A Fragile Watermark Method for Improving Medical Images Security

Liangyong Huang

1. Department of Mathematics and Computer Science, Liuzhou Teachers College, Liuzhou, Guangxi, China
2. College of Information Engineering, Wuhan University of Technology, Wuhan, Hubei, China.
Email: huangliangyong@126.com

***Abstract*—Aiming at the medical images security problem during storage and transmission, the author provides a fragile watermark method to protect it. And this method can be able to achieve integrity detection and accurate tampering localization. This method adopts image block, chaotic modulation in watermark information and encryption to set password. The watermark information will be embedded to the least significant bits of original medical image's sub-block area. Experimental results show that the algorithm has the following features: (1) The watermarked medical images has high and stable quality. (2) It is sensitive to manipulations, and any manipulation of any pixel can be detected. (3) The tampering localization can be accurate into 2×2 pixel area. (4) The algorithm achieves the blind detection with high security.**

***Index Terms*—medical images, fragile watermark, integrity detection, tampering localization**

I. INTRODUCTION

The medical images, produced by diagnostic equipment, such as X-ray images, ultrasound images, endoscopic images, microscopic images, tomography and magnetic resonance images, has widely applied to the whole progress of clinical activities. It plays an important role in medical diagnosis, accounting for 70% -80% or more in medical information [1]. The medical image not only increases in number, but also doubles in capacity. Numerous data of it does not only take large memory and store space, but brings potential risks to the management of information. The extensive application of Picture Archiving Communicating System (PACS) provides a good platform to information management in hospital [2]. However, because the low security level of public network platform, medical images and doctor-patient information cannot be protected and certificated effectively. And the data sharing between hospitals is limited. Therefore, the PACS systems of each hospital are like "information isolated island", which restricts the application of PACS and the integration goal between medical institutions at all levels and academic communities [3]. With the rapid development of computers and network technique, it is difficult to avoid the problems, like the illegal diffusion of medical images information, the deliberate manipulations and falsifications of doctor-patient information or even medical disputes due to these manipulations and falsifications. Therefore, the integrity, authenticity and credibility of medical images seem to be very essential. It is urgent for the market to have a feasible technology to defend the security of medical images.

Digital watermarking is an effective technology to protect the copyright and information security of digital products. As an important branch of the study for information hiding technology, it is used to testify the copyright of the products and provide evidences to authenticate and prosecute illegal tort. At the same time, it ensures the integrity and credibility of image information by testing and analysis of watermarks, becomes effective measure of property rights protection, multimedia security and safety certification of information, and supplies the reference and decision for the medical diagnosis and academic communication [4]. Although some progress is made in the digital watermark technology applied to the study of the identification and protection of medical images, the result is unsatisfying. The recent researches show that it realizes the tampering detection and localization of medical images with the method of discrete cosine transform [5] and discrete wavelet transform [6-8]. we can also adopt the reversible watermarking technique to protect medical images [9-10], but it has smaller watermarking storage by using these methods, and it can not be able to achieve tampering localization when the image is tempered. But, due to the adoption of bigger image block, it can only tamper the position to image sub-block, relatively reducing the accuracy of algorithm to tamper the position. The Image is protected by embedding the image sub-block to vary capacity of watermark information in documents [11-12], but the change of capacity leads to the instability of image quality after embedding watermark information. In this research, we believe that the key points of designing the fragile watermark algorithm are as follows. (1) The invisibility is good, which means that it is impossible for human eyes to perceive the watermark and distinctions between the original and watermarked medical images. It is significant for medical images. (2) The sensitivity of the tampering detection is high. That is, any modification can be detected after medical images are embedded with

Manuscript received September 16, 2013; revised November, 2013; accepted December, 2013.

Copyright credit, No. 201203YB185 , No.2013YB280, Liangyong huang, etc.

doi:10.4304/jcp.9.9.2043-2049

watermark. (3) With the ability of tampering localization, it can position the manipulation area more accurately, providing effective references for further decisions. (4) Blind detection that means the original medical images is unnecessary when testing. For watermark system of medical images identification, the users are unaware of them. In general, there is no need to make integrity detection if the original has been known, so the testing of watermark must achieve blind detection. (5)The algorithm is safe. The algorithm of watermark is completely open. Though the attackers know it, they do not know the keys, so they cannot embed, extract, replace or modify the watermark.

Based on the above requirements, we adopt chaotic technology and provide the algorithm of totally fragile watermark identification, used for integrity detection and tampering localization of medical images. This paper focuses on the integrity detection and accurate tampering localization of medical images.

II. The Selection and Pretreatment of Watermark Information

A. The Selection of Watermark Information

Image block is a common method in digital watermark technology. It disposes medical images in divided blocks, which obviously can improve the capacity of embedding water information. Nevertheless, in order to position the area of tampered medical images precisely, the smaller blocks are better for the precise relative positions. Thus, considering the position accuracy and capacity of embedding watermark information, this paper proposes the designing scheme of water information generation. The scheme is the original medical images in 2×2 pixels not overlapping the blocks, then calculating gray mean (exact value) of 6 bytes in 4 pixels of image blocks and encoding them to binary system as watermark information of this image block. For this, the gray mean of image blocks is identical to watermark information in theory and the generated watermark information correlates with the image block. Therefore, it can be detected accurately, when the blocks of medical images are tampered, even only one byte.

B. Pretreatment of Watermark Information

The pretreatment work of watermark information affects the effective implement of watermark system directly. Based on such consideration, we adopt the chaotic mapping system to modulate, encrypt and preprocess the watermark information to improve security of the system.

- Chaotic dynamic system and chaotic sequence
  Logistic chaotic mapping is a widely used and simple chaotic dynamic system. It can be described by nonlinear difference equation and defined as:

$$x_{k+1}=u \times x_k \times (1-x_k),\ x_k \in [0,1] \qquad (1)$$

  The initial value is $x_0 \in (0, 1)$ and u is a bifurcation parameter. When the parameter satisfies the condition $3.5699456<u<=4$, Logistic mapping is in the state of chaos. Theistically, it is proved that chaotic system is sensitive to the initial value. As to the slightly different initial value of given chaotic mapping, the system can offer plenty of unrelated and pseudo-random sequence signals that are sure to regenerate. The characteristics of the sequence information is aperiodic, not convergent, unlimited length and very sensible to the initial value. The u and x is respectively defined as *primary* and *lambda* of *key*1(*primary*1, *lambda*1) here. The probability density function generated by Logistic mapping indicates that statistical property is equivalent to white noise, so it is a pseudo-random sequence. With the certainty, ergodicity and pseudo-randomness of chaotic sequence, we use it to modulate image watering information. The information has good random, security and high complexity.

- Binaryzation and encryption of chaotic sequence
  The pseudo-random sequence generated by chaotic mapping implements the binaryzation so that watermark is safe and random, ensuring the security of the whole system. By threshold function $f(x_k)$, the real values of chaotic sequence $x_0,x_1,x_2,\ldots, x_n$ are translated into binary 0 and 1, forming the binary sequence $S_0,S_1,S_2,\ldots,S_n$. The definition of threshold function is as follows.

$$f(x_k)=\begin{cases}1 & x>=0.5\\ 0 & x<0.5\end{cases} \qquad (2)$$

  The binary sequence $S_0,S_1,S_2,\ldots,S_n$. encrypts the above watermark information by XOR operation, obtaining the watermark W_k waiting to be embedded.

  The application of chaos to modulate and encrypt watermark signal preserves the characteristics of chaotic sequence. It has good autocorrelation and cross-correlation. From the above discussion, we can conclude that the use of chaotic technology has three advantages. Firstly, it is easy to be created by using 1 dimension chaotic mapping equations only. Secondly, it can create numerous chaotic watermark signals. The key to decoding is breaking through the secret keys effectively, that is, forecasting u and x0 effectively. With exhaustive attack, it needs to research so numerous secret keys space that it is nearly impossible to decode. Hence, it has a good security. Thirdly, chaotic sequence has no periodicity. It is sensitive to the initial value. Even a tiny initial error will completely alter the following state and chaotic sequence modulates the encrypted watermark information in random. All of these measures can enhance the security of algorithm.

III DESIGNING THE METHOD OF MEDICAL IMAGE WATERMARKS

A. The Embedding of Watermark Information of Medical Images

Set the medical grey image I as $I = \{I_{(x,\ y)}|0<x<=M,\ 0<y<=N,\ 0<= I_{(x,\ y)}<256\}$. $I_{(x,\ y)}$ is the gray value of (x, y). M and N represent the length and width of images respectively and they are integer multiple of 2. (If M and N are not the integer multiple of 2, the medical image is implemented boundary treatment). The steps of embedding watermark information to medical images are shown as Figure 1.

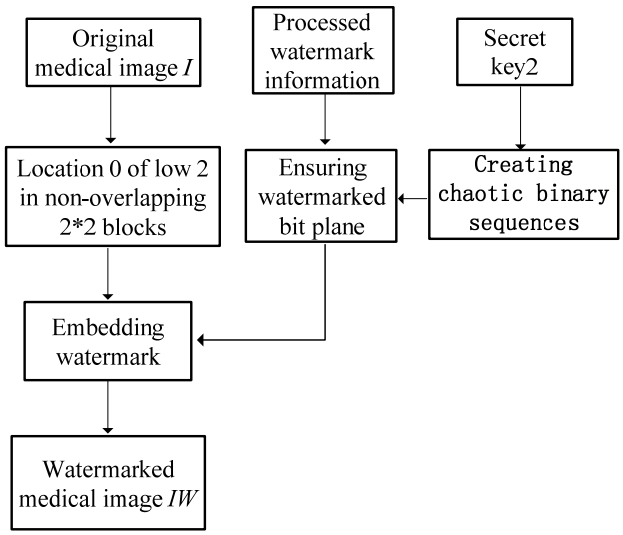


Figure 1.The insertion of watermark information

The steps of embedding fragile watermark information to medical images are as follows.

Step1: Every lowest pixel 2bits, location 0, of the original image $I_{(x,\ y)}$, does non-overlap blocks in 2×2 pixels from top to bottom and left to right, gaining every block B_k (k=1,2,3,…,M×N/4) of medical images.

Step2: In accordance with *key*2(*primary*2,*lambda*2), the binary pseudo-random sequence $S2_j$, (j=1,2,3,…,M×N) is created and its size is equivalent to image I.

Step3: If the corresponding value of $S2$ is 0 in any pixel of image block B_k, 1~4 places of block watermark information W_k are embedded to LSBs. Otherwise, it is embedded to the seventh bit of this pixel, the 5 ~ 8 planes of other watermark information are embedded to the rest. The corresponding bit plane and watermarked number are shown in Figure 2.

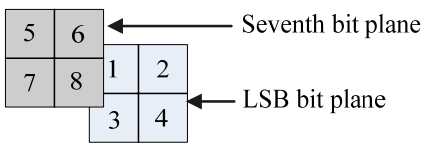


Figure 2. Bit plane of embedded watermark information

Step4: After being modulated and encrypted, watermark information W_k is embedded to current block of the lowest 2 significance bits, gaining the watermarked medical images IW.

B. The Tamper Detection and Location of Watermarked Medical Image

In order to ensure the integrity of watermarked medical images during storage and transmission, it is necessary to exact watermark information to be authenticated. What's more, when hospitals hold a consultation with other medical institutions, we need more to authenticate the integrity of the receiving images more. When hospitals make academic exchange and share resource with other communities, it is also needed. For this, the specific steps of tampering detection and localization are described as follows :

Step1: Exacting watermark information: watermark information W_k of every watermarked image block is exacted from the medical image IW to be detected.

Step2: Generating reference watermark: the medical image IW to be detected generate, encrypts watermark and bit plane, gaining the reference watermark W_k'.

Step3: Generating manipulation signal matrices: after comparing the blocks of exacting watermark W_k and reference watermark W_k' one by one, providing the blocks are equal, the valve of signal matrix *flag*(M/2,N/2) is 1, or it is 0.

Step4: Tampering detection and localization: traversing the signal matrix flag, if all value of *flag*(M/2,N/2) is 1, it passes the authentication and the image are not modulated, or image is modulated. White points show the manipulation area, while black areas pass authentication.

IV THE PERFORMANCE ANALYSIS AND SIMULATION EXPERIMENT OF WATERMARKING ALGORITHM

A. Performance Analysis

- The analysis of image quality

  Watermark information embedded in medical images should be invisible. The quality of medical images is protected as well as possible. There is no difference from human vision. PSNR (Peak Signal to Noise Ratio) is introduced to measure the quality of watermarked image in order to judge the difference between the original and watermarked image. The bigger the value is, the higher the quality is. Let the original medical mage I be 256 gray images. The watermarked image is I', so the MSE (Mean Squared Error) and PSNR are defined as follows.

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_{(i,j)} - I'_{(i,j)})^2}{M \times N} \qquad (3)$$

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad (4)$$

In paper, water information is embedded to the lowest 2bits of medical images. Let $P_{e\text{-}k}$ be probability of pixel change k (k=1, 2, 3). The mathematical expectation of square of single pixel difference between watermarked image and the original is $E\left[(I_{(i,j)} - I'_{(i,j)})^2\right] = \sum_{i=0}^{3} k^2 \times P_{e-k} = 7/2$. So the mathematical expectation of MSE and PSNR are E(MSE)=7/2 and E(PSNR)=42.69dB separately. Thus it can be seen that analyzing the algorithm of the paper can get higher peak signal to noise ratio. That is, the watermarked image has high quality and the watermark algorithm has good invisibility.

- Analysis of the tamper detection

  Whether the image is tampered or not is determined by comparing if W and W' are equal. The W matrix is obtained by partitioning IW the image containing a watermark and calculating the mean value of 4 pixels with upper 6 bits, while W' is obtained by extracting the value of the lowest 2 bits in the image IW and encrypting *key*1 and *key*2. If the two are not equal, it will indicate that the image has been tampered and the tampered position is the current block, i.e., the image block with 2×2 pixel can be located accurately. False alarm probability means the detection result reports the image has been tampered but it is not tampered actually. In accordance with the algorithm, we can know that misjudgment cannot occur because the calculation of the embedded watermark and the extracted one is completely the same in the situation that each pixel bit of the image which need to be identified is invariable. Thus, the false alarm probability of the algorithm is 0.

  False dismissal probability means the detection result does not report the image has been tampered but it has been tampered actually. For the detecting unit of a certain image block, the embedded watermark information is the gray average of four pixel points of the image block. The gray average is expressed by 8-bit binary digit. Specifically, the upper 6 bits stand for the integer part of the gray average and the last two bits represent the decimal part of the gray average. This, the embedded watermark information can present the gray average of the image block accurately. According to this, we know the algorithm will detect the image has been tampered as long as there is one-bit data change in the image information part or the watermark information part.

- Safety analysis of the algorithm

  The algorithm generates watermark information according to the content of images, uses the speciality that the chaotic mapping is featured by periodicity, misconvergence and strong sensibility to original values to encrypt the watermark information in the image content and embeds it in the 2-bit lowest plane of the image. The embedded bit position is also decided by the chaotic sequence generated by secret keys. The large threat that the fragile watermark algorithm used for the image block authentication mainly faces with is the attack on vector quantization (VQ). This algorithm utilizes the chaotic sequence under the control of two secret keys *key*1 and *key*2 to carry out encryption settlement for the image.

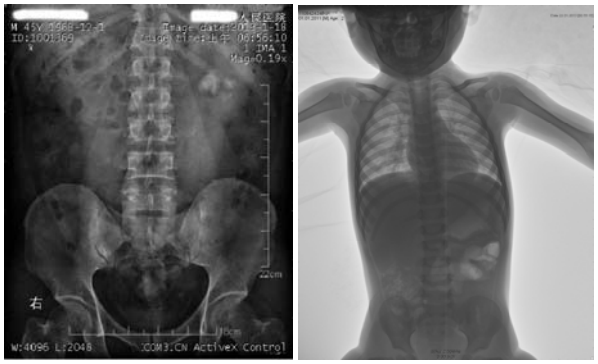
  The key1 uses the encryption of the embedded watermark information. Each bit of key1 is different from its corresponding watermark information bit, which ensures the information of each image block is different from the encryption of each pixel. The space of iterations is large enough, so it is quite difficult for attackers to use the method of exhaustion to obtain secret keys so that the safety of the algorithm is ensured. In addition, the selection of the position at which the watermark is embedded adopts chaotic scrambling technology, which makes watermark information embedded in different positions and changes the situation that traditional methods of spatial domain watermarks use the same bit plane to embed watermarks. Moreover, the application of the chaotic sequence makes any 2×2 image block in the authentication image and each pixel point correlate to its surrounding blocks or pixels, which eliminates the independence of blocks and enables each 2×2 block in the whole image to be relevant. Thus, the authentication will fail if one block or one bit is replaced, so the algorithm can completely withstand the attack on VQ.

B. Experimental Results

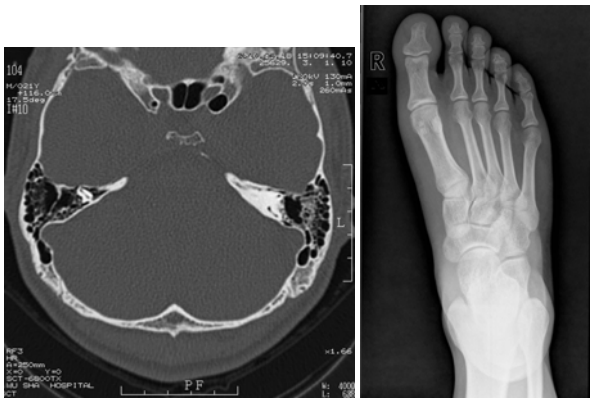
The algorithm simulates this experiment under MATLAB 7.0 platform, selecting several different types of medical images and testing them in the process of image insertion and detection. When it comes to the authentication results of medical images integrity, black area stands for no manipulation, passing the authentication and the white area represents the opposite. The whole experiment operations can be divided into two steps.

- Generation and Embedding Experiment of Medial Image Watermark

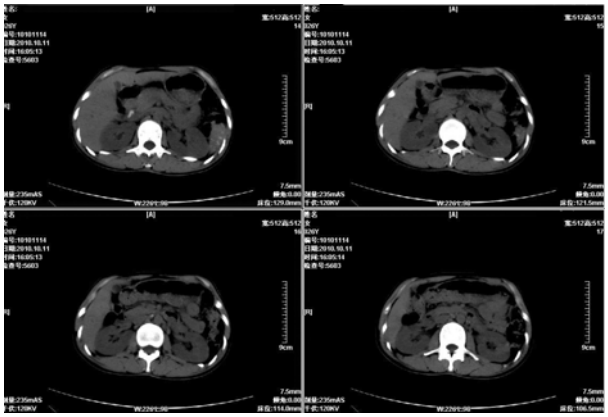
  According to the above method of watermark embedding, a medical image is embedded watermark. The effect is shown in Figure 3.



(a) (b)

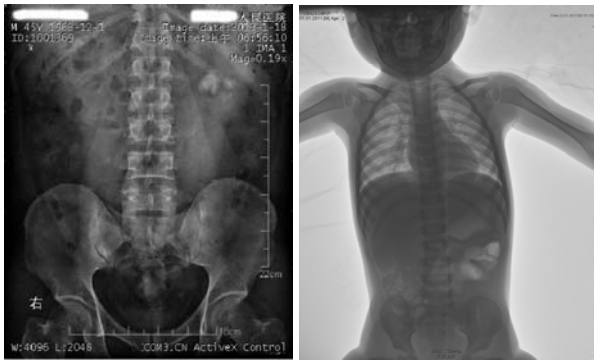


(c) (d)

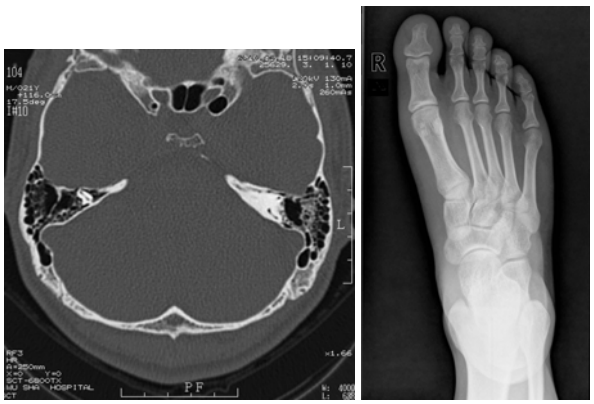


(e)

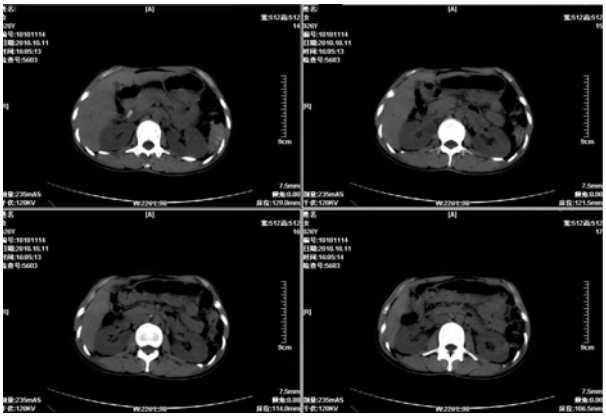
Figure3. Original medical images example



(a) (b)



(c) (d)



(e)

Figure4. Watermarked medical images

Figure 4 indicates the result when medical image is embedded with authentication watermark by this algorithm. The experiential result shows there is no difference between the embedded image and the original from human vision, without any reduction in image quality.

Table I. shows all the peak signals to noise ratio of watermarked medical image achieve over 44bB, a little higher than the results analyzing in theory. That is because a part of watermark information is the same as the original by statistical analysis.

TABLE I
PSNR OF WATERMARKED MEDICAL IMAGES

Medical images	(a)	(b)	(c)	(d)	(e)
PSNR :Peak signal to noise ratio (dB)	44.3517	44.0978	44.2682	44.1573	44.3218

It can be seen that the algorithm mentioned in this paper can gain stable PSNR, after medical images is embedded with watermark from the numerical calculation, experiential results and statistical analysis. .It has good invisibility and completely satisfies with medical images authentication's requirements in quality that watermarking algorithm cannot be seen.

- Tampering detection of watermarked medical images

  (1) Detection results of medical images tampering slightly

  Watermarked medical images is tamper by Photoshop or other image processing software in random. We make two manipulation operations to the watermarked medical image 4(a). First, change "Image Date: 2013-1-18" into "Image Date: 2018-1-18". We merely tamper the left side of "3". Second, increase a black noise point in patient's last lumbar freely. The tampered medical image is shown as Figure 5.

Figure5. Tampered medical image

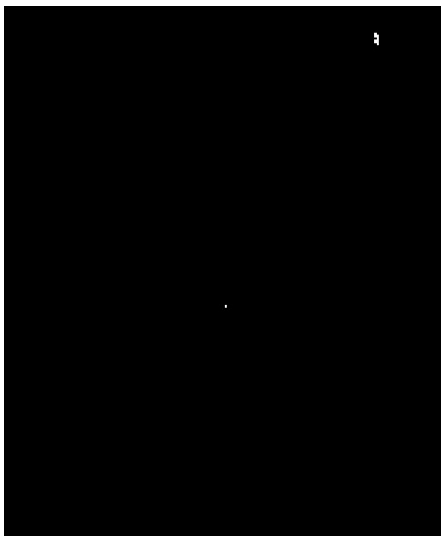


Figure6. Result of the tampering localization

By using the algorithm, tampered medical images is made integrity authentication and tamper location, gaining the tamper location result shown as Figure 6. It can be seen that it can be reflected accurately when manipulating medical images in a small area in Figure 6. And even a pixel manipulation can be detected, locating in 2×2 block. Therefore, the fragile watermark algorithm provided by this paper has good sensibility to manipulation and locates it accurately, and figures out manipulation in 2×2 the image blocks, proving the correctness of theoretical analysis.

(2)Regional manipulation and detection result of medical images

In order to check integrity authentication and tamper localization performance when the manipulation area is bigger, Figure 7 suggests the manipulation situation that this algorithm tampers watermarked medical images in bigger area. Figure 8 suggests the tampered local area in the detection test. White area is the area of tampered medical images.

Figure7. Tampered Medical Image

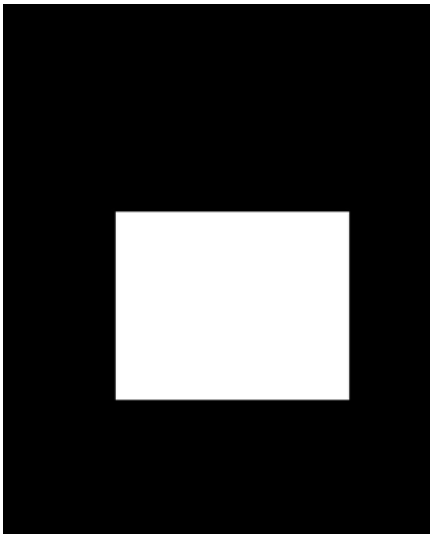


Figure8. Result of Tampering Localization

A rectangle in unified color is added to Figure 3(a), which has tampered the medical images. The area of all tampered medical images can be detected.

Although some pixel points are in accordance with filled color, the algorithm takes the blocks to be detected, so a slight alteration will be judged as manipulation in a block.

Furthermore, there is no need for the original image when watermarked medical image is authenticated. Only using secret keys can realize the tampering detection and localization. It is a safe and practical approach to authenticate the medical images.

V CONCLUSION

This paper provides a fragile watermark method to improve the security of medical images. This method can be used to realize accurate localization of integrity detection and manipulation. Meanwhile, it has a stable signal to noise ratio, realizing blind detection. It is sensitive to manipulation, with accurate localization and high security. The paper analyzes the feasibility and correctness of this method from the theory and experiential results.

ACKNOWLEDGMENT

This work is supported by the innovation fund for technology based firms, project number: 13C26214504766. and the research fund project of Guangxi university scientific research No. 201203YB185, No.2013YB280 and Liuzhou teachers college scientific research innovation team.

REFERENCES

[1] Deng X. H., Chen Z. G., Deng X. H., et al. “A Novel Dual-Layer Reversible Watermarking for Medical Image Authentication and EPR Hiding”. Advanced Science Letters, vol.4, no.11, pp.3678-3684, 2011.

[2] ZHAN Y. F., FENG X., FU C., et al. “An efficient medical image cryptosystem based on chaotic maps”. International Journal of Digital Content Technology and its Applications, vol. 6, no. 13, pp. 265-274, 2012.

[3] U. Mustafa, U. Guzin, V. V. Nabiyev. “Medical image security and EPR hiding using Shamir's secret sharing scheme”. Journal of Systems and Software, vol. 84, no. 3, pp. 341-353, 2011.

[4] Tan C. K.,Ng J. C., Xu X. T., et al, “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, 2011.

[5] Gao L, Gao T, Sheng G, et al. “A new reversible watermarking scheme based on Integer DCT for medical images”. Wavelet Analysis and Pattern Recognition (ICWAPR), 2012 International Conference on. IEEE, PP. 33-37, 2012.

[6] Qian Z., Feng G., Zhang X., Wang S., “Image Self-embedding with High-quality Restoration Capability”, Digital Signal Processing, vol.21, no.2, pp.278-286, 2011.

[7] Yong C. W., Shen J. J., “Recover the Tampered Image Based on VQ Indexing”, Signal Processing, vol.90, no.1, pp.331-343, 2010.

[8] Jian H., Zhang H. L.. “A Watermarking Scheme for Medical Images Based on the Quad tree Structures”, Journal of Computer Research and Development, vol.46, no.1, pp.11-15, 2009.

[9] N. V. Dharwadkar, B. B. “Amberker, Supriya,P. B. Panchannavar. Reversible fragile medical image watermarking with zero distortion”. In Proceedings 2010 International Conference on Computer and Communication Technology, pp. 248-254, 2010.

[10] S. C. Liew, J.M Zain. “Reversible medical image watermarking for tamper detection and recovery”. In Proceedings of 2010 3rd IEEE International Conference on Computer Science and Information Technology, vol. 5, pp. 417-420, 2010.

[11] Osamah M A, Bee E K. “High capacity data hiding schemes for medical images based on difference expansion”. Journal of Systems and Software, vol.84, no.1, pp.105-112, 2011.

[12] Chen F., He H., Wang H. “Variable-payload Digital Image Authentication, Chinese Journal of Computers”, vol.35, no.1, pp.154-162, 2012.

Liangyong Huang was born in GuangXi Province, China, in September 1971,He received the Master degree of computer software and theory from HuNan University, HuNan, China in 2009. He is currently a Ph.D. candidate in School of information engineering, WuHan University of Technology, China. His current research fields include multimedia information processing and digital watermarking technology. He has published 3 books, and more than 20 research papers in journals and international conferences. He is currently an associate professor at School of Information Science and Engineering,