EE326 Final Project Proposal:

High security blind-watermark for medical images

11911214 杨鸿嘉

1 Project Background

Telemedicine is a form of medical care using information and communication technology. Telemedicine mainly transmits data including patients' text and image records. It has many advantages, especially for remote health care institutions. However, it also has security and data protection risks. Specifically, this risk mainly comes from three aspects:

The patient's personal privacy, such as health status, may be leaked;

The patient's diagnostic information may be maliciously tampered with;

The ownership of some medical images may be controversial.

Fig 1.Medical images

Therefore, some people propose watermark to improve the security of shared images. However, traditional watermark scheme has some limitations for medical images. The inserted watermark mark often irreversibly changes the image and may hide subtle details. Blind-watermark is proposed to add watermark to the image without distortion of image details. This watermark is added to the image in spatial domain or transform domain, and the watermark can not be seen from the image itself.

New blind-watermark methods have been proposed to provide better security and robustness. At the same time, method of medical image segmentation and blind-watermark based on **region of interest(ROI)** is also proposed, which only adds build-watermark to the **non region of interest(NROI)** in the image to ensure that the important information will not be distorted.

At the same time, blind-watermark also needs to resist the noise such as bit error in communication and man-made attacks such as distortion, filtering, degradation and so on.

Based on the existing blind-watermark method, this project will optimize the efficiency and performance of the existing method by reproducing the existing scheme and testing the robustness. At the same time, the application program will be developed to realize batch adding blind-watermark and high human-computer interaction.

2 Existing Research

2.1 Classification of watermark

According to whether the watermark embedding is carried out in the spatial domain or in the transform domain, the digital watermark can be roughly divided into two categories. In the pixel domain, the watermark is directly inserted into the image pixels**[6,7]**. The algorithm based on spatial domain has low computational complexity and high hiding ability. In contrast, watermarking in transform domain require more computational overhead, but they are found to be more robust to various image processing attacks**[8]**.

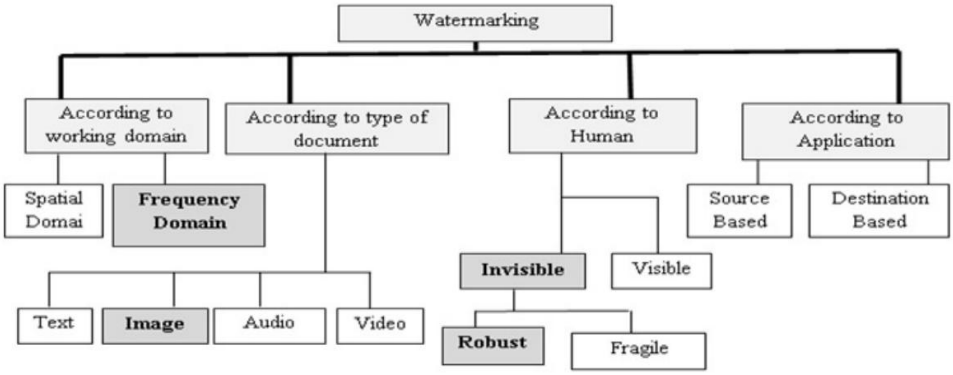

Fig 2.Classification of watermark

2.2 Main process for blind-watermark

The main process for blind-watermark is shown in the following figure:

The original image is passed through a transform and generate domain data. This transform mainly contains the spatial domain method like LBS and transform domain method like DFT(Discrete Fourier Transform), DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transformation), DWT-SVD. Also in this transform we should consider the segmentation for ROI, and this can be achieved by threshold method or deep learning.

The watermark, which may be logo or text message will go through a pre process. Some common method for this process like mapping(Arnold, Hilbert, Fibonacci) and signature(MD5, Hash) will disrupt the information and thus increase security. Also, coding like BCH can be used to reduce the impact of transmission bit errors in the channel.

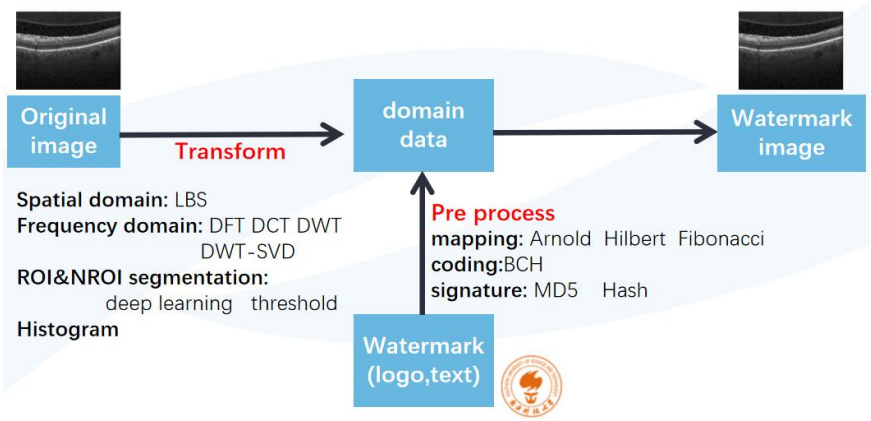

Fig 3.Main process for blind-watermark

After pre process, watermark is added to the domain data and finally generates the watermark image.

2.3 Spatial domain blind-watermark

In the spatial domain, the most common blind-watermark method is **LSB(least significant bit)**, for the least significant bit contains the least message for image, we can insert watermark in it to minimize the influence. And the insert approach is change the value of the pixels according to the coding generated from watermark.

The main measurement criteria of image watermarking algorithm are mean square error (MSE), peak signal to noise ratio (PSNR) and signal to noise ratio (SNR)**[4]**, etc.

Following shows the performance of several LSB blind-watermark researches**[5]**:

Table 1. Perceptual transparency comparison.

PSNR in dB					*Proposed scheme with watermark embedded in different planes*				
Image	*Lee et al. (2014) scheme*	*Ying et al. (2015) scheme*	*Das et al. (2014) scheme*	*Li et al. (2009) scheme*	LSB	1st ISB	2nd ISB	3rd ISB	4th ISB
Lena	41.29	43.96	41.78	43.21	68.02	62.50	57.03	53.75	44.95
Baboon	39.79	43.75	40.24	44.16	68.51	62.70	57.24	55.43	45.22
Barbara	37.21	44.25	–	–	68.70	63.80	57.20	56.90	44.98
Peppers	41.91	43.87	–	44.20	68.72	62.32	57.24	57.21	44.85
Jet	40.37	–	40.79	–	68.66	63.49	57.14	56.91	45.42

LSB: Least significant bit; ISB: intermediate significant bit; PSNR: peak signal to noise ratio.

Table 2. Perceptual quality comparison for 'Peppers'.

	PSNR in dB	
Bit plane	Zeki and Manaf (2008)	Proposed
LSB	51.20	68.72
1st ISB	51.23	62.32
2nd ISB	47.17	57.24
3rd ISB	42.41	57.21
4th ISB	37.24	44.85

LSB: Least significant bit; ISB: intermediate significant bit; PSNR: peak signal to noise ratio.

Table 1,2.Performance of related LSB blind-watermark algorithm

2.4 Transform domain blind-watermark

Transform domain mainly includes DFT, DCT, DWT, DWT-SVD, and the blind-watermark is achieved through modifying parameters of these transforms.

Following process shows the DWT-SVD transform domain blind-watermark method's integration and extraction process**[2]**.

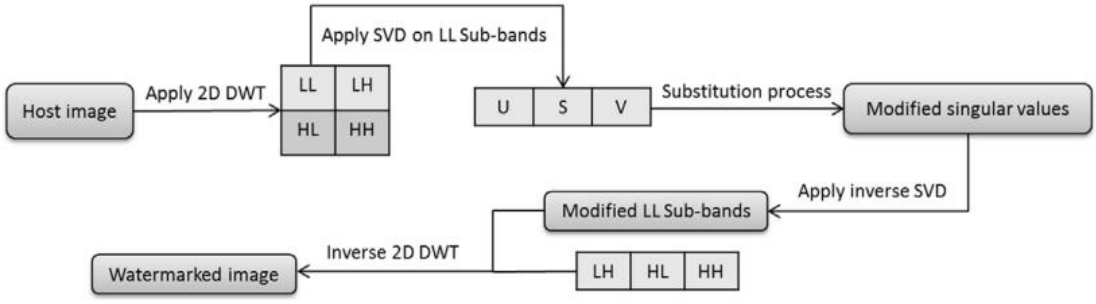

Fig 4.Integration process

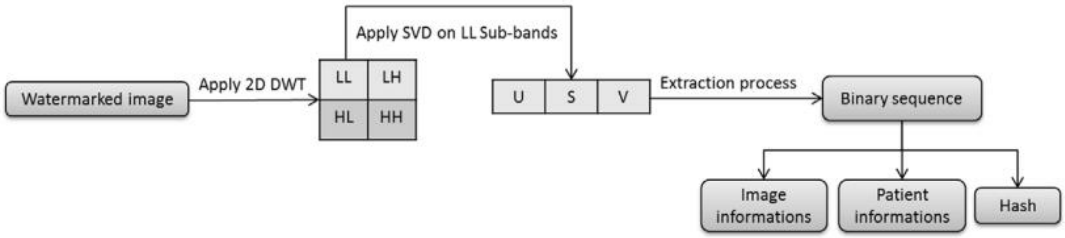

Fig 5.Extraction process

And according to the discuss above, sometimes only NROI region will be used to added blind-watermark, following research use deep learning to segment the ROI and NROI to add watermark into NROI**[1]**.

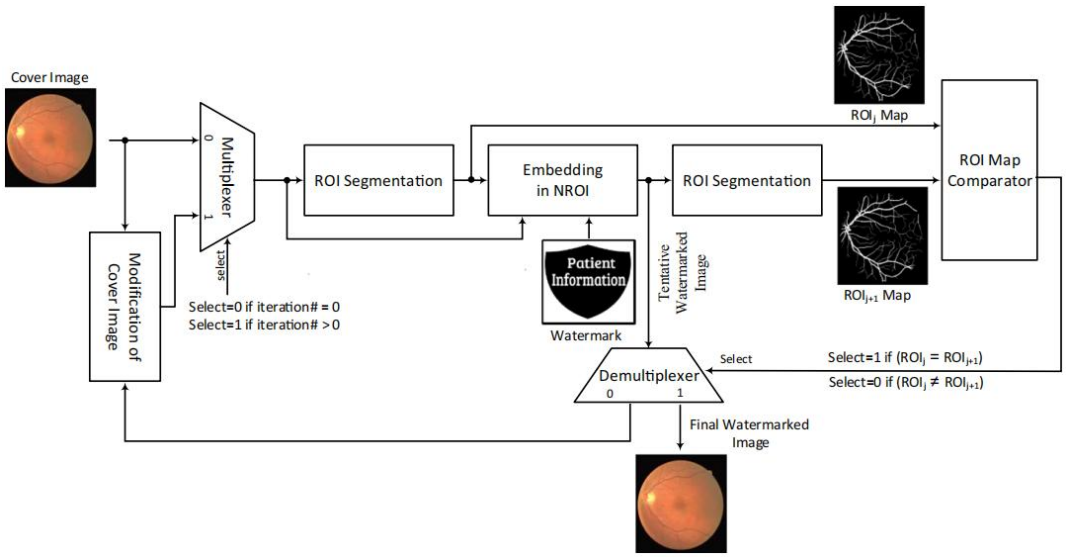

Fig 6.Segmentation for ROI and NROI

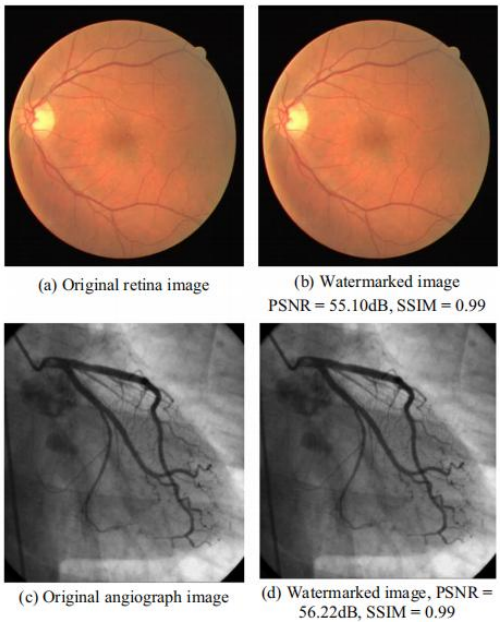

Fig 7.Original image and blind-watermark results

3 Project Plan

The **anticipate result** for this project mainly comes from three aspects:

Fast speed: I will achieve current spatial and transform domain blind-watermark algorithm according to the related research paper and improve current algorithm, reducing the algorithm complexity. The improvement can be expected in the traverse and data structure. Correct improvement for the algorithm will reduce the build-watermarking time significantly.

High robustness: the build-watermark should have the ability of anti-interference so I will do simulation for image damage like bit error from transmission and degradation of noise, filter to verify my build-watermark's robustness. I will use the measurement parameters like MSE, SNR discussed above to test my blind-watermark algorithm.

Batch operation and human computer interaction: I will use **python PyQt5** to design GUI and executable file. This GUI will provide user multiply choice of the build-watermark methods, watermark messages, mapping and signature methods and the image or folder of images to be build-watermarked. It also provide user the simulation to test their watermark's robustness.

The **project schedule** is shown as follow:

Project plan	Time	Main content
Algorithm implementation	1-2 week	Spatial domain build-watermark Transform domain build-watermark ROI segmentation algorithm
Robustness verify	1 week	Simulation for noise, filtering, interpolation Simulation for bit error of transmission
GUI development	1 week	Batch processing Multiple modes

Project basis

Through the study of digital image course, I master and can realize the basic image processing methods. The algorithms related to this project are described in detail in the related research literature, but there may not be many existing codes, which need to be completed by myself.

I have the foundation of data structure and algorithm analysis, and can reasonably optimize the algorithm and improve the efficiency of the algorithm.

I have python PyQt5 GUI interface design experience and can quickly develop the application program of the project.

4 Main Challenges

It can be expected that some difficulties will be met in the implementation of the project and solving these challenges will greatly promote the final realization of the project.

4.1 Medical image ROI segmentation

For most medical images, such as CT and X-ray, it is difficult to distinguish ROI, because the outline in the image is not very clear, and because most of the pictures are monochrome, it is difficult to distinguish in color. **Accurately distinguishing ROI is of great significance to doctors' evaluation of medical images**. In the related literature, some use deep learning or threshold algorithm to distinguish ROI and NROI. I will try the above methods to realize my own ROI segmentation algorithm. It should be noted that the **position** of ROI in most medical images is relatively fixed, such as CT images, so the position in the image is a feature that can be used.

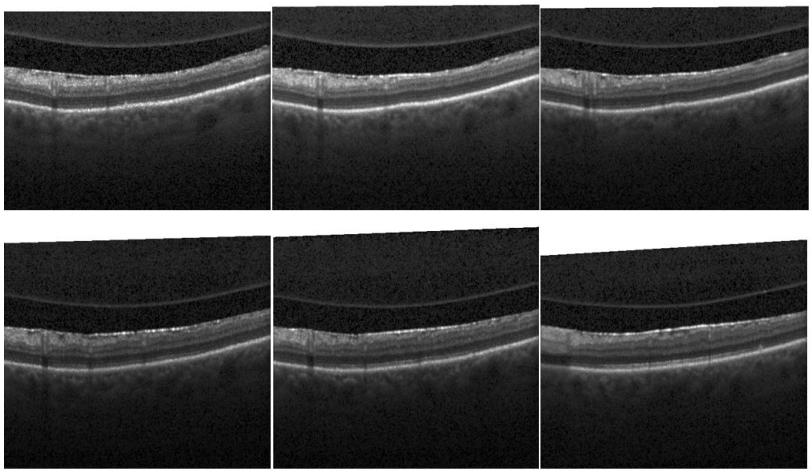

Fig 8. Six eye OCT iamges(positions of ROI are similar)

4.2 Transform domain blind-watermark algorithm

The blind watermarking algorithm in transform domain is different from the general image analysis in transform domain. The algorithm in transform domain often includes many special processing, such as quadrant differentiation and singular value decomposition. To analyze these problems, we need to understand the principle of the algorithm and the image of each transform domain operation.

At the same time, the mathematical principle of transform domain algorithm is also very complex, which needs me to deeply understand. It is expected that this will take some time. Once I can understand the mathematical principle of the algorithm, it will help me to optimize and redesign the algorithm.

4.3 Algorithm performance test

Although relevant parameters have been proposed to evaluate the blind-watermark algorithms, the definitions of these parameters such as SNR are inconsistent in different related literatures. Therefore, we need to find a suitable and general method to evaluate the performance of different algorithms.

Secondly, the robustness of our algorithm to noise, distortion and damage depends largely on the size of our noise and the degree of distortion like rotation, which we need to make

quantitative analysis and explanation.

References

[1] Zarrabi H, Emami A, Khadivi P, et al. BlessMark: a blind diagnostically-lossless watermarking framework for medical applications based on deep neural networks[J]. Multimedia Tools and Applications, 2020, 79(31): 22473-22495.
[2] Zermi N, Khaldi A, Kafi R, et al. A DWT-SVD based robust digital watermarking for medical image security[J]. Forensic Science International, 2021, 320: 110691.
[3] Kahlessenane F, Khaldi A, Kafi R, et al. A DWT based watermarking approach for medical image protection[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(2): 2931-2938.
[4] 李九高. 医学 CT 图像数字水印算法的研究[D].南京邮电大学,2013.
[5] Parah, Shabir A., et al. "Realisation and robustness evaluation of a blind spatial domain watermarking technique." International journal of electronics 104.4 (2017): 659-672.
[6] Parah, S. A., Sheikh, J. A., Assad, U. I., & Bhat, G. M. (2015). Hiding in encrypted images: A three tier security data hiding technique. Multidimensional Systems and Signal Processing.
[7] Yan, H., Li, J., & Wen, H. (2011). A key points-based blind watermarking approach for vector geo-spatial data. Computers, Environment and Urban Systems, 35, 485-492.
[8] Parah, S. A., Sheikh, J. A., Hafiz, A. M., & Bhat, G. M. (2014a). Data hiding in scrambled images: A new double layer security data hiding technique. Computers & Electrical Engineering, 40, 70-82.