simple to implement and it is relatively suitable to design systems.

$$MSE = \|\boldsymbol{s} - \boldsymbol{x}\| = \frac{1}{M.N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(s_{ij} - x_{ij}\right)^2 \qquad (1)$$

$$PSNR = 10\log_{10}\frac{\left(2^b - 1\right)^2}{MSE} \qquad (2)$$

It is clear that a good watermarking technique should have high *PSNR* value and low *MSE* value. It can be derived that *MSE* metric only depends on the number of embedded LSB planes, while *PSNR* also depends on bit depth of original image. It means that with the same *MSE*, the larger bit depth of image is, the better the quality of image obtains. Figure 2 shows the embedded images with different number of LSB planes corresponding with original CT image. Due to the effect of Human Visual System, the quality degradation of the embedded image is not perceptible in the case of using three LSB planes, somehow perceptible with four LSB planes and noticeable significantly for five LSB planes. Similaritily, the 3-LSBs embedded images corresponding with original images of US, DX and MR are shown in Figs. 3, 4 and 5. From these results, it can be derived that the *PSNR* should be more than around 37 dB in order to obtain the imperceptible embedded image.

Fig. 2 Original CT image and embedded images with different number of LSB planes

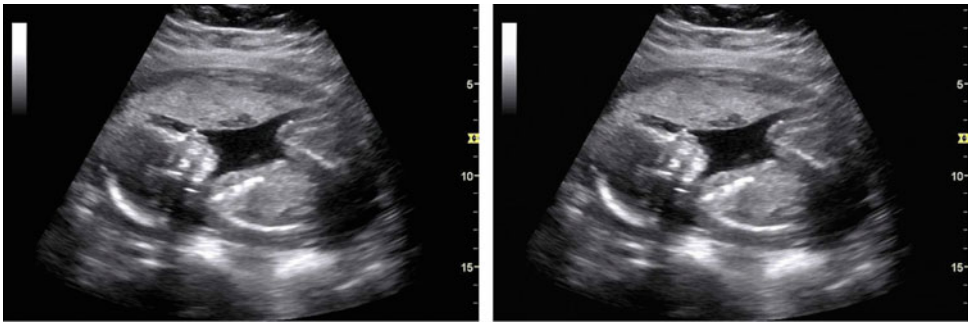


Original image (8 bits)

5- LSBs embedded image (25.02 dB)

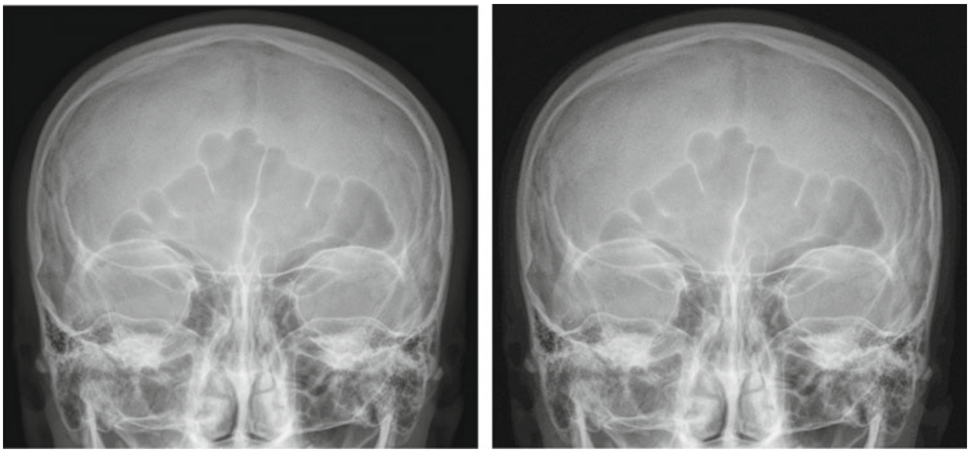
4-LSBs embedded image (32.43 dB)

3-LSBs embedded image (38.9 1 dB)



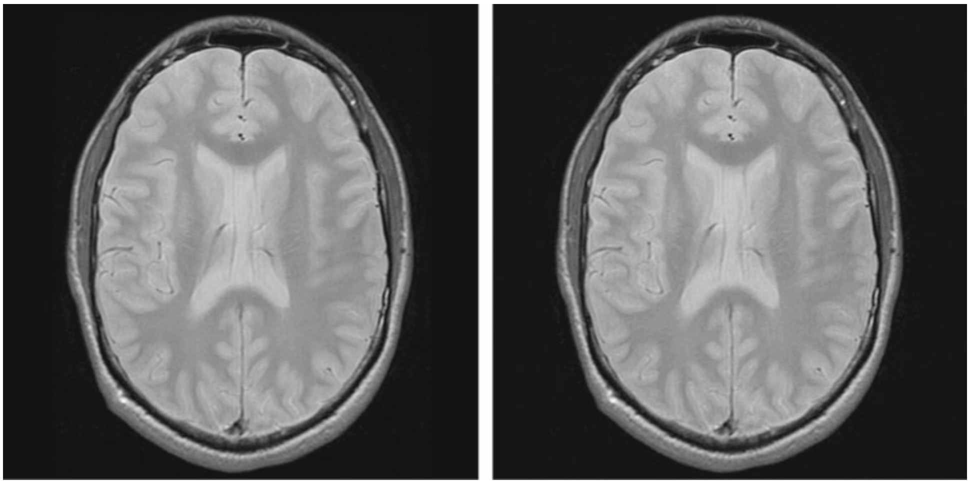
Original image (8 bits) 3-LSBs embedded image (36.89 dB)

Fig. 3 Original US image and 3-LSBs embedded image



Original image (8 bits) 3-LSBs embedded image (38.02 dB)

Fig. 4 Original DX image and 3-LSBs embedded image



Original image (8 bits) 3-LSBs embedded image (37.40 dB)

Fig. 5 Original MR image and 3-LSBs embedded image

Table 4 shows theoretical values of *PSNR* versus bit depth of original image and the number of embedded LSB planes. From this table, the maximum number of LSB planes for embedding can be derived corresponding to different bit depth images in order to obtain imperceptible degradation. Moreover, with high capacity up to 1 bit per pixel (bpp) for each embedded LSB plane, our solution allows to secure a large amount of private information; in particular, we can

Table 4 Theoretical values of PSNR (dB)

Bit depth	Number of embedded LSB planes										
	1	2	3	4	5	6	7	8	9	10	11
8	51.1	44.2	37.9								
10	63.2	56.2	50.0	43.9	37.7						
12	75.3	68.3	62.0	56.0	49.9	43.9	37.9				
16	99.3	92.4	86.1	80.1	74.0	68.0	62.0	56.0	49.9	43.9	37.9

embedded 98,304 bytes of private information into the grayscale image with the size of 512 × 512 in the case of using three embedded LSB planes. When comparing between our solution for DICOM images and the algorithm in [10] for nature images, we obtain the same results of them about the quality of embedded image and the capacity of embedded information. However, the security of their method is extremely weak due to using only inverse bit. Unlike them, our solution is supplemented the security property for embedded information by cryptography technique and fully compatible with DICOM standard, adapting to the requirements for the practice of telemedicine.

4 Conclusions

Even though there are some disadvantages, DICOM is one of the most ambitious international standards for medical imaging archiving and exchanging and has proved to be a very helpful standard in telemedicine. However, when the patients' medical images are transmitted through the network, interception and tampering of medical information become easier so that there is a risk of leakage of patient information. Hence, in this paper, we proposed an efficient solution to secure embedded private information in DICOM images to adapt to telemedicine. By the combination of encoding, encryption and watermarking, our method allows two-level security (one key for encryption and one key for watermarking), and lossless retrieval of the embedded information without the original image. As a result, in the normal mode, any physician can also view medical images with full support of DICOM standard while in the secure mode, personal information can only be extracted and decrypted to the user with complete access to the patient's data. In addition, the proposed solution not only improves information security but also obtains the high capacity and good imperceptibility with various DICOM images. The simulation results agree with the theoretical derivation.

Acknowledgements This research is funded by Ho Chi Minh City's Department of Science and Technology (HCMC-DOST) under grant number 82/2017/HĐ-SKHCN.**Conflict of Interest** The authors declare that they have no conflict of interest.

References

1. Ekeland, G., Bowes, A., Flottorp, S.: Effectiveness of telemedicine: a systematic review of reviews. Int. J. Med. Inform. **79**(11), 736–771 (2010)
2. Oleg, S. Pianykh: Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide, 2nd edn. Springer, Heidelberg (2012)
3. Gackowski, et al.: Development, implementation and multicenter clinical validation of the TeleDICOM–advanced, interactive teleconsultation system. J. Digit. Imaging **24**(3), 541–551 (2011)
4. Canavan, J.E.: The Fundamentals of Network Security. Artech House (2001)
5. Panchal, U.H., Srivastava, R.: A comprehensive survey on digital image watermarking techniques. In: Fifth IEEE International Conference on Communication Systems and Network Technologies, pp. 591–595 (2015)
6. Mousavi, S.M., Naghsh, A., Abu-Bakar, S.A.R.: Watermarking techniques used in medical images: a survey. J. Digit. Imaging **27** (6), 714–729 (2014)
7. Priya, S., Santhi, B., Swaminathan, P.: Study on medical image watermarking techniques. J. Appl. Sci. **14**(14), 1638–1642 (2014)
8. Acharya, R., Anand, D., Bhat, S., Niranjan, U.C.: Compact storage of medical images with patient information. IEEE Trans. Inf. Technol. Biomed. **5**(4), 320–323 (2001)
9. Singh, A.K., Kumar, B., Dave, M., Mohan, A.: Multiple watermarking on medical images using selective DWT coefficients. J. Med. Imag. Health Inform. **5**(3), 607–614 (2015)
10. Bamatraf, A., Ibrahim, R., Salleh, M.: A new digital watermarking algorithm using combination of least significant bit and inverse bit. J. Comput. **3**(4), 1–8 (2011)
11. Hajjaji, M.A., Mtibaa, A., Bourennane, E.L.: A watermarking of medical image: method based LSB. J. Emer. Trends Comput. Inf. Sci. **2**(12), 656–663 (2011)