Multiple Watermarking On Digital Medical Images for Tamper Detection and Integrity Control

M.T. Kurniawan
Graduate School and Faculty of Industrial Engineering, Telkom Institute of Technology, Bandung, Indonesia
E-mail: ujangtegoeh@gmail.com

Adiwijaya
Faculty of Science, Telkom Institute of Technology
Bandung, Indonesia
E-mail: adiwijaya@ittelkom.ac.id

Wiseto Agung
R&D Center, PT. Telekomunikasi Indonesia
Bandung, Indonesia
E-mail: wiseto.agung@gmail.com

***Abstract*—In the current digital era, patient data in the form of digital medical images in several hospitals are widely used. There are two important thin to use of digital medical images namely the ownership authority (integrity control) and the authenticity of the image (authentication), because digital medical images are very easily manipulated. To maintain the authority of ownership, it needs robust watermarking techniques in which the embedded data is not easily damaged if the image has been manipulated. Meanwhile, to detect the authenticity of the image, it needs fragile watermarking technique in which the embedded data is easily damaged if the image has been manipulated. In this paper, we implement Reed-Solomon code for robust watermark in wavelet domain and SHA-256 for fragile watermark in Hash Block Chaining. The proposed multiple watermarks can be implemented simultaneously on an image so that the integrity control and authenticity of the image detection can be applied at once.**

Keywords-component; Multiple watermarking, medical images, robust watermarking, fragile watermarking

I. INTRODUCTION

Nowadays, patient's data in the hospital can be stored in electronic media. The data in digital medical images form such as X-ray image, mammogram form and others can be very easily manipulated by the rapid development of information technology today. Medical images in digital form must be stored well to preserve stringent image quality standards and prevent unauthorized disclosure of patient data [4].

There are two important things must be concerned in digital medical images such as the authority of ownership (Integrity control) and the authenticity of the image (Authentication). As consequences to ward these cases it is necessary to apply watermarking techniques. The principle of watermarking is embedding digital data (either text or image) into the original digital medical image to meet the needs of integrity control (to maintain the authority of ownership) and Authentication (to detect the authenticity of the image).

. Multiple watermarks has two parts: signature watermark in the form of robust watermark and reference watermark in the form of fragile watermark [4]. Signature watermark is used to maintain the authority of ownership because it has robust characteristic that is not prone to damage if the embedded image is manipulated so the data remains safe. The reference watermark is used to detect the authenticity of the image. This reference watermark is highly vulnerable to the manipulation of imagery, however due to its fragility that will easily detect the manipulation of the image so that the authenticity of the image can be maintained [1].

Methods used to embed a watermark in digital medical images are very diverse. The first is a watermark on the image method which does not allow embedding in the image areas that are considered important (Region of Interest). Although this method produces good image quality in the ROI area, but the main problem is that it is easy to do copy attack in the area (areas that are not embedded watermark).

II. MULTIPLE WATERMARKING

Multiple watermak has two watermark namely robust watermark for integrity control and fragile watermark for tamper detection. There are several research in mutliple watermarking. Woo, et al. [4] proposed method multiple watermarking on digital medical image which is suitable for privacy control and tamper detection in medical images. To provide data security and patient privacy, patient information embedded into an annotation watermark. This annotation watermark is embedded into RONI (region of non interest) image using a robust embedding method. Then, it is embedded using a linear additive method into the three high pass bands of discrete wavelet transform (DWT) of original image border or RONI. And to provide integrity of the medical image can be authenticated using a fragile watermark. This fragile watermark is embedded into the ROI (region of interest) image using the least significant bit (LSB) method.

Kallel, et al. [1] proposed to use the following scheme in order to preserve the image history in the digital medical field. This method divided into two parts. The first one is to embed the patient's diagnoses in the digital medical images

978-1-4244-9983-0/11/$26.00 ©2012 IEEE

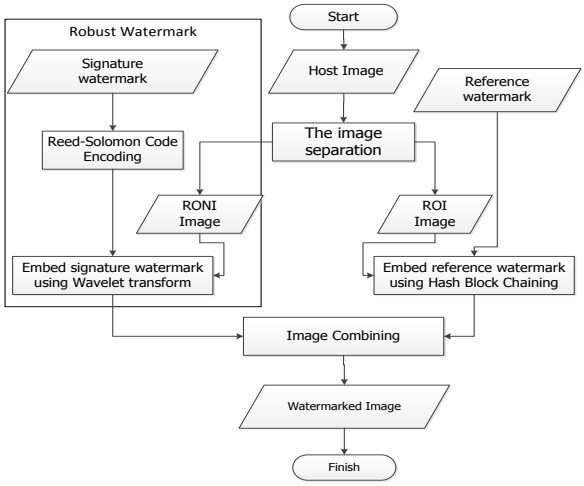
and the second is about how to extract it [3]. Two watermarks is embedded into original image using the least significant bit (LSB) method.

Memon, et al. [2] proposed scheme embeds two different types of watermark namely, robust watermark and fragile watermark. Robust watermark is embedded in the high frequency coefficient of Integer Wavelet Transform (IWT) of RONI. And fragile watermark is embedded using the least significant bit (LSB) method.

III. PPOPOSED SCHEME

Multiple watermarks system in the medical image consists of three main processes, namely the embedded of watermark in the host image, the provision of attack at a watermarked image, and the extraction of the watermark from the watermarked image both embed attack or not. There are two types of watermark to be embedded, namely a signature watermark in the form of text and reference watermark in the form of binary image.

The following algorithm of multiple watermarking was implemented into two parts. The process input was digital medical images where the image is divided into two parts, namely the Region of Non-Interest (RONI) part of the medical image and the Region of Interest (ROI) center of medical images. Signature watermark is embedded at RONI image based on wavelet domain. The signature watermark is encoded by Reed-Solomon code in order to protect the text. This watermark is used to maintain the authority of ownership (Integrity control) so it must be robust. Meanwhile, reference watermark is embedded at ROI image using Hash Block Chaining (HBC) method. This watermark used to detect the authenticity of digital medical images (Authentication) so it must be fragile. We proposed multiple



watermark system as show in Figure 1.

Figure 1 Embedding Process

When RONI and ROI images has been splitted, the watermark signature encoded first by using the Reed-Solomon Code. After that, the Codeword (the message of encoded signature watermark) is embedded in the coefficients of decomposition result of Discrete Wavelet Transform (DWT) in the RONI image by using Mother Wavelet Daubechies. Meanwhile, the reference watermark is embedded into ROI image by using the Hash Block Chaining. The hash function to be used is SHA-256 with the MAC technique. After the embedding process, both in RONI and ROI images, the next step is to merge the parts into a whole image that has been watermarked

In the extraction process, the reference and signature watermark are extracted separately.. So as to extract the watermark and the reference signature watermark, the watermark image (the result of multiple watermarking either has or has not been subjected to attacks) separated in advance to get RONI and ROI image. Signature watermark extracted using Wavelet transformation. Then the extraction decoded again using the Reed-Solomon Code in order to repair if there are bits in error on the extraction. Decode the message that this is the signature watermark previously embedded in the medical image. Before extraction watermarked image give attack is illustrated in figure 2.

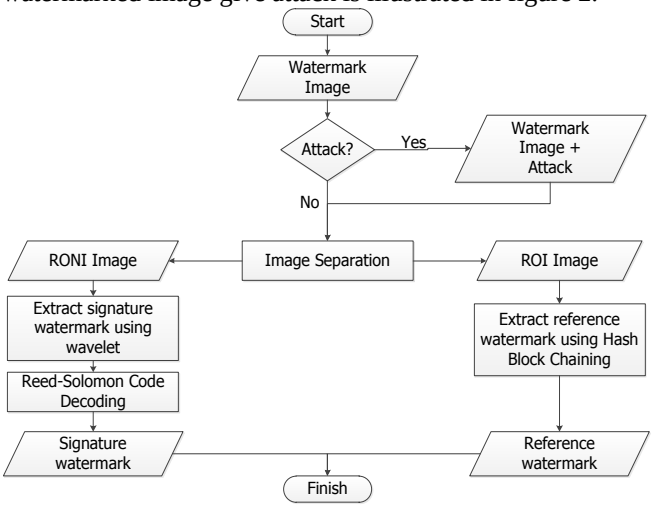


Figure 2 Extraction Process

IV. EXPERIMENT RESULT

After the system was implemented in accordance with the design that has been made, the system is tested so that the performance can be measured. The objective of this test is to find out the level of robustness signature watermark, the level of fragility reference watermark, and the quality of watermarked image.

The embedded of signature watermark uses the Reed Solomon Code and is Wavelet-based, while the embedded of reference watermark uses the Hash Block Chaining. The Reed-Solomon Code used is RS (7.3) while the hash value used is the MAC value with the hash function SHA-256.

The host images used in the testing of multiple watermark system were the 8 bit bitmap format grayscale images with 512 x 512 pixels size. For the signature watermark, the texts used were those that had two sections of text: for doctors and for patients. The ROI size used in

the testing varies, with the maximum length of character for patients and various length of character for doctors depending on the ROI size used in the testing. For the reference watermark, the image embedded is in form of binary image with various sizes.

One of the conditions that the watermarked image is said to have great result is the quality of the image is not decreased significantly compared to the original one, and the embedded watermark also has a high imperceptibility value. The parameter that can be used to measure the quality of the watermarked image is PSNR. This parameter is types of objective assessment.

Besides that subjective assessment was done in this research. Whereas the subjective assessment is performed by human eye sight, then the result is calculated by expert assessment (the radiology medical doctor).

Figures 3, 4, and 5 show an effect of scale factor, subband wavelet, and Block Size HBC to quality of watermarked image.

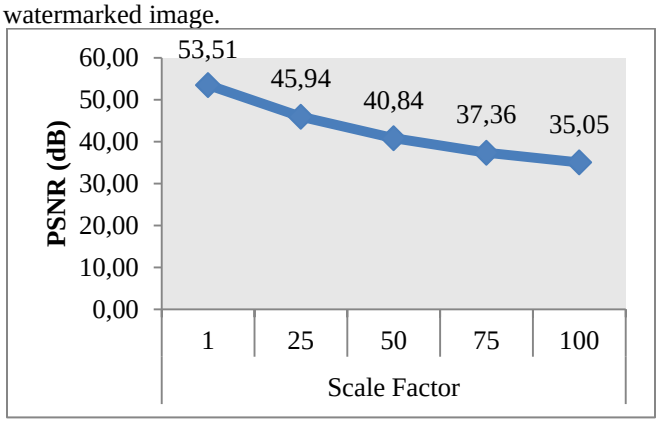


Figure 3 Effect of scale factor.

As can be seen in the figure above, the scale factor has effect on the signature watermark embedding. The larger the scale factor, the bits that are embedded into the signature watermark will change too. This is in accordance with the formula below in which the scale factor is a multiplier of the codeword generated by a Reed-Solomon encoder. The larger the scale factor used, the bigger the change of bits in the host image as show in the equation below.

$$Vw_{i,j}^{k} = V_{i,j}^{k} + \alpha_k \cdot W_{i,j}$$

where :

$Vw^{k}_{i,j}$: coefficient in k-subband after modified. k = 1, 2, 3, 4.
$V^{k}_{i,j}$: original coefficient in k-subband before modified.
α_k : embedding scale factor for k-subband.
$W_{i,j}$: signature watermark bits to be embedded.
k : 2D DWT decomposed subband *(1 = LL, 2 = LH, 3 = HL, 4 = HH)*

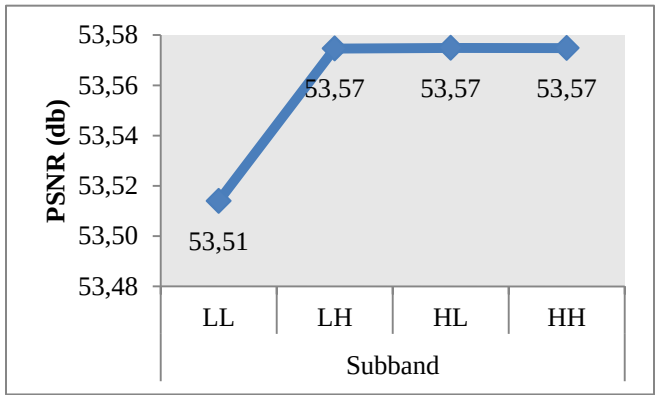


Figure 4 Effect of subband

The selection of subband as the location of signature watermark insertion has effects on the PSNR watermarked image. The watermark embedding in a different subband produces a different image quality as well. The signature watermark embedding in subband LH, HL and HH has a better quality than that in subband LL. It can be seen from the PSNR values in subband LH, HL and HH which are larger than that in subband LL. This is because when the forward 2D DWT transformation is performed, the subband LL has the largest energy compared to the other three subbands. Thus, if part of the image that has the largest energy is lost, then the image quality will decrease as well. Overall, the watermarked images have good quality, which is seen from the average PSNR values for all the test data that reach 53.55 dB.

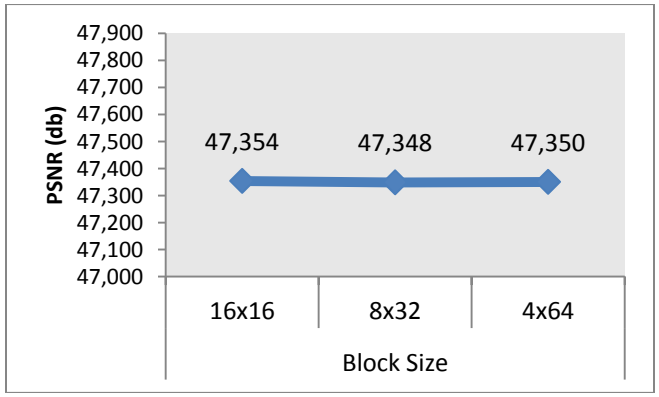
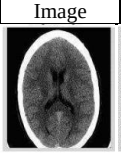
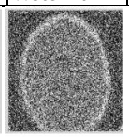
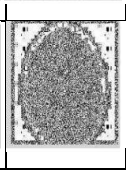


Figure 5 Effect of Block size HBC

In the figure above, it is seen that the block size used does not really affect the quality of watermarked image. This is because the MAC value of each block will be calculated and then the results will be converted into a binary format. Although the size of the blocks are different, but the MAC output for each block is in the same size that is 256 bits. Thus, the embedded does not really change the pixel values of the host image and the PSNR values resulted are not much different. For all the tested data, the average PSNR value is 47.35 dB

Comparison with Woo, et al. [1] fragile watermark for tamper detection

Table 1 Comparison of fragility

No	Attack	Woo, et al [4]		Proposed method	
		Original Image	Detected Watermark	Original Image	Detected Watermark
1	Gaussian noise 0.0002				
2	JPEG Compression quality factor 90%				

From the table above shows that the Fragility of fragile watermark in the proposed method with a hash block chaining method was more fragile. This can be seen from the image after the extraction image generated by the proposed method is more damaged compared with the previous method.

Each character has its own ASCII code in which the ASCII code can be converted into an 8-bit binary number. Reed-Solomon Code, particularly the RS (7.3) as one of the types of Error Correction Code (ECC), is able to encode each 8 bit into a codeword whose length is 8 bits and is able to correct errors as much as 2 bit. To test the use of Reed Solomon code, it was performed the Gaussian noise attacks with various SNR values. The following are the results of the tests on the influence of the use of error correction code.

Table 2 Effect of Using ECC to CER

NO	SNR	CER (%)	
		Without ECC	With ECC
1	20	82.63	82.91
2	30	67.24	36.03
3	40	29.54	10.93
4	50	12.02	3.77
5	60	5.49	0
6	70	2.06	0
7	80	1.01	0
8	90	0.93	0

As can be seen in the Table 2, there is a difference in the CER percentage between that uses ECC and that does not use it. By using the ECC, the CER percentage is always smaller than that does not use it. Reed-Solomon (RS) code as ECC has the ability to detect 2 bit errors for each 8 bit. The use of RS can improve the resistance of the signature watermark, compared to that does not use it at all. In average, the Reed-Solomon Code is able to reduce as much as 8.4% of the CER without RS.

V. CONCLUSION

In this paper, multiple watermarking systems has been presented. The proposed method has two watermark namely robust watermark for integrity control and fragile watermark for tamper detection. The fragility of reference watermark is very good. With a small value attack, which is 0.0002 and quality factor JPEG 90%, the reference watermark is experiencing a serious damage. And the robustness of signature watermark with ECC better than without ECC. The used of ECC (Reed-Solomon Code) can be reduced as much as 8.4% CER (SNR Gaussian noise attack 20-90 dB) rather than without Error Correction Code. For future works to improve the robustness of signature watermark, Reed Solomon code with higher order or other ECC method can be explored. And then to test the robustness of signature watermark and fragility of reference watermark of medical image, malicious attacks can be utilized. There problems will be investigated in our going work.

ACKNOWLEDGMENT

The authors would like to thank Graduate School and Faculty of Industrial Engineering, Telkom Institute of Technology for supporting this research.

REFERENCES

[1] Kallel, M., Lapayre,, J.C., Bouhlel, M.S., *A multiple watermarking sheme for Medical Image in the Spatial Domain*, Sciences and Technologies of Image and Telecommunications (SETIT),ISBS, 2007.

[2] Memon N.A., "Multiple Watermarking of Medical Images for Content Authentication and Recovery" Multitopic Conference, 2009. INMIC, pages 305-310, 14-15 Dec. 2009.

[3] Miller, M., Doërr, G., and Cox I.. Applying informed coding and informed embedding to design a robust, high capacity watermark. IEEE Tran. Image Processing, 13(6):792–807, June 2004.

[4] Woo, C. S., Du, J., and Pham, B. L. *Multiple Watermark Method for Privacy Control and Tamper Detection in Medical Images*, Proceedings APRS Workshop on Digital Image Computing (WDIC2005), pages pp. 59-64, Brisbane, Southbank, 2006.