Authentication of Biomedical Images Based on Zero Location Watermarking

Anthony T. S. Ho and Xunzhan Zhu

School of Electrical and Electronic Engineering
Nanyang Technological University
Nanyang Avenue, Singapore 639798.
Email: etsho@ntu.edu.sg

Jun Shen

DataMark Technologies Pte. Ltd.
100 Jurong East Street 21, Singapore 609602.
Email: shenjun@datamark.com.sg

Abstract

In this paper, a fragile watermarking method for authentication of biomedical images is proposed in the z-transform domain based on the zero locations. The z-transform is a convenient yet invaluable tool for representing, analyzing and designing discrete-time signals and system. Our watermarking method is designed by exploiting the sensitivity of the positions of z-transform zeros on the unit circle to any tampering made on the host image, such that the watermarking system can localize the portions of a watermarked image that have been tampered maliciously with high accuracy. Simulation results are presented to demonstrate the effectiveness and efficiency of the proposed scheme.

1 Introduction

Biomedical imaging and biomedical image analysis are drawing a great deal of research interests over the past decades [1], [2], [3]. Biomedical images are important source of anatomical and functional information for medical and biologic studies. There is a need for verification or authentication of the integrity of the image content, for example, of a patient's record in a hospital database. In our work, we propose a novel fragile watermarking scheme based on the zero locations of the z-transform. A fragile watermarking detects changes to the watermarked image such that it can provide some form of confidence that the image has not been intentionally tampered with and is originated from the right source [4].

The z-transform domain is a new transform space for fragile watermark embedding. It has the advantage of easy implementation and pixel-wise sensitivity to external tampering such as content modifications. Moreover it has better security consideration than the normal LSB check-sum fragile watermarking techniques [5], [6]. The next section presents a brief review of the z-transform. The watermark embedding and authentication methods are elaborated in Section III and Section IV. Section V gives the simulation results followed by the conclusion in Section VI.

2 Fundamental of z-Transform

The z-transform is a convenient yet invaluable tool for representing, analyzing and designing discrete-time signals and system [7]. The z-transform of a sequence, $x(n)$, which is valid for all n, is defined as

$$X(z) = \sum_{n=-\infty}^{\infty} x(n)z^{-n} \qquad (1)$$

where z is a complex variable. In a causal system, which is the case of an image pixel sequence, $x(n)$ may be nonzero only in the interval $0 \le n < \infty$ and Equation (1) reduces to the so-called one-sided z-transform:

$$X(z) = \sum_{n=0}^{\infty} x(n)z^{-n} \qquad (2)$$

Clearly, the z-transform is a power series with an infinite number of terms and so may not converge for all values of z. The region where the z-transform converges is known as the region of convergence (ROC), and in this region the values of $X(z)$ are finite. The image pixel value sequence is a causal, finite duration sequence, in this case $X(z) = \infty$ only when $z = 0$. Thus the region of convergence is everywhere except at $z = 0$.

In z-transform domain representation of signal, values of z for which $X(z) = \infty$ are referred to as poles of $X(z)$; values of z for which $X(z) = 0$ are referred as the zeros of $X(z)$. For the case of an image pixel sequence, only zeros are considered; all the poles are equal to zero in this system.
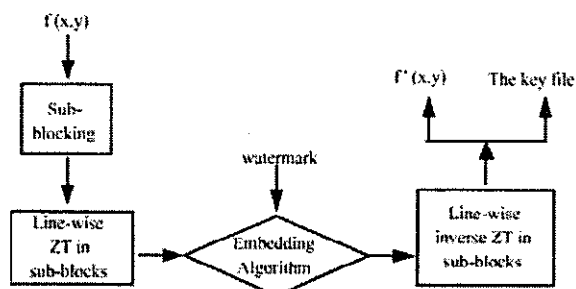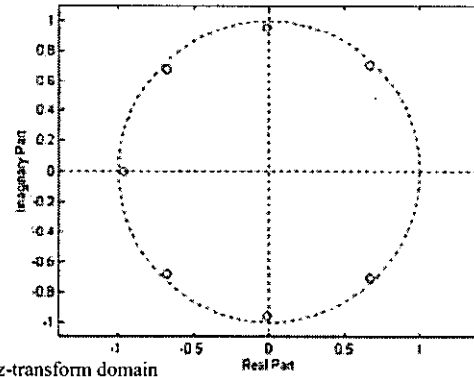

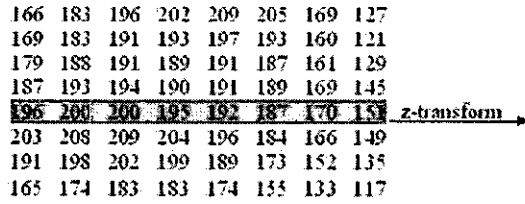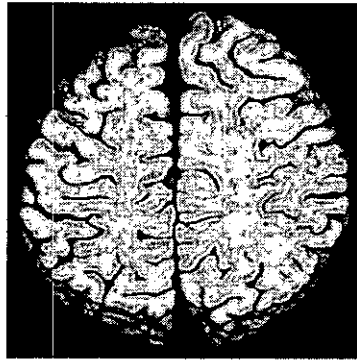Fig. 1. The watermark embedding process.

166	183	196	202	209	205	169	127
169	183	191	193	197	193	160	121
179	188	191	189	191	187	161	129
187	193	194	190	191	189	169	145
196	200	200	195	192	187	170	151	z-transform →
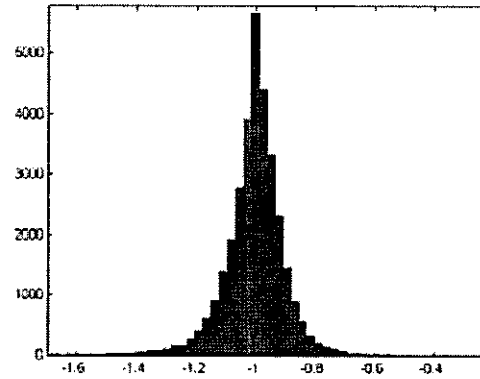| 203	208	209	204	196	184	166	149
191	198	202	199	189	173	152	135
165	174	183	183	174	155	133	117

Fig. 2. Transform a line into z-transform domain

Fig. 3. Statistical property of the negative real root amplitudes: (a) The original image Brain (b) Histogram of negative real
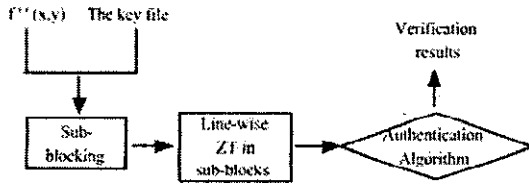
(a)

(b)

Fig. 4. The image authentication process.

The inverse z-transform (IZT) allows us to recover the discrete-time sequence, $x(n)$, given its z-transform. Symbolically, the inverse z-transform may be defined as

$$X'(n) = Z^{-1}[X'(z)] \quad (3)$$

where $X(z)$ is the z-transform of $x(n)$ and Z^{-1} is the function for the inverse z-transform.

Moreover, there also exists a 2-D z-transform, which can be used in image processing applications as a useful generalization of the Fourier series [8]. In this paper, the 1-D z-transform is used for fragile watermark embedding and authentication of image pixel sequences. The detailed process is discussed in the following section.

3 Date Hiding of Watermarks in the z-Transform Domain

The watermark embedding process is described in Figure 1. The original image, $f(x, y)$, is divided into a set of non-overlapped blocks of size $h \times h$ denoted by $f_k(x', y')$, $k = 0, 1, ..., K - 1$, where the subscript k denotes the index of the blocks and K is the total number of the blocks. In our experiment, a sub-block size of 8×8 is used, which is commonly used in image processing. For a test image of size 512×512, there exists 4096 sub-blocks. We then perform 1-D z-transform on a line-by-line basis for each sub-block using Equation (2). For example, consider a sub-block, $f_k(x', y')$, one horizontal line which is denoted by $x(n)$, $1 \le n \le h$ is taken out for processing. Before the z-transform, the first non-zero pixel value of each line needs to be normalized to be one due to the practical computer implementation of the z-transform and inverse z-transform used in the watermarking system.

In the z-transform domain, a signal is represented by its zeros and poles. Real sequences such as image pixel values concern only the zeros. Figure 2 illustrates the situation of transforming a line of pixels into the z-transform domain (for a line of 8 pixels).

In the z-transform domain, the maximum number of zeros for a sequence of n numbers is $n-1$. As we can see there are 7 zeros in Figure 2 when $n = 8$. All the zeros are distributed around the unit circle. To avoid the phase change caused by the complex number computation, we

select the amplitude of negative real roots to encode the checking bits. Figure 3 shows the statistical property of the negative real root amplitudes for a biomedical image using the sub-blocking and transformation mentioned above, before watermarking is performed. We find that the histogram distribution has a mean value of −1, which is the magnitude of the unit circle. This enables us to use −1 as the threshold to decide between the binary check-bits (watermark). The check-bits are randomly generated and would be stored into the output key file. In our experiment, 8 check-bits are embedded into every block.

The data hiding process is defined as follows:

if check-bit = 1 *then*
    if real − root < *a then*
        real − root = *a*
    end if
else if check-bit = 0 *then*
    if real − root > *b then*
        real − root = b
    end if
end if

where $a = -1 + \varepsilon$, $b = -1 - \varepsilon$, and ε is a small positive offset which determines the trade-off between the fragility of the watermarking scheme and the quality of the watermarked image. The above algorithm illustrates the method of embedding the check bits into the z-transform domain. Depending on the check bits sequence and the root location, occasionally, we need to force some roots to cross the -1 boundary for the encoding of bit 1 or 0. This may introduce some minor distortion to the original image. However, as we will find from the experimental results, such distortion is not perceptually visible and is negligible.

After the watermark embedding process, we then transform the zeros back to the sequence using the inverse z-transform:

$$x'(n) = Z^{-1}[X'(z)] \qquad (4)$$

After this process, we obtain another sequence. It is slightly different from the one before watermarking. After rearranging and scaling the sequence to the pixel values, we obtain the watermarked sub-block, $f_k'(x', y')$. Applying the above process to all the relevant sub-blocks, we obtain the watermarked image $f'(x, y)$.

4 Image Authentication

As shown in Figure 4, in the authentication process, we need both the watermarked image and the key file to identify the watermark. Let the watermarked image after passing through the communication channel be $f''(x, y)$. The check-bit sequence is first read from the key file. By applying z-transform to each line sequence of the sub-blocks we obtain the corresponding zeros. We find the negative real roots from the zeros and compare them to the check-bits on the following conditions:

if real − root > −1 && check − bit == 1 *then*
    authentication result = 1
else if real − root < −1 && check − bit == 0 *then*
    authentication result = 1
else
    authentication result = 0
end if

where "0" represents the altered regions while "1" represents unchanged sub-blocks. After checking all the image sub-blocks, we obtain the overall authentication result.

5 Experimental Results

We use two 512 × 512 gray-scale biomedical images skin and brain as shown in Figure 5(a) and (c) to test our authentication algorithm. Figure 5(b) and (d) display the watermarked images. We can see that the watermarked images look identical to the original images, with PSNR values of approximately 40 dB and 38 dB, respectively. We modified the content of the watermarked images as shown in Figure 6: (a) some parts of the image were replaced and (c) some features of the medical image were removed. As illustrated in Figure 6(b) and (d), the modified areas were accurately detected and identified.

Moreover, the proposed algorithm was very efficient in terms of processing time. For a grey-scale image of size 512×512, it took approximately 3 seconds for the embedding process and only 1.8 seconds for the authentication process in MATLAB 6.5. The experiments were performed on a PC equipped with P III 550MHz CPU and 196 Mbytes RAM.

6 Conclusion

In this paper, we discuss a novel fragile watermarking in the z-transform domain for the authentication of biomedical images. The watermark bits are embedded by slight displacement of the zeros. The z-transform zeros on the unit circle are very sensitive to any change of the host image. This important property provides the scheme with special sensitivity to any alteration to the watermarked image and the ability of accurate localizing. The efficiency of the new method has also been demonstrated by experimental results.

References

[1] A. Abubakar, P. M. van den Berg, and J. J. Mallorqui, "Imaging of biomedical data using a multiplicative regularized contrast source inversion method," IEEE Trans. Microwave Theory Tech., vol. 50, pp. 1761 – 1771, July 2002.

[2] B. C. Wilson, E. M. Sevick, M. S. Patterson, and B. Chance, "Time-dependent optical spectroscopy and imaging for biomedical applications," Proceedings of the IEEE, vol. 80, pp. 918 –930, June 1992.

[3] G. Vernazza, S. Serpico, and S. Dellepiane, "A knowledge-based system for biomedical image

processing and recognition," IEEE Trans. Circuits Syst., vol. 34, pp. 1399–1416, Nov. 1987.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. CA: Academic Press, 2002.

[5] M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in proc. Int. Conf. Image Processing (ICIP 97), Santa Barbara, CA, Oct. 1997.

[6] P. W. Wong, "A watermark for image integrity and ownership verification," in Proceedings of IS & T PIC conference, OR, Portland, May 1998.

[7] R. Vich, z-Transform Theory and Applications. Dordrecht: D. Reidel Publishing Company, 1987.

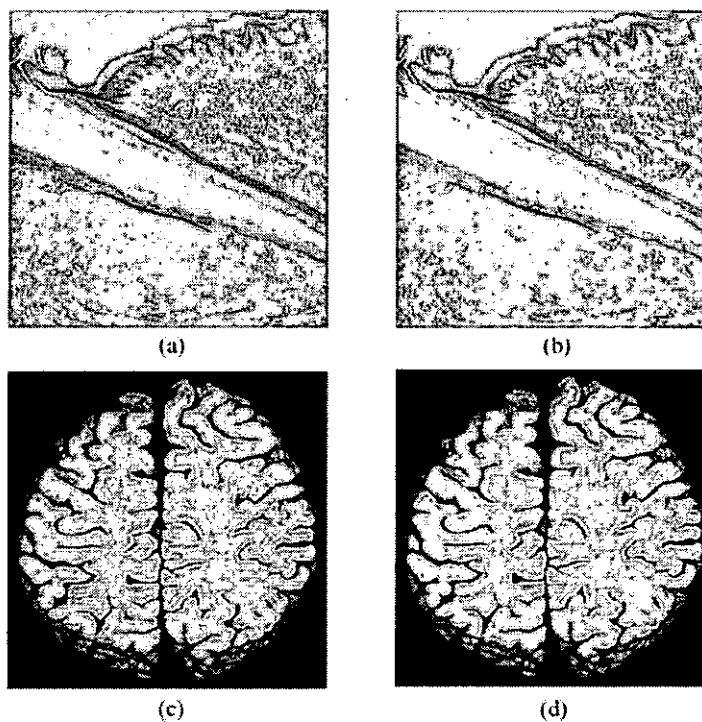[8] A. K. Jain, Fundamentals of Digital Image Processing. Englewood Cliffs, NJ: Prentice-Hall, 1989.

(a)

(b)

(c)

(d)

Fig. 5. Experimental results: (a) the original Skin; (b) the watermarked Skin; (c) the original Brain; (d) the watermarked brain.
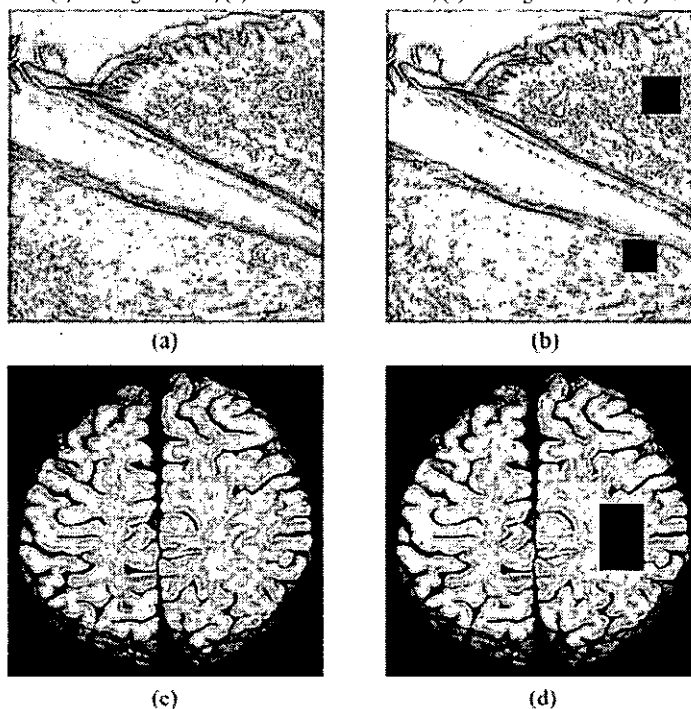

(a)

(b)

(c)

(d)

Fig. 6. Experimental results: the attacked images (a) (c) and the authentication results (b) (d).