The usage of block average intensity in tamper localization for image watermarking

CONFERENCE PAPER · OCTOBER 2011

DOI: 10.1109/CISP.2011.6100301

2 AUTHORS:

Siau-Chuin Liew
Universiti Malaysia Pahang
24 PUBLICATIONS **30** CITATIONS
SEE PROFILE

Jasni Mohamad Zain
Universiti Malaysia Pahang
69 PUBLICATIONS **293** CITATIONS
SEE PROFILE

The Usage of Block Average Intensity in Tamper Localization for Image Watermarking

Siau-Chuin Liew
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Kuantan, Malaysia
eliewsc@gmail.com

Jasni Mohamad Zain
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Kuantan, Malaysia
jasni@ump.edu.my

***Abstract*—Tamper localization capable image watermarking scheme is able to detect the location of manipulated areas, and verify other areas as authentic. The usage of block average intensity in the tamper localization process is one of the popular techniques due to its easy implementation. The effectiveness of using average intensity for tamper localization had not been properly tested. Experiments were performed using a tamper localization watermarking scheme for medical image which is based on block average intensity. The results shows that the tamper localization process will fail in certain conditions and caused some tampering left undetected.**

Keywords-component; tamper localization; medical images; block average intensity;effectiveness

I. INTRODUCTION

Watermarking can be used in medical images to prevent unauthorized modification by authenticating the content of the image. Tamper localization capable watermarking scheme can detect and locate modification of pixel values on the image. Tamper localization is useful for deducing the motive of the tampering and whether any modification is legitimate.

Tan et al. [1] proposed a tamper localization watermarking scheme. The image is divided into 16 x 16 pixel blocks and Cyclic Redundancy Code (CRC) is computed for each block. Each CRC is embedded into its own block and in the event that the CRC cannot be embedded into its own block, the remaining bits will be carried over to the next block. The watermarked image can be verified by extracting the watermark and comparing the CRC of each block. Any mismatch of CRC values during comparison indicates tampering. Other type of tampering localization technique is by using block average intensity. Chiang et al. [2] divides an image into blocks. The authentication information is generated by taking the average pixel value of each block and embedded as watermark. The whole image can be verified by comparing the retrieved average pixel value from the watermark with the current average pixel value of the image. Any mismatch indicates tampering and tampered region can be localized to an accuracy of 4 x 4 pixels. Osamah and Khoo [3] had also used the same technique. A region of interest(ROI) is defined and divided into 16x16 pixel blocks. Average intensity of each block is embedded as part of the watermark. Tamper localization is done by comparing the average intensity of each block in the ROI with the retrieved average intensity from the watermark.

The usage of block average intensity in tamper localization is popular due to its easy implementation. The usage of average intensity significantly reduces the watermark payload because the authentication information is generated for a group of pixels rather than each pixel in an image. At the same time, the block average intensity can also be used as the recovery information of tampered blocks. This directly reduces the total watermark payload. The effectiveness of using average intensity for tamper localization had not been properly tested. The objective of this paper is to perform further effectiveness test on the previous work done by Liew and Jasni [4] where average intensity was used in the tamper localization process. The next section explains the usage of block average intensity in tamper localization. It is followed by the experiment results. The discussion of the results is in section four. The final section is the conclusion.

II. TAMPER LOCALIZATION

One of the requirements of an effective watermarking based authentication system is the ability to identified manipulated area or also known as localization where the authentication watermark should be able to detect the location of manipulated areas, and verify other areas as authentic [5]. The tampered area can be recovered using information that is stored as the watermark.

Block average intensity had been used in the scheme developed by Liew and Jasni [4]. This scheme divides an image into blocks and each block is further divided into sub-blocks as shown in Fig.1. Average intensity of the block and its sub-blocks will be used in the authentication and recovery process. The average intensity of a block is calculated based on:

$$\text{Block average intensity} = \frac{(P_1+P_2+P_3\ldots+P_{15}+P_{16})}{16} \quad (1)$$

978-1-4244-9306-7/11/$26.00 ©2011 IEEE

where P_1 to P_{16} are the pixels intensity in a block. The average intensity of a sub-block is:

$$\text{Sub-block average intensity} = \frac{(P_1+P_2+P_5+P_6)}{4} \quad (2)$$

where P_1 ,P_2 , P_5 and P_6 are the pixels intensity in a sub-block.

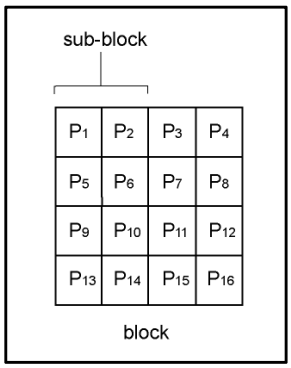


Figure 1. A block divided into four sub-blocks.

The authentication information for each block consist of one bit of authentication bit and one bit of parity check bit which are generated with the following algorithm:

- The average intensity for block denoted as x1 and its sub-blocks, x1s will be computed, denoted by avg_x1 and avg_x1s respectively. As an example, the value for avg_x1 is 85 and the values for avg_x1s are 99, 84, 81 and 77 respectively as shown in Fig 2.
- Generate the authentication bit, v, of each sub-block as:

$$v = \begin{cases} 1 & \text{if avg\_x1s} \geq \text{avg\_x1}, \\ 0 & \text{otherwise}, \end{cases} \quad (3)$$

- Generate the parity check bit, p, of each sub-block as:

$$p = \begin{cases} 1 & \text{if num is odd}, \\ 0 & \text{otherwise}, \end{cases} \quad (4)$$

where num is the total number of 1s in the seven most significant bits of avg_x1s.

The authentication information generated is embedded as the watermark together with the block average intensity that will be used for recovery purposes.

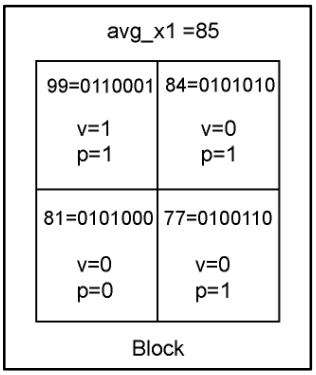
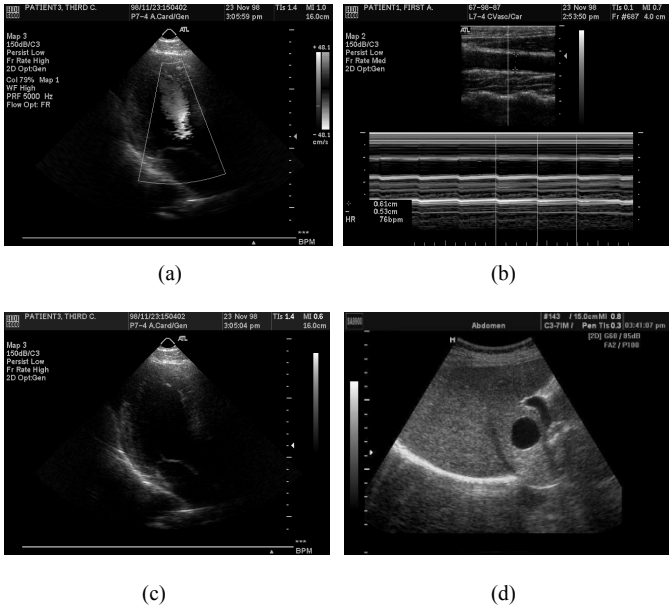


Figure 2. Block x1 is divided into sub-blocks with its computed average intensities to generate value for v and p

III. RESULTS

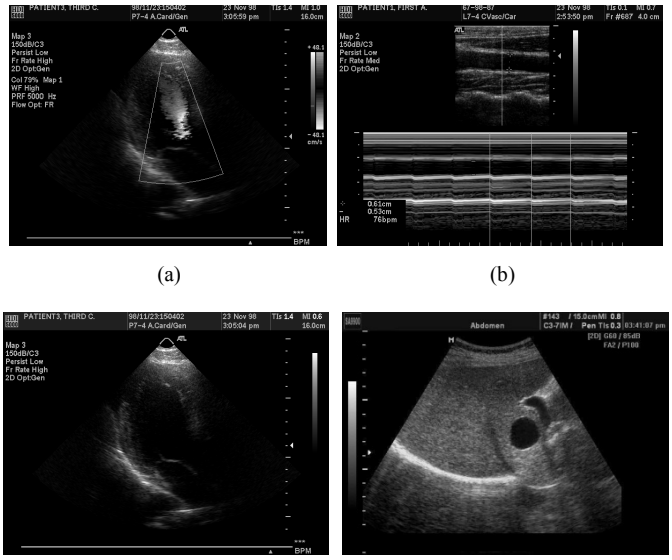
Experiments were carried out by watermarking four different ultrasound images as shown in Fig.3. The ultrasound images are in 8-bit monochrome grayscales and 640x480 pixels in size. The watermarked images are shown in Fig.4.



(a) (b)

(c) (d)

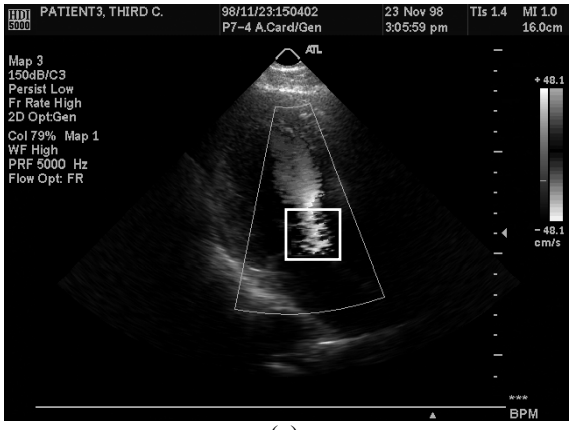
Figure 3. Original images (a) Sample 1 (b) Sample 2 (c) Sample 3 (d) Sample 4



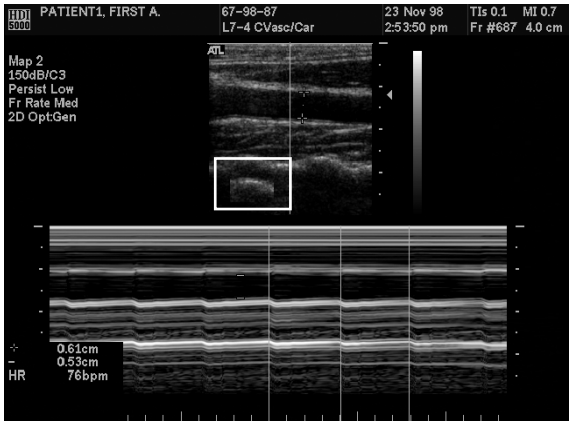
(a) (b)

(c) (d)

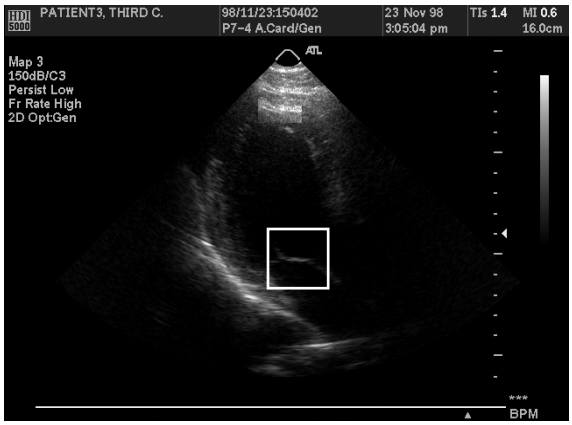
Figure 4. Watermarked images (a) Sample 1 (b) Sample 2 (c) Sample 3 (d) Sample 4



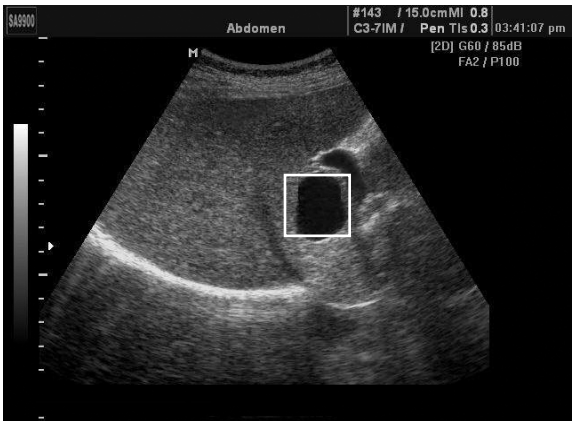
(a)



(b)



(c)

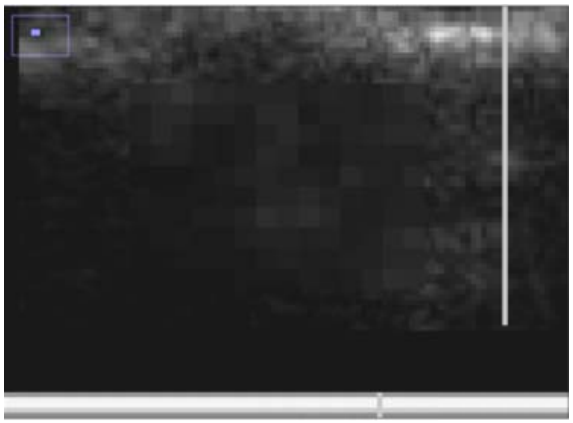


(d)

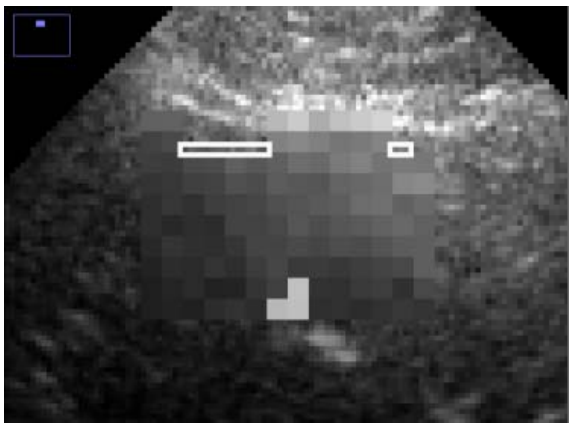
Figure 5. Highlighted area had been manipulated (a) Sample 1 (b) Sample 2 (c) Sample 3 (d) Sample 4

The watermarked images were tampered by cloning the highlighted area measuring 50 x 30 pixels as shown in Fig.5. The recovered image is shown in Fig.6. The tampered area for Sample 3 and 4 which were not detected is highlighted. The success rate for each sample is shown in Table I. The average tamper localization and recovery success rate is 99.99%.

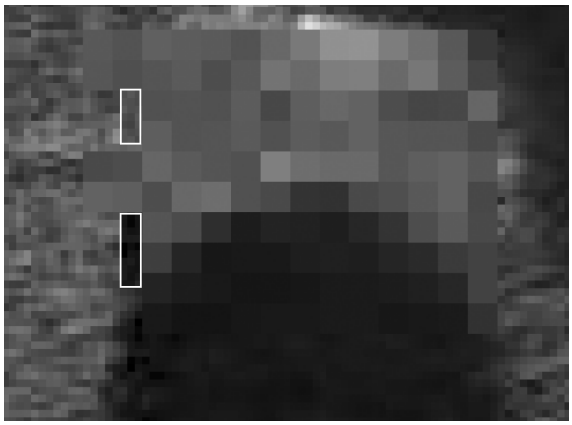
(a)



(b)



(c)



(d)

Figure 6. Recovered images (a) Sample 1 (b) Sample 2 (c) Sample 3 with undetected area highlighted (d) Sample 4 with undetected area highlighted

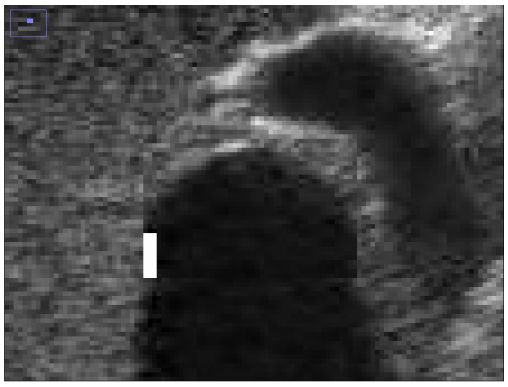


Figure 7. The undetected area of Sample 4 was painted in white and the rest of the tampered area is identical with Fig.5(d).

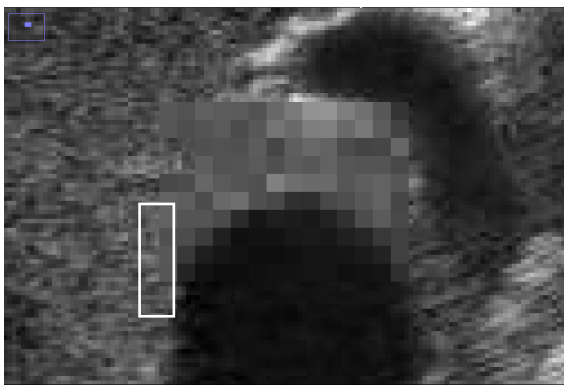


Figure 8. Tampered area had been recovered as highlighted

TABLE I. : NO. OF UNDETECTED PIXELS AND TAMPER DETECTION RATE FOR EACH SAMPLE

	1500 pixels tampered	
	No. of pixels undetected	**Success rate(%)**
Sample 1	0	100
Sample 2	0	100
Sample 3	19	99.99
Sample 4	50	99.97
	Average	99.99

The watermarked image of Sample 4 was used and the tampered region was modified as shown in Fig.7. One area which tampering was previously undetected was painted in white and the rest of the tampered area is identical with Fig.5(d). The recovered image in Fig.8 shows the area tampered in white which was previouly undetected was detected and recovered.

IV. DISCUSSION

Based on the experiments performed, some tampered areas were not detected as shown in Fig.6(c) and 6(d). Tampering in Sample 4 was detected when the same location was tampered with a different pixel value as shown in Fig.7 and Fig.8. It clearly shows that the authentication bit and parity bit check was ineffective. A further analysis was done based on the following Fig.9. As an example, the average intensity of the block, avg_x1 is 85. The average intensities for its sub-blocks are 99, 84, 81 and 77. The values of v and p were computed based on the average intensities and embedded as part of the watermark. The two sub-blocks in the first row were tampered where the average intensities had been changed to 101 and 82 respectively. The value of avg_x1 remains unchanged. During the tamper detection process, the authentication bit and parity check bit is computed, denoted as v' and p'. The values of v' and p' for the two sub-blocks in the first row remained unchanged. In this situation, the tampered sub-block will pass the detection process and left unrecovered when the embedded v and p were retrieved for comparison.

V. CONCLUSION

The usage of block average intensity in tamper localization is easy to perform without much computation needed. It can also be used for recovery purposes. Based on the experiments and analyses performed, the tamper localization technique that is based on block average intensity will fail in certain conditions even with the additional usage of authentication and parity bits. The main weakness lies within the technique of using block average intensity. Other schemes that were developed based on block average intensity in the tamper localization process may also have the same weakness. It is crucial that the tamper localization process in image watermarking to achieve 100% success rate so that any malicious tampering can be detected especially in protecting medical images. A more reliable technique in tamper localization is needed.

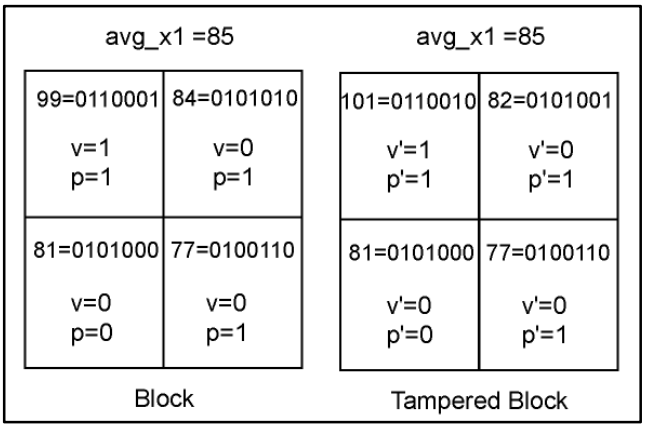


Figure 9. The authentication bit and parity check bit for the original block and tampered block

ACKNOWLEDGMENT

We would like to thank Research and Innovation Centre of University Malaysia Pahang for the financial support provided for the research work.

REFERENCES

[1] Tan,C.K., Ng,C., Xu,X., Poh C.L., Yong, L. G. and Sheah, K., "Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability," *Journal of Digital Imaging*, vol. 24, no.3, pp. 528-540, June 2011, doi: 10.1007/s10278-010-9295-4.

[2] Chiang,K., Chang, K., Chang, R. ,Yen, H., "Tamper Detection and Restoring System for Medical Images Using Wavelet-Based Reversible Data Embedding," *Journal of Digital Imaging*, vol. 21, no.1, pp.77-90, Mac 2008, doi: 10.1007/s10278-007-9012-0.

[3] Osamah,M.,Khoo,B. E., "Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images," *Journal of Digital Imaging*, vol. 24, no.1, pp.114-125, Feb 2011, doi: 10.1007/s10278-009-9253-1.

[4] Liew, Siau-Chuin, Jasni M. Zain, "Reversible Tamper Localization and Recovery Watermarking Scheme With Secure Hash," *European Journal of Scientific Research*, vol. 49, no.2, pp. 249-264, Jan 2011, ISSN:1450-216.

[5] Liu, Tong, Qiu,Zheng-ding, "The survey of digital watermarking-based image authentication techniques," Proc. 6th International Conference on Signal Processing, pp. 1556- 1559, Aug 2002, doi:10.1109/ICOSP.2002.1180093.