TELKOMNIKA, Vol.17, No.5, October 2019, pp.2684~2696
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i5.13292

Advanced watermarking technique to improve medical images' security

Media Anugerah Ayu*, Teddy Mantoro, I Made Alan Priyatna
Department of Computer Science, Faculty of Engineering and Technology
Sampoerna University, Jakarta, Indonesia
*Corresponding author, e-mail: media.ayu@sampoernauniversity.ac.id

Abstract

Advances in imaging technology have made medical images become one of the important sources for information in supporting accurate diagnoses and treatment decisions by doctors for their patients. However, the vulnerability of medical images' security is high. The images can be easily 'attacked', which altered their information that can lead to incorrect diagnoses or treatment. In order to make the images less vulnerable from outside attacks, this study proposes to secure them by advancing the watermarking using dual-layer fragile technique. It is expected that this dual-layer fragile watermarking will guarantee the integrity, authenticity, and confidentiality of patient's and any other important information and also the pixel data of the medical images. The work in this study implements two LSBs of image where the role of the first LSB is as a tamper detector, and the second LSB is used to store patient's and any other important information. Medical images of four deadliest diseases in Indonesia were used to test the proposed watermarking technique. Results from the conducted tests show that the proposed technique able to generate a watermarked image that has no noticeable changes compared to its original image, with PSNR value more than 44 dB and SSIM value of almost 1, where the tamper detector can correctly detect and localize any tampering on the watermarked image. Furthermore, the proposed technique has shown to have a higher level of security on medical images, compared to DICOM standard and standard watermarking method.

Keywords*: DICOM, fragile watermarking, LSB, medical image, tamper detection*

1. Introduction

The Development in medical imaging technology has made medical images can be used to do early detection of various diseases, including diseases regarded as deadliest diseases. Data from World Health Organization (WHO), in 2013, stroke and heart disease are the deadliest disease in Indonesia. Around 3 million of Indonesian were diagnosed with heart disease and 2 million were diagnosed with stroke. On woman side, in the same year, cervical cancer and breast cancer are the deadliest disease in Indonesia with 98,692 cases for cervical cancer and 61,682 cases for breast cancer [1]. In line with that the high number of cervical cancer cases has made Indonesia become the country with the second highest in the world for cervical cancer [2].

Early detection of the diseases utilizing medical imaging technology is expected to be able to minimize the number of deaths caused by those diseases. Medical imaging technology is an advanced technology that has a function to produce a visual representation of human body which is used to do more accurate diagnoses and appropriate treatment decision. In addition, medical image can be send over the internet (well known as telemedicine) which allow doctors, physicians, and any other health care professionals do an evaluation, diagnose and treatment from a distance [3]. There are various types or modalities of medical images available, such as radiography, computed tomography, magnetic resonance imaging, ultrasound imaging [4]. Whereas, the difference between each modality is on the types of energies and acquisition technology used to produce medical image. Magnetic Resonance Imaging and Computed Tomography (CT) modalities are the most common used to diagnose stroke, heart disease, cervical and breast cancer [5, 6]. The use of medical imaging technology continues increasing in every year. Figure 1 shows the usage of CTs and MRIs devices increasing from the last 30 years in Organization for Economic Co-Operation and Development (OECD) countries [7]. According to Ministry of Health Indonesia, governors will support in increasing the number of

Received January 5, 2019; Revised May 28, 2019; Accepted June 12, 2019

health devices including CTs and MRIs devices twice or even three times more to the previous number within year 2015–2019 [8].

Increase in the number of medical imaging technology can lead to more and new cyber-threats since it is transferable over the internet. Therefore, it is a must to secure the medical images from any kind of attack, since any changes on medical images may lead to incorrect diagnoses and treatment decisions for the patient. In medical imaging technology arena, Digital Imaging and Communication in Medicine (DICOM) is used as an international standard for transferring, storing, retrieving medical image information. In short, DICOM image format containing two important parts: The header file which save important information such as patient information, study information, and the pixel data. DICOM Standard implement several security schemes on both, the confidential data and images as stated in PS3. 15 of the DICOM Standard, which about Security System Management Profiles [9].

DICOM Standard currently implements digital signature to guarantee the authenticity and integrity of the pixel data and saved in group tag (FFFA,FFFA). Furthermore, DICOM Standard implements encryption such as AES and triple DES on selected DICOM Data Set, one of them is the Electronic Patient Record (EPR).Moreover, DICOM Standard also specifies anonymization scheme by deleting or changing any confidential DICOM Data Set in order to allow the DICOM file uploaded publicly for certain purposes such as research, presentation, study, etc. [9]. The limitations of the security schemes implemented by DICOM Standards are integrity and authenticity are not addressed for selected DICOM Data Set and the anonymized DICOM file could not be used for further diagnoses anymore, since the information about patient was removed permanently Furthermore, unauthorized people could edit partly or completely alter the pixel data of the medical image and cannot localize of altered pixel. Those become the major limitations in the DICOM Standard [10, 11].

Knowing the limitations of current security schemes, the work presented in this paper tries to find and develop a security scheme for medical images. This study proposes a securing technique which based on dual-layer fragile image watermarking to ensure the integrity, confidentiality and authenticity of the medical images. The remaining of the paper is organized as follows: section 2 discusses the literature review on digital image watermarking for medical images; then section 3 explains about the proposed method; followed by section 4 which describes the methodology used; section 5 illustrates the examination result of our proposed method; and finally, section 6 presents the conclusions of the study.

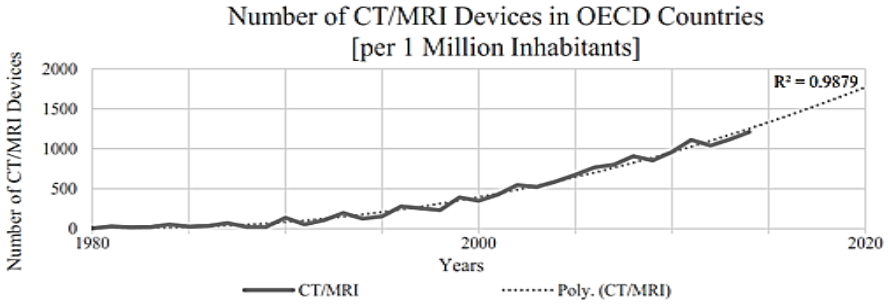


Figure 1. Number of CT/MRI devices in OECD countries in 1980-2014

2. Digital Watermarking for Medical Images

Digital watermarking is a technique for embedding data or information called ‘watermark’ into a multimedia object which called the ‘cover’ such as image, video, audio or even only a text. According to its functionalities, digital watermarking can be classified into two categories: robust and fragile watermarks. Robust watermarks are good for authentication and characterizing resistant to a common signal processing such as compression. On the other hand, a fragile watermark will not survive from signal processing, however it is good to be used for data integrity [12]. Therefore, this study develops a fragile watermarking to ensuring the integrity of the medical image which also followed by ensuring its authenticity and confidentiality. Moreover, in this study, Least Significance Bit (LSB) modification, a spatial

domain watermarking scheme is implemented to develop a fragile watermarking for medical images. Whereas, the LSB modification image watermarking works by changing the least significant bit (LSB) of the cover image with the watermark bits [13]. Embed the watermark into the last two significant bits for example (2nd and 1st LSB of cover image) for each pixel value, the watermark mostly not going to detectable by human eyes [14]. For example, if the image pixel is 180 which has binary value of 10110100 and the watermark bits 0, the value of the pixel will be the same, 180. Same pixel value with watermark bits 1, the pixel value will be 10110101 which is 181 in decimal. Thus, human eyes are less sensitive with two colors that have value 180 and 181 in gray colors between black is 0 and white is 255 [15].

Digital watermark techniques have been proposed for securing medical images. [16] proposed a robust and imperceptible dual watermarking. In their proposed method hybrid error correcting codes (combination of BCH & repetition code) are utilized to encode the watermark data before embedding it into the cover image. Since they use another image as the cover image, their method requires cover image which can hold all the watermark data (the medical image). The [17, 18] proposed methods with the idea of combining digital watermarking with compression or/and cryptography algorithm. Both methods utilize the encryption and compression on watermark data (EPR and bits of ROI) and do the process before inserting it into LSB of the cover image. The difference between them is [17]'s method use Region of Interest (ROI) as the cover image, thus may cause degradation on ROI's quality. [18]'s method on the other hand, use Region of Non-Interest (RONI) as the cover image which means the RONI part should be large enough to hold all the watermark.

Instead of just hiding EPR or image's bits into cover image (same image or other unrelated image), researchers also develop method for tamper detection and localization to know whether the image has been tampered and its location. [19, 20] proposed a tamper detection and localization of image based on watermarking block. However, their methods only focus whether the image has been tampered or not, and they ignore the DICOM tags such as EPR, image properties, study and series properties, etc. [21] proposed a dual-layer watermarking for medical images. The method embeds the EPR data into 2nd LSB of RONI part and block-based image on 1st LSB of a medical image for tamper detection and localization. Other proposed method by [6] do the combining of cryptography and watermarking to provide confidentiality, authenticity and integrity of the medical image. Both [12]'s and [21]'s methods embed the EPR data into RONI part of the images, which means their method really depend on the size of the RONI who can hold all watermark bits.

The study presented in this paper proposes a technique to secure medical images which based on dual-layer fragile digital watermarking. The proposed technique uses hash value of DICOM tags to ensure the integrity of the DICOM tags, encrypts the EPR to provide confidentiality and authenticity, and then embeds it in the 2nd LSB of the medical image and lastly calculates the hash value of 8x8 non-overlapped block, and creates an id for each block which then embeds it into 1st LSB to provide integrity of the medical image. The proposed technique has been tested on CT and MRI medical images of heart diseases, strokes, cervical cancers and breast cancers which are the deadliest disease in Indonesia. The detail of proposed technique is discussed in section 3.

3. The Proposed Security Technique

There are two core processes that need to be performed in our proposed technique, i.e. watermark embedding process and watermark extraction process. This section discusses the processes in details.

3.1. Watermark Embedding Process

The watermark embedding process mainly has two main sub-processes, which are the watermark generation and watermark insertion. The flow of the process is summarized in a diagram which presented in Figure 2. In our study, two watermarks are used and embedded into its corresponding medical image: concatenation of EPR and hash of DICOM Data Set (DICOM Tags) and the concatenation of id and hash value of each non-overlapped block. Here is more detail about the watermark generation:

a. Separate the EPR tags and implement AES256 encryption algorithm to encrypt (EncCt) used to guarantee the confidentiality and authenticity of the EPR.

b. Calculate the hash of DICOM tags (HashDt which is used to guarantee the integrity of it using SHA 256 algorithm.
c. Concatenation of the HashDt and EncCt to become the 1st watermark: ConDC.
d. After embedding the ConDC into 2nd LSB of the cover image, prepare 8x8 non-overlapped blocks image concatenate with the row & column as an id of each non-overlapped blocks. Then calculate the hash of it using SHA256 algorithm. This watermark data act as tamper detector and able to show the tamper's location.

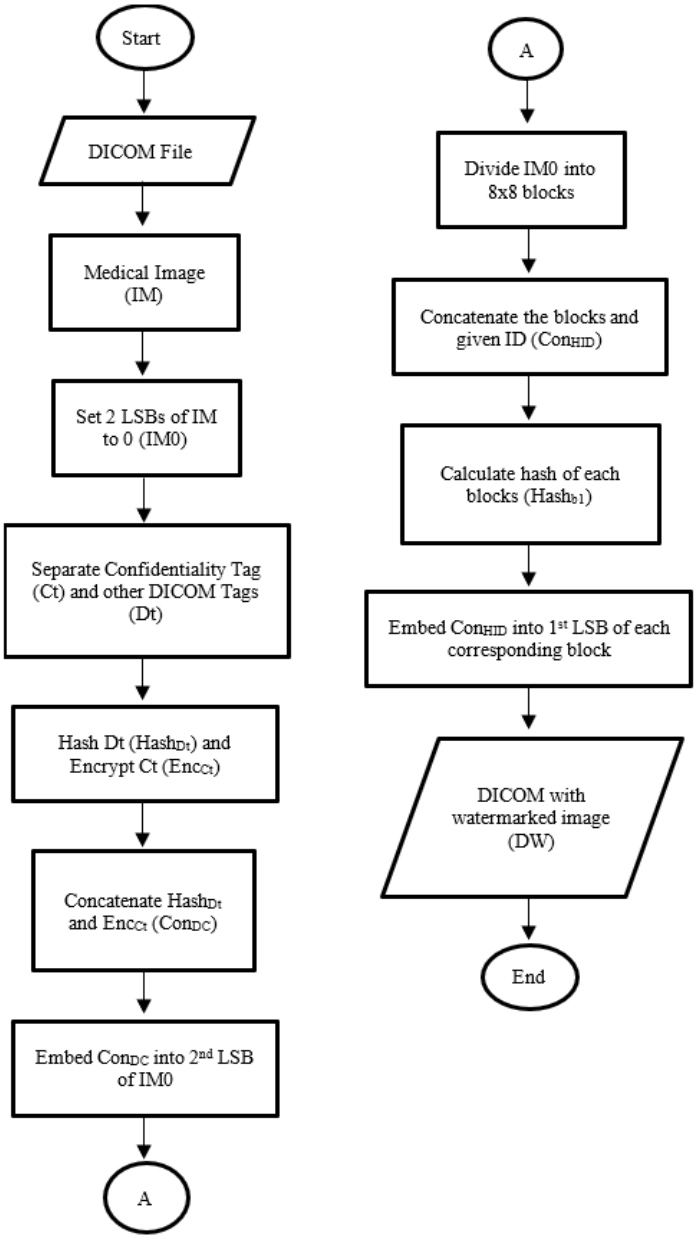


Figure 2. Watermark generation and insertion of the proposed technique

The next step is watermark insertion (embedding) process. Embed the ConDC into 2nd LSB and concatenation of id and hash of each block into its corresponding blocks. The detail of insertion method discusses in the following manner:

a. Expand the length of ConDC to fit the size of the cover image
b. To increase the security, insert randomly each bit of ConDC into 2nd LSB of image using the following equation:

$$f(x) = kx \bmod n + 1 \quad (1)$$

whereas, k is the secret prime key in which k ∈ [1, n]; x is the bit position of ConDC with x ∈ [1, length of ConDC]; and n is the total number of pixels available for watermark embedding.

c. Then move for second watermarks. Since We use SHA256 on each block, which generate 64 hex-bytes characters, then We need to choose randomly 16 hex-bytes characters to fit the total bits available on 8x8 non-overlapped blocks using formula:

$$f(x) = kx \bmod n + 1 \quad (2)$$

whereas, k is the secret prime key in which k ∈ [1, n]; x is the characters position of the hash result with x ∈ [1, 16]; and n is the total number of pixels available for watermark embedding.

d. Embed randomly the selected characters into 1st LSB of corresponding block using following formula:

$$f(x) = kx \bmod n + 1 \quad (3)$$

whereas, k is the secret prime key equal to previous k used in previous step; x is the characters position of the concatenated string in binary x ∈ [1, 64]; and n is the total number of pixels available for watermark embedding.

3.2. Watermark Extraction Process

The main objective of watermarking extraction process is to check the integrity, confidentiality and authenticity of the image. Details on this process are presented in Figure 3. As depicted in Figure 3, there are two phases to check the data integrity, first check whether the image has been tampered or not, then check whether the DICOM Tags has been tampered or not. Here is more detail about the watermark extraction:

a. Divide the medical image into 8x8 non-overlapped blocks and extract 1st LSB of each block.
b. Calculate hash of each block then compare the calculation result with the extracted hash value. If the value is not the same, this means the image has been altered. The non-overlapped blocks can show the location of tampered image. Otherwise, continue to the next steps.
c. Extract the 2nd LSB of the cover image to get the concatenated string of DICOM Tags hash value and the encrypted EPR.
d. Calculate the hash of the DICOM tags then compare with the extracted DICOM tags. If the values are same, then continue to the next steps, otherwise the DICOM tags have been altered.
e. Lastly, after checking the medical image and the DICOM tags, decrypt the encrypted EPR.

4. Methodology

The schematic flow of this study is firstly by reviewing previous works and identifying the study position and contribution to the topic of securing medical images. Then, design and implementation of the proposed technique, followed by collecting the study materials and data collection. Lastly, analyze the data and draw a conclusion.

4.1. Source of Materials

Medical images which related with four deadliest diseases in Indonesia are used in this study to test the proposed watermarking technique. The anonymized medical images are taken from open website. The image format from of the medical image originally is in “dcm” format (DICOM format). The size of medical image of CT scan is about 512x512-pixel matrix and the MRI is about 256x256-pixel image with 16 allocated bits and the image in monochrome mode. Those sizes are the common size of medical image for CT scan and MRI modalities [22]:

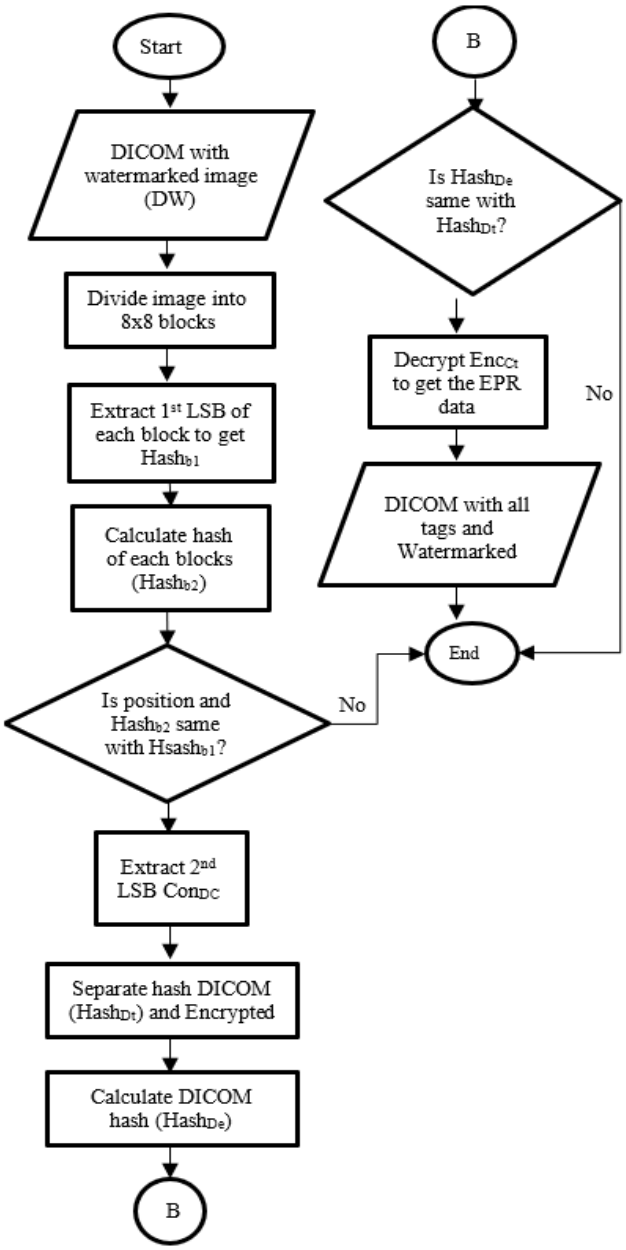


Figure 3. Watermark extraction of the proposed technique

4.2. Performance Analysis on Image Quality (Imperceptibility Analysis)

In this research work, the proposed schematic use of LSB watermarking technique is to embed the watermark to the cover image. As a result, an image quality degradation will occur. The good quality of image watermarking technique is that the image can hold as much data as possible, and the image quality degradation level is low [23]. There are various techniques to evaluate the difference between an original image and a watermarked image whether qualitatively or quantitatively. Among those techniques, the most and commonly used criteria and become the standard evaluation of image quality measurements are Mean Squared Error (MSE) and the Peak Signal to Noise Ratio (PSNR) for quantitative method and Structural Similarity Index Metrix (SSIM) for qualitative method.

The goal of MSE is to measure or provide quantitative scores of two signals/images which describe how similar the signal/image to each other, the degree of error or distortion

among them. MSE can be obtained by calculating the average of squared intensity of two or more (inputs) images as shown in the formula of MSE below:

$$MSE = \frac{1}{NM}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}(x_{j,k} - x'_{j,k})^2 \quad (4)$$

where NM is the image size, xj,k indicates the jk-th pixel value of watermarked image and x'j,k indicates the jk-th pixel value of the original image. The smaller the MSE value indicates the degradation level of the watermarked image is low.

Peak Signal to Noise Ratio (PSNR) is a mathematical way to measure the image quality based on the pixel different between the two images: the original image and watermarked image. MSE need to calculated first before calculating the PSNR which can be calculated by following formula:

$$PSNR = 10\ log_{10}\frac{L^2}{MSE} \quad (5)$$

whereas, L is the range of image pixel intensity. As example, for image of 8 bit/pixel of grayscale image, $L=2^8-1=255$. The higher value of PSNR indicates the better quality of watermarked image.

Both MSE and PSR values are simple and easy to calculate, however, they are not very well matched to perceived visual quality. For that reason, in 2004, Structural Similarity Index Metrix were proposed by [24]. SSIM is one of Human Visual System (HVS) method to check image quality and SSIM used to compare two images quality by measuring their similarity. Three aspects are calculated to determine the similarity of two images: luminance, contrast and structure of the images. The luminance functions l (x y) for reference image x (in this case is the original image) and test image y (the watermarked image) is:

$$l(x,y) = \frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1} \quad (6)$$

where μ_x and μ_y are the mean values of x and y, and C1 is a stabilizing constant.

The structure comparison function s (x y) of SSIM is expressed as:

$$s(x,y) = \frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \quad (7)$$

where σ_{xy} is the correlation between x and y and C3 is constant stabilizer. Then, the SSIM index can be written as:

$$SSIM(x,y) = [l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} \quad (8)$$

in [24], α = β = γ = 1 and C3 = C2/2. Those, SSIM(x,y) finally can be expressed as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (9)$$

SSIM is a decimal value between -1 to 1. Whereas, -1 for non-identical dataset and the opposite, 1 if all pixel values are identical. In this study, the SSIM value calculated using python library called "scikit-image" library.

4.3. Performance Analysis on Tamper Detection (Fragility Analysis)

Several malicious attacks such as image cropping, copy-paste attacks, collage attack and constant-average attack are commonly used to the fragility of watermarking scheme [25]. Whereas, image cropping and copy-paste attacks were done by crop or copy-paste some part of the watermarked image randomly. Collage attack in this study done by copying the authenticated block of watermarked image into another part of the image. Constant-average attack done by modifying the part of the image and keep the average intensity of the image the same with the original one. Fragile digital watermarking in which depend on average image

intensity will not resist to this kind of attack. These attacks are chosen in order to compare the proposed scheme with other fragile digital watermarking which proposed by [26] and [27]. Calculated tampered detection rate can be used to evaluate the quality of the tamper detection method. Tampered detection rate calculates the number of tampered blocks detected in the image. Higher rate of tampered block indicates a good tamper detection method. Here is the formula to calculate the tampered detection rate (TDR):

$$TDR = \frac{number\ of\ detected\ blocks}{number\ of\ tampered}\ x\ 100\% \quad (10)$$

5. Results and Discussion

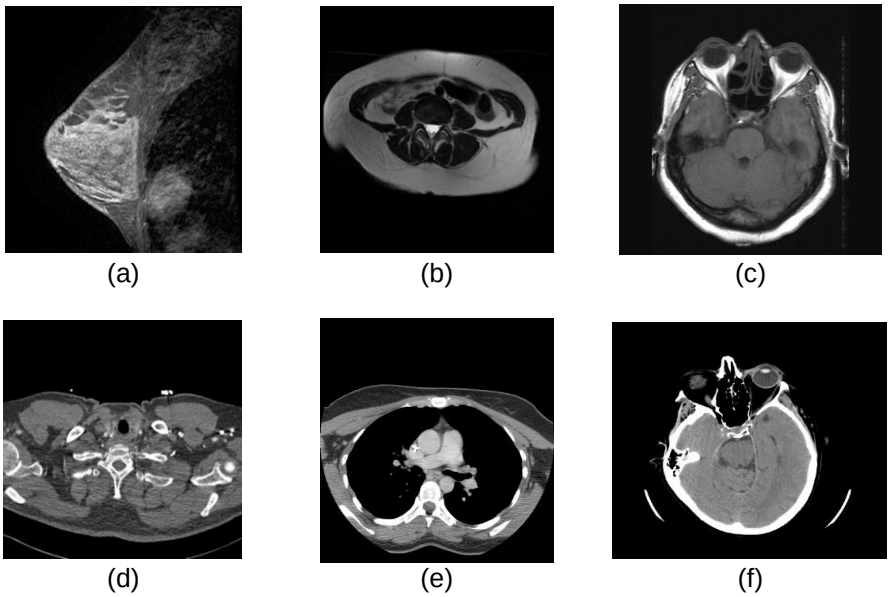
This section presents the results of study conducted and discusses the interpretation of the results and its implications.

5.1. Medical Images Dataset

The proposed technique was developed and implemented using python programming language. It was then tested on medical images which related to the four deadliest diseases in Indonesia. Figure 4 shows all medical images dataset used in this research work with detail properties stated in Table 1.

Table 1. Properties of Medical Images Dataset

No	Name	Modality	Size	Bit Depth	Color Type
1	Breast_MRI	MRI	256 x 256	16	Monochrome
2	Cervix_MRI	MRI	512 x 512	16	Monochrome
3	Brain_MRI	MRI	256 x 256	16	Monochrome
4	Heart_CT	CT	512 x 512	16	Monochrome
5	Breast_CT	CT	512 x 512	16	Monochrome
6	Brain_CT	CT	512 x 512	16	Monochrome



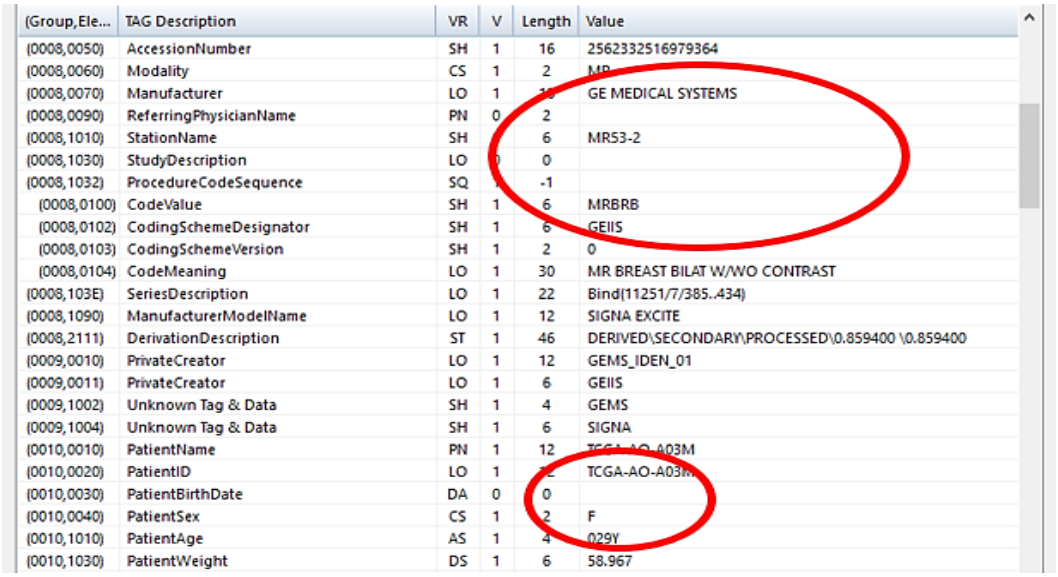
(a) (b) (c)

(d) (e) (f)

Figure 4. Image dataset: (a) breast (MRI), (b) cervix (MRI), (c) brain (MRI), (d) heart (CT), (e) breast (CT), (f) brain (CT)

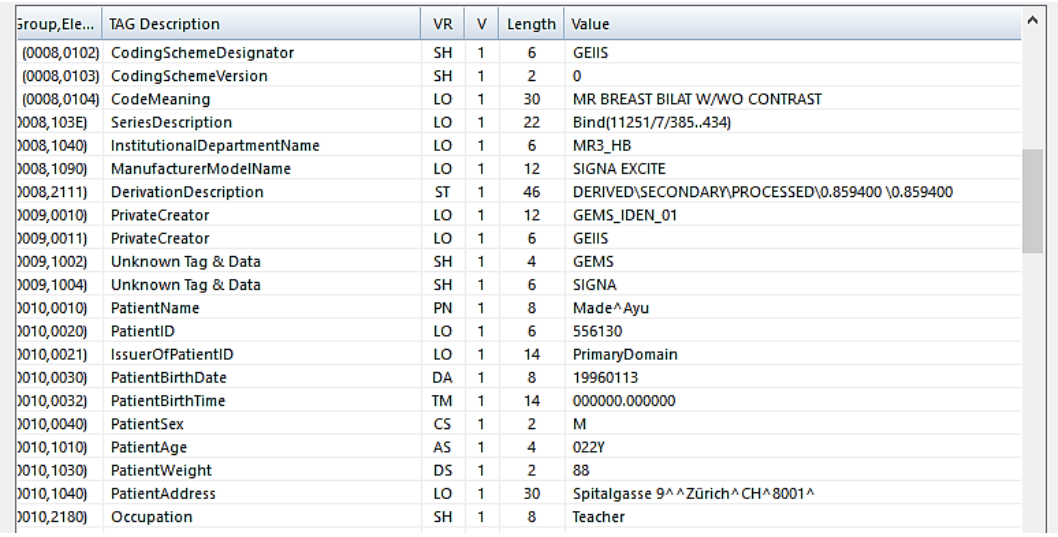
Since all images are taken from open website named as http://www.cancerimagingarchive.net/, this means the images are anonymized medical images in which point the patient information or other confidential tags has been removed or changed with random value as shown in Figure 5. For that reason, before using the images for further process, rational dummy values are inserted into removed DICOM tags. This process of putting

dummy values known as de-identifier as shown in Figure 6. After the de-identifier process, a DICOM file with complete DICOM tags is ready to use for testing the performance of the proposed technique.



(Group,Ele...	TAG Description	VR	V	Length	Value
(0008,0050)	AccessionNumber	SH	1	16	2562332516979364
(0008,0060)	Modality	CS	1	2	MR
(0008,0070)	Manufacturer	LO	1	18	GE MEDICAL SYSTEMS
(0008,0090)	ReferringPhysicianName	PN	0	2	
(0008,1010)	StationName	SH	1	6	MR53-2
(0008,1030)	StudyDescription	LO	0	0	
(0008,1032)	ProcedureCodeSequence	SQ	1	-1	
(0008,0100)	CodeValue	SH	1	6	MRBRB
(0008,0102)	CodingSchemeDesignator	SH	1	6	GEIIS
(0008,0103)	CodingSchemeVersion	SH	1	2	0
(0008,0104)	CodeMeaning	LO	1	30	MR BREAST BILAT W/WO CONTRAST
(0008,103E)	SeriesDescription	LO	1	22	Bind(11251/7/385..434)
(0008,1090)	ManufacturerModelName	LO	1	12	SIGNA EXCITE
(0008,2111)	DerivationDescription	ST	1	46	DERIVED\SECONDARY\PROCESSED\0.859400 \0.859400
(0009,0010)	PrivateCreator	LO	1	12	GEMS_IDEN_01
(0009,0011)	PrivateCreator	LO	1	6	GEIIS
(0009,1002)	Unknown Tag & Data	SH	1	4	GEMS
(0009,1004)	Unknown Tag & Data	SH	1	6	SIGNA
(0010,0010)	PatientName	PN	1	12	TCGA-AO-A03M
(0010,0020)	PatientID	LO	1	12	TCGA-AO-A03M
(0010,0030)	PatientBirthDate	DA	0	0	
(0010,0040)	PatientSex	CS	1	2	F
(0010,1010)	PatientAge	AS	1	4	029Y
(0010,1030)	PatientWeight	DS	1	6	58.967

Figure 5. Anonymized DICOM tags



Group,Ele...	TAG Description	VR	V	Length	Value
(0008,0102)	CodingSchemeDesignator	SH	1	6	GEIIS
(0008,0103)	CodingSchemeVersion	SH	1	2	0
(0008,0104)	CodeMeaning	LO	1	30	MR BREAST BILAT W/WO CONTRAST
)008,103E)	SeriesDescription	LO	1	22	Bind(11251/7/385..434)
)008,1040)	InstitutionalDepartmentName	LO	1	6	MR3_HB
)008,1090)	ManufacturerModelName	LO	1	12	SIGNA EXCITE
)008,2111)	DerivationDescription	ST	1	46	DERIVED\SECONDARY\PROCESSED\0.859400 \0.859400
)009,0010)	PrivateCreator	LO	1	12	GEMS_IDEN_01
)009,0011)	PrivateCreator	LO	1	6	GEIIS
)009,1002)	Unknown Tag & Data	SH	1	4	GEMS
)009,1004)	Unknown Tag & Data	SH	1	6	SIGNA
)010,0010)	PatientName	PN	1	8	Made^Ayu
)010,0020)	PatientID	LO	1	6	556130
)010,0021)	IssuerOfPatientID	LO	1	14	PrimaryDomain
)010,0030)	PatientBirthDate	DA	1	8	19960113
)010,0032)	PatientBirthTime	TM	1	14	000000.000000
)010,0040)	PatientSex	CS	1	2	M
)010,1010)	PatientAge	AS	1	4	022Y
)010,1030)	PatientWeight	DS	1	2	88
)010,1040)	PatientAddress	LO	1	30	Spitalgasse 9^^Zürich^CH^8001^
)010,2180)	Occupation	SH	1	8	Teacher

Figure 6. De-identifier DICOM tags

5.2. Performance Analysis on Image Quality (Imperceptibility Analysis)

Perceptual imperceptibility is one of the most significant indexes in the watermarking performance analysis. This means that human eyes should not be able to detect the embedded watermark in the cover image. Figure 7 gives the watermarked images generated by proposed watermarking schemes on medical images. We can see that the watermarked images in Figure 7 are almost the same as the original image in Figure 4. It shows the proposed scheme provides a satisfactory watermark imperceptibility. The small difference between the images can be seen from their MSE, PSNR and SSIM values as describes in Table 2.

Table 2 shows the comparison of LSB standard watermark and proposed watermarking technique in term of MSE, PSNR and SSIM values. Standard watermarking in this state is

where the watermark bit embedded into the LSB of cover image without randomization and the proposed watermarking technique randomized the insertion of the watermark bits. Both, standard and proposed watermarking techniques has PSNR values more than 44 dB, and SSIM values almost 1 whereas 1 is the maximum value of SSIM) these prove the imperceptibility of the watermark objectively. From this table, then generate graphs like shown in Figure 8 and Figure 9. From these figures, PSNR and SSIM values of proposed technique consistently show higher values than the standard watermarking. This means that randomized the insertion of watermark bits gives higher value of PSNR and SSIM which indicate the proposed technique produces better watermarked image quality compare with the standard watermarking technique.

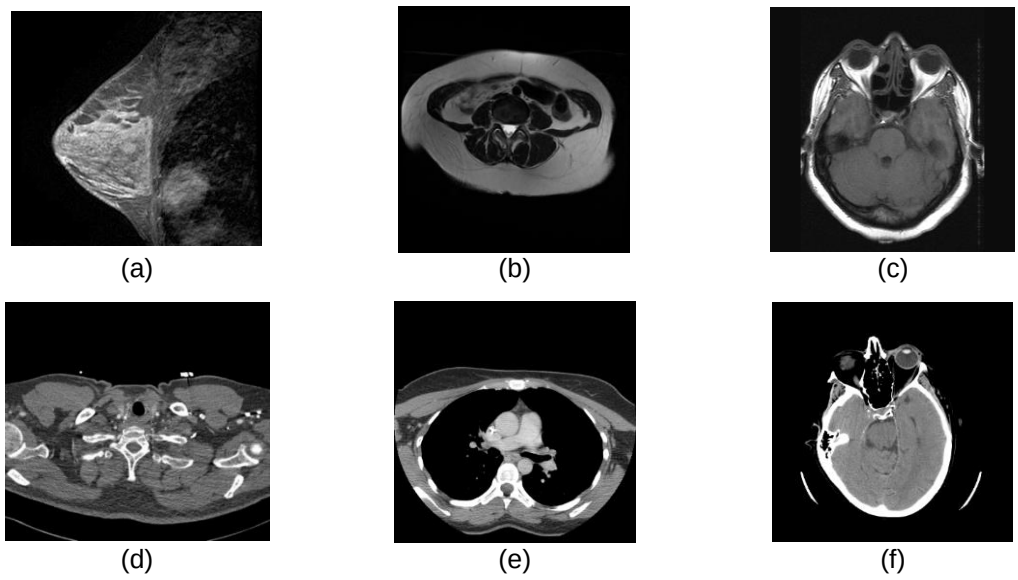


Figure 7. Watermarked image: (a) breast (MRI), (b) cervix (MRI), (c) brain (MRI), (d) heart (CT), (e) breast (CT), (f) brain (CT)

Table 2. Watermarked Images Quality Comparison

Medical Images	Standard Watermarking			Proposed Scheme		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM
ct_brain	2.09525681	44.91843101	0.99988070	2.02343369	45.06991385	0.99987874
mr_brain	2.18028259	44.74567573	0.99896836	2.18138123	44.74348790	0.99903757
ct_breast	2.18967438	44.72700824	0.99954084	2.11228180	44.88328504	0.99963537
mr_breast	2.32829285	44.46042757	0.99912262	2.19120789	44.72396779	0.99947824
ct_heart	2.49826431	44.15441977	0.99982775	2.50180435	44.14827017	0.99981621
mr_cervix	2.43020630	44.27437219	0.99935902	2.39344788	44.34056387	0.99937462

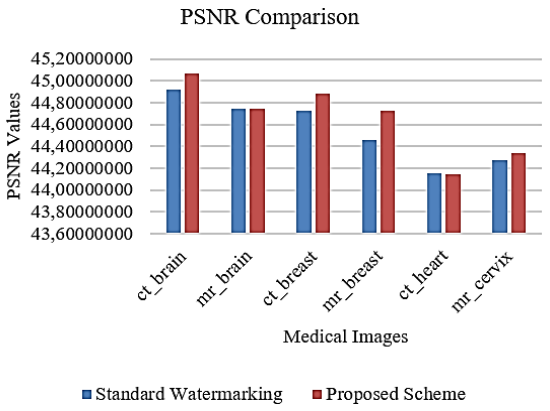


Figure 8. PSNR comparison

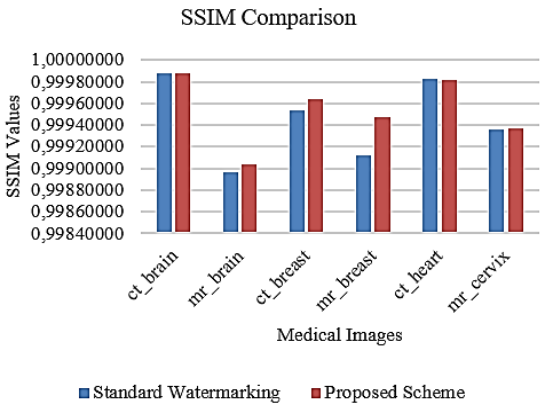
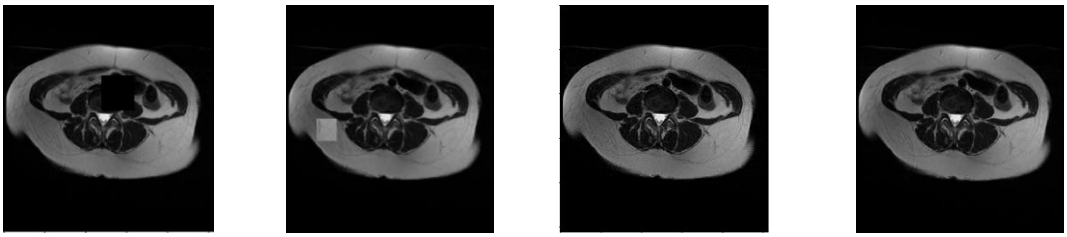


Figure 9. SSIM comparison

5.3. Performance Analysis on Tamper Detection (Fragility Analysis)

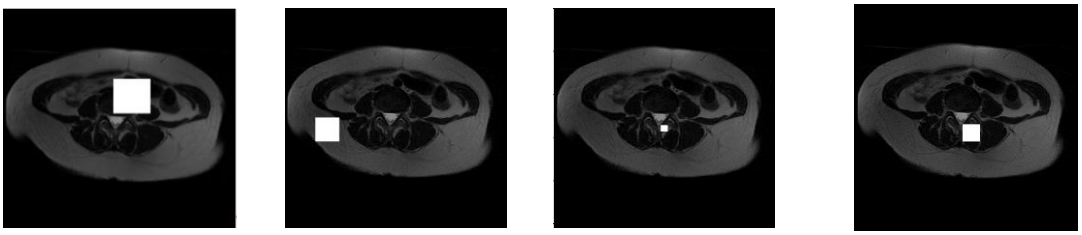
Malicious attacks are commonly used to test the fragility of digital watermarking [25]. Some classical malicious attacks are performed on the watermarked images such as image cropping, copy-paste, collage attack, and constant-average attacks to test the fragility of proposed watermarking technique. These attacks are chosen in order to compare the proposed technique with other fragile digital watermarking technique which proposed by [26, 27]. These attacks performed on one of the sample images, the "mr_cervix" image as shown in Figure 10.

The proposed technique is a blind watermarking technique where there is no need for original image to detect whether the watermarked image has been tampered or not. The tamper localization maps obtained by the proposed watermarking technique are shown in Figure 11. From that figure, we can see that the falsified areas are clearly identified by the proposed technique. It means that the proposed watermarking technique has achieved good tamper identification and localization results for various malicious attacks.



(a) (b) (c) (d)

Figure 10. Several malicious attacks on watermarked image (a) cropping attack (b) copy-paste attack (c) collage attack (d) constant-average attack



(a) (b) (c) (d)

Figure 11. Tamper detection and localization results (a) cropping attack (b) copy-paste attack (c) collage attack (d) constant-average attack

Table 3 shows the fragility comparison of proposed technique and other fragile digital watermarking which proposed by [26] and [27]. Data in the table clearly show that the proposed technique offers better security in term of fragility of the watermarked image. The proposed technique is a blind watermarking technique and more resist on collage and constant-average attacks compare with the references.

The proposed watermarking technique then is compared with current DICOM Standard security and the standard watermarking techniques which stated in [12]. The proposed technique provides authenticity and confidentiality for header data of medical image by implementing AES256 encryption before the embedding process. Moreover, the integrity of the header data can be achieved by checking the hash value of the header during extraction process. The comparison of proposed technique, DICOM Standard and the standard watermarking technique is shown in Table 4. Based on data on Table 4, it can be concluded that the proposed watermarking technique provides better security to medical images compared to the current DICOM security technique and proposed watermarking technique by [12]. The proposed technique succeeds in providing the integrity, confidentiality and authenticity for medical images.

Table 3. Fragility Comparison

Items	[27]	[26]	Proposed Scheme
Blind Watermarking	No	Yes	Yes
Image cropping	Yes	Yes	Yes
Copy-paste attack	Yes	Yes	Yes
Collage Attack	No	Yes	Yes
Constant-average attack	No	No	Yes

Table 4. Medical Image Security Scheme's Performance Comparison

Indicator	Algorithm		
	DICOM Standard	Standard Watermarking Scheme	Proposed Algorithm
Confidentiality (header)	√	√	√
Confidentiality (pixel data)			
Authenticity (header)			√
Authenticity (pixel data)	√	√	√
Integrity (header)			√
Integrity (pixel data)	√	√	√

6. Conclusion

In this study a dual-layer fragile digital watermarking is proposed to secure medical images especially with DICOM format. In the proposed watermarking technique, first, the confidentiality of DICOM tags is encrypted using AES256 encryption algorithm and concatenated with the other DICOM tags, then embed randomly into 2nd LSB of the medical image. This step is to guarantee the authenticity, confidentiality and integrity of header data. Next, to guarantee the integrity of the medical image, the image divided into 8x8 non-overlapped block, calculate hash value of its block using SHA256 algorithm and concatenate with the row and column of the block then embed into 1st LSB of the image.

The proposed technique has been tested on six medical images from four deadliest diseases in Indonesia with CT and MRI modality. The images are in monochrome mode and has 16 bits for each pixel and the size between 256x256 and 512x512 pixel. From the result, it can be concluded that the proposed technique has a good quality of watermarked image where the human eyes could not be able to detect the embedded watermark data in the image and watermarked image has high value of PSNR above 44dB and SSIM value above 0.99 that almost reach the maximum value which is 1. Furthermore, the proposed watermarking technique also resist from several malicious attacks such as cropping attack, copy-paste attack, collage attack and constant-average attack. The proposed technique able to detect and locate the tampering precisely. Lastly, comparing with current DICOM security standard and another fragile watermarking technique for medical image, the proposed technique has offered more aspect of security for medical image. The proposed technique has succeeded to guarantee the authenticity, integrity and confidentiality of medical image for both header data and the image pixel data.

As a suggestion for further research; a proposed dual-layer fragile digital watermarking is far from a perfect security scheme for medical image, hence many improvements need to be done to close its flaws. First suggestion is to test the proposed technique on more medical images to get more reliable results. Moreover, proposed technique needs to be tested on original medical images and the quality of watermarked image needs to be examined directly by the doctor, physician, or other experts since current result is only based on calculation of PSNR and SSIM. Moreover, proposed technique still focuses only on MRI and CT modalities of medical images in which having monochrome image mode. There are still other modalities which have colored image. Therefore, the second suggestion for future research is to improve proposed technique in order to work properly on colored medical images and can be used for any modality of medical images.

References

[1] Pusdatin. Care for Breast Cancer Month (in Indonesia: Bulan Peduli Kanker Payudara). 22 December 2016. [Online]. Available: http://www.pusdatin.kemkes.go.id/article/view/ 17013100001/bulan-peduli-kanker-payudara.html.

[2] Maharani E. Cancer Cervix Patients in Indonesia is Ranked Number Two (in Indonesia: Penderita Kanker Serviks di Indonesia Tempati Urutan Kedua), 27 August 2017. [Online]. Available: http://www.republika.co.id/berita/gaya-hidup/info-sehat/17/08/27/ovc44v335-penderita-kanker-serviks-di-indonesia-tempati-urutan-kedua.
[3] WHO. Diagnostic Imaging. 21 2 2017. [Online]. Available: http://www.who.int/diagnostic_imaging/en
[4] Bushberg JT, Seibert JA, Leidholdt EM JR, Boone M. The Essential of Physics of Medical Imaging. Philadelphia: Wolters Kluwer. 2011.
[5] M Donohue. Cervical MRI Scan. 30 March 2017. [Online]. Available: https://www.healthline.com/health/cervical-mri-scan.
[6] Cancer.Net. Breast Cancer: Diagnosis. April 2017. [Online]. Available: https://www.cancer.net/cancer-types/breast-cancer/diagnosis.
[7] OECD. Health Care Resources. 2017. [Online]. Available: http://stats.oecd.org/viewhtml.aspx?datasetcode=HEALTH_REAC&lang=en#
[8] Kementerian Kesehatan RI. *Action Plan 2015-2019 Activities of Directorate for Production and Distribution of Medical Tools and Devices (in Indonesia: Rencana Aksi Kegiatan Tahun 2015-2019 Direktorat Bina Produksi dan Distribusi Alat Kesehatan)*. Direktorat Jendral Bina Kefarmasian dan Alat Kesehatan Kementrian Kesehatan RI, Jakarta. 2015.
[9] NEMA. DICOM PS3. 15 2018a. Security and System Management Profiles. Nema. 2018.
[10] Al-Haj A. Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. *Journal of digital imaging*. 2014.
[11] Pianykh OS. Digital Imaging and Communications in Medicine (DICOM). Berlin Heidelberg: Springer. 2012.
[12] Al-Haj A, Mohammad A, Amer A. Crypto-Watermarking of Transmitted Medical Images. *Society for Imaging Informatics in Medicine*. 2016; 30(1): 26-38.
[13] Shukla R, Manish P, Arora AK. Analysis of Image Watermarking: LSB Modification and Spread-Spectrum Technique. *IOSR Journal of Electronics and Communication Engineering (IOSRJECE)*. 2012: 11-15.
[14] Chopra D, Gupta P, Sanjay G, Gupta A. LSB Based Digital Image Watermarking for Gray Scale Image. *IOSR Journal of computer Engineering (IOSRJCE)*. 2012; 6(1): 36-41.
[15] Chou CH, Wu TL. Embedding Color Watermarks in Color Images. *EURASIP Journal onApplied Signal Processing*. 2003: 32-40.
[16] Singh AK, Kumar B, Dave M, Mohan A. Robust and Imperceptible Dual Watermarking for Telemedicine Applications. *Wireless Personal Communication*. 2014.
[17] Badshah G, Liew SC, Zain JM, Ali M. Watermark Compression in Medical Image Watermarking Using Lempel-Ziv-Welch (LZW) Lossless Compression Technique. *Journal of Digital Imaging*. 2016; 29(2): 216-25.
[18] Nithya S, Amudha K. *Watermarking and Encryption in Medical Image Through ROI-Lossless Compression*. International Conference on Communication and Signal Processing. 2016: 610-614.
[19] Adiwijaya FP, Permana FP, Wirayuda TA, Wisesty UN. *Tamper Detection and Recovery of Medical Image Watermarking using Modified LSB and Huffman Compression*. International Conference on Information and Application. 2013: 129-132.
[20] Zain JM, Fauzi ARM. *Medical Image Watermarking with Tamper Detection and Recovery*. EMBS Annual International Conference. New York City. 2006: 3270-3273.
[21] Tan CK, Ng JC, Xu X, Poh CL, Guan YL, Sheah K. Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability. *Journal of Digital Imaging*. 2011; 24(3): 528-540.
[22] Varma DR. Managing DICOM images: Tips and tricks for the radiologist. *Indian Journal of Radiology and Imaging*. 2012; 22(1): 4-13.
[23] Zeng L, Huang L. *A Research on the Medical Image Authentication Watermark Method Based on Chaos*. International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC). 2013: 1679-1683.
[24] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*. 2004; 13(4): 1-14.
[25] Zhang H, Wang C, Zhou X. Fragile watermarking for image authentication using the characteristic of SVD. *Algorithms*. 2017; 10(1): 27.
[26] Benrhouma O, Hermassi H, El-Latif AAA, Belghith S. Chaotic watermark for blind forgery detection in images. *Multimedia Tools and Applications*. 2016; 75(14): 8695-8718.
[27] Rawat S, Raman B. A chaotic system based fragile watermarking scheme for image tamper detection. *AEU-International Journal of Electronics and Communications*. 2011; 65(10): 840-847.
[28] Su K, Kundur D, Hatzinakos D. Statistical invisibility for collusion-resistant digital video watermarking. *IEEE Transactions on Multimedia*. 2005; 7(1): 43-51.