Correspondence

Fragile Watermarking Based on Encoding of the Zeroes of the z-Transform

Anthony T. S. Ho, Xunzhan Zhu, Jun Shen, and Pina Marziliano

***Abstract*—In this paper, a new fragile watermarking method for digital image authentication is proposed based on the zero locations of the z-transform. The z-transform domain is a new transform space for fragile watermark embedding. Our watermarking method is designed by exploiting the sensitivity of the positions of the zeroes of the z-transform around the unit circle to any change made on the host image. The watermarking system can localize the portions of a watermarked image that have been tampered with with high accuracy. In addition, the newly proposed scheme is more secure than normal least-significant bits-based fragile watermarking techniques. Experimental results as well as the theoretical analysis demonstrated the fragility and accuracy of the new method.**

***Index Terms*—Authentication, fragile watermarking, z-transform.**

I. Introduction

Digital image authentication is increasingly becoming more important with the tremendous development of the Internet. The ability of fragile watermarking to detect changes in the watermarked image to provide authenticity and integrity of the image makes it go a long way toward solving the image authentication problem.

In contrast to a semifragile watermark [1], [2], which only seeks to detect a predefined set of illegitimate distortions to the host image, a fragile watermark is designed to detect any change to the host image. Hence, a variety of fragile watermarking methods has been proposed by embedding identifying information in the least-significant bits (LSBs) of the image [3]–[6]. Unfortunately, these methods are somewhat unsecured as the use of LSBs could be easily detected and manipulated. In [7], a fragile watermarking scheme using a statistical model was proposed. However, the scheme was only able to localize distorted pixels altered in the five most significant bits. In our work, we propose a novel fragile watermarking scheme in the z-transform domain. The z-transform is a convenient yet invaluable tool for representing, analyzing, and designing discrete-time signals and systems [8]–[10]. However, to our knowledge, this is the first time that this transform has been applied to digital watermarking. The locations of zeroes of the z-transform are very susceptible to any pixel value change. It has the advantage of easy implementation and pixel-wise sensitivity to external tampering. Moreover, it provides better data-hiding security protection than the normal LSBs check-sum fragile watermarking techniques.

Manuscript received August 2, 2006; revised January 30, 2008. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Ton Kalker.

A. T. S. Ho is with the Department of Computing, University of Surrey, Guildford, Surrey GU2 7XH, U.K. (e-mail: a.ho@surrey.ac.uk).

X. Zhu and J. Shen were with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. They are now with the R&D Center, Tongfang Asia Pacific Pte Ltd., Singapore (e-mail: judyzhu@thtf.com.cn; shenjun@datamark-tech.com).

P. Marziliano is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: epina@ntu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2008.926994

II. Zeroes of z-Transform

Theorem: Assume that $f[n]$, $n = 0, 1, \ldots, N-1$ is a non-negative real sequence which is not uniformly zero. Then, the z-transform of $f[n]$ must have negative real root(s) if $f[0] \neq 0$, $f[N-1] \neq 0$, and N are even.

Proof: By the definition of z-transform [10]

$$F(z) = \sum_{n=0}^{N-1} f[n] z^{-n} = \frac{A}{z^{N-1}} \prod_{i=1}^{N-1} (z - z_i). \tag{1}$$

From (1), it can be concluded that $\{z_i\}$ must either be real or occur in conjugate pairs to ensure that the coefficients $f[n]$ are real. Meanwhile, since $f[0] \neq 0$ and $f[N-1] \neq 0$, the z-transform series has an even number of items. Therefore, the total number of roots should be odd. It follows that there is at least one real root. Consider z_{pr}, which is a root of $F(z)$ such that it is real and positive. Then, we have

$$F(z)\Big|_{z=z_{pr}} = \sum_{n=0}^{N-1} f[n](z_{pr})^n = 0.$$

Since $f[n]$ is nonnegative, we have

$$f[n] = 0 \forall\, n$$

which contradicts the hypotheses that the sequence is not uniformly zero.

In conclusion, $F(z)$ must have real root(s), and this (these) real root(s) can only be negative. Moreover, most of the negative real zeroes are distributed in the neighborhood of the unit circle.

III. Proposed Method

The diagram of the algorithm is illustrated in Fig. 1. The original image $\mathbf{X}$ is divided into nonoverlapping blocks of size $N \times N$, where N is an even positive integer. By viewing it row by row, each block can be expressed as a sequence of vectors $\{\mathbf{x}_m\}$, $m = 0, 1, \ldots, N-1$, where $\mathbf{x}_m = \{x_m[n]\}$, $n = 0, 1, \ldots, N-1$. We then perform the z-transform and obtain the zeroes, which are denoted as $\{z_{m,i}\}$, $i = 1, \ldots, N-1$, and $m = 0, \ldots, N-1$.

We embed the watermark $\mathbf{w}$ by slightly perturbing the locations of the zeroes, where $\mathbf{w}$ is a binary sequence of N. The watermark bits are randomly generated and the initial seed number is contained in a secret key file. A watermark signal of N bits long is embedded into every block, that is, one bit is embedded into every vector. To avoid the complex number computation, we embed the authentication watermark by slightly modifying the modulus of negative real zeroes, which are denoted by z_{nr}. As proven in Section II, since N is even, which is the case under most circumstances for natural images, there must be at least one real negative zero in the zero set of a pixel vector. Besides the negative real zero, there are $(N/2)-1$ pairs of complex zeroes for every vector (the number of complex zeroes would be less if multiple negative real zeroes exist). Consider the vector $\mathbf{x}_m$ and denote V_m as the number

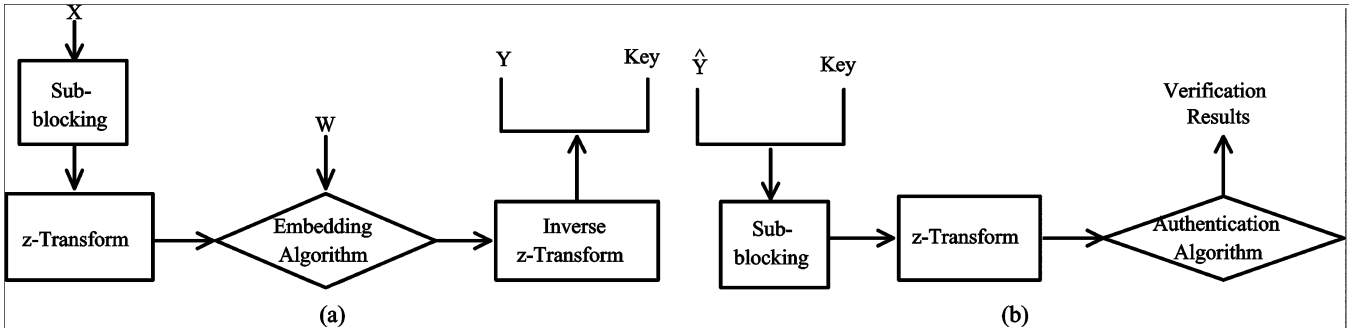

Fig. 1. Fragile watermarking. (a) Watermark embedding. (b) Image authentication.

of associated complex zeroes with phase angle $\theta \in (0, (\pi/2)]$, and letting K be a user defined key, we have

$$\mathbf{h} = \mathcal{H}(K, V_0, V_1, \ldots, V_{N-1}) \tag{2}$$

where $\mathcal{H}$ is a hash function and $\mathbf{h}$ is the N bits output. We then compute

$$\mathbf{p} = \mathbf{w} \oplus \mathbf{h} \tag{3}$$

where $\oplus$ is the exclusive OR function. The watermarking is performed by embedding $\mathbf{p}$ into the negative real zeroes. The data-hiding process is defined as follows:

$$z'_{nr} = \begin{cases} -1 + 1.5\epsilon + U(z_{nr} + 1)(0.5\epsilon), & \text{if } p = 1 \\ -1 - 1.5\epsilon - U(-z_{nr} - 1)(0.5\epsilon), & \text{if } p = 0 \end{cases} \tag{4}$$

where

$$U(t) = \begin{cases} 1, & \text{if } t \geq 0 \\ 0, & \text{if } t < 0 \end{cases}$$

$z_{nr}, z'_{nr} \in \mathbb{R}^-$ are the original and the watermarked zeros, respectively, and $0 < \epsilon < 0.1$. The small positive offset ϵ determines the tradeoff between the fragility of the watermarking scheme and the quality of the watermarked image.

After the watermark embedding process, we transform the zeroes back to the sequence using the inverse z-transform. We then obtain another vector $\mathbf{x}'_m$, which is slightly different from the one before watermarking. By applying the aforementioned process to all of the relevant blocks, we obtain the watermarked image $\mathbf{Y}$.

In the authentication process, we need the watermarked image and the secret key to identify the watermark. Let the watermarked image after passing through variant communication channels be $\hat{\mathbf{Y}}$. The watermark sequence $\mathbf{w}$ is generated using the initial state number contained in the key. The authentication process also starts by dividing the image into small blocks of size $N \times N$. In every block, by applying the z-transform to every row, we obtain the zeroes. We find the values of $\{V_m\}$ and compute $\mathbf{h} = \mathcal{H}(K, V_0, V_1, \ldots, V_{N-1})$. We then obtain $\mathbf{p}$ by (3). The negative real zeroes $\{\hat{z}_{nr}\}$ are compared to the bits of $\mathbf{p}$ based on the following conditions:

$$R_m = \begin{cases} 1, & \text{if } (\hat{z}_{nr} > -1 + \epsilon \& p = 1) \vee (\hat{z}_{nr} < -1 - \epsilon \& p = 0) \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

where $\vee$ is an OR function and R_m is a Boolean variable which indicates the authenticity of the pixel vector $\mathbf{x}_m$, $m = 0, \ldots, N-1$.

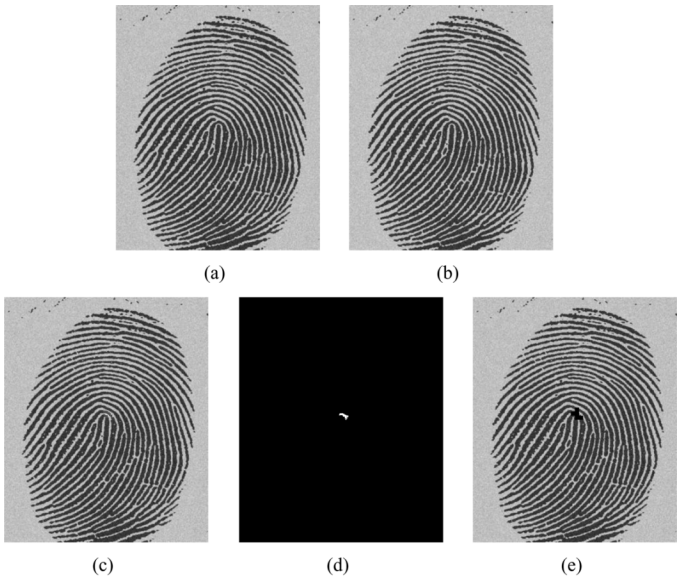

Fig. 2. Experimental results. (a) Original images. (b) Watermarked image. (c) Tampered image. (d) Difference image between the tampered image and the watermarked image. (e) The authentication result.

$R_m = 0$ represents the altered regions while $R_m = 1$ represents intact areas. The authenticity of a block can be indicated by

$$R = R_0 \vee R_1 \vee \cdots \vee R_{N-1}. \tag{6}$$

After checking all of the image blocks, the tampered parts are located to determine the authenticity of the input image.

IV. Results and Analysis

In this section, we demonstrate the effectiveness of our proposed method with experimental results, followed by the performance analysis of the method.

A. Experimental Results

In our experiment, we set $\epsilon = 0.02$. We used gray-scale image Fingerprint as shown in Fig. 2(a) to test our authentication algorithm. A block size of 8×8 was used, which is commonly used in image-processing applications. The watermarked image is displayed in Fig. 2(b). We shall see that the watermarked image looks identical to the original image, with a peak-to-signal noise ratio (PSNR) value of approximately 45 dB. As shown in Fig. 2(c) and (d), a small part of the fingerprint image was modified. The authentication result by our algorithm

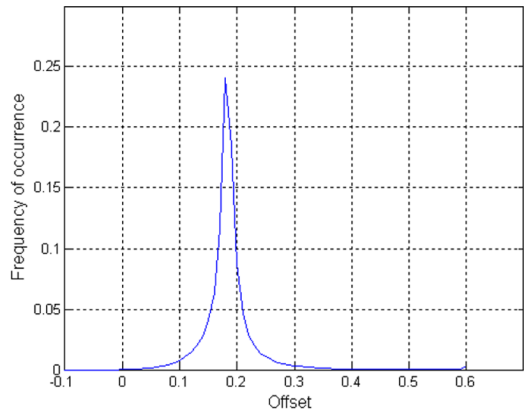

Fig. 3. Offset of the modulus of negative real zeroes caused by one gray-scale value change.

is shown in Fig. 2(e) and we can observe that the tampered area was accurately detected.

B. Fragility of Watermark to Pixel Perturbation

From our observation, the zero locations of the z-transform are very sensitive to the value change of even a single pixel, which renders the z-transform domain ideal for fragile watermarking. We have investigated this property experimentally. We collected 1000 gray-scale natural images and calculated the negative real zeroes of the z-transform of their pixel sequences as described in Section III. We then randomly changed one pixel value in every sequence and calculated the amplitudes of the offsets of the negative real zeroes, which are reported in Fig. 3. It can be observed that even a single pixel's change unavoidably disturbs the zero locations. In addition, we found that 98% of the negative real zeroes tend to shift toward the unit circle and as illustrated in Fig. 3, the distribution peaks at an offset of 0.18, which is enough to change the watermark detection results.

V. Conclusion

In this paper, we discuss a novel fragile watermarking method based on the z-transform domain. The watermark bits are embedded by slight perturbation of the zero locations. The zeroes of the z-transform around 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. In addition, the proposed method is more secure than normal fragile watermarking techniques based on LSB embedding. Simulation results confirmed the applicability of the proposed algorithm.

References

[1] C.-S. Lu and M. H.-Y. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[2] A. T. S. Ho, X. Zhu, and Y. L. Guan, "Image content authentication using pinned sine transform," *EURASIP J. Appl. Signal Process., Special Issue Multimedia Security Rights Manag.*, vol. 2004, no. 14, pp. 2174–2184, Oct. 2004.

[3] M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in *Proc. Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997, vol. 2, pp. 680–683.

[4] P. W. Wong, "A watermark for image integrity and ownership verification," presented at the IS & T PIC Conf., Portland, OR, May 1998.

[5] P. W. Wong, "A public key watermark for image verification and authentication," in *Proc. IEEE Int. Conf. Image Processing*, 1998, vol. 1, pp. 455–459.

[6] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," *IEEE Trans. Image Process.*, vol. 11, no. 6, pp. 585–595, Jun. 2002.

[7] X. Zhang and S. Wang, "Statistical fragile watermarking capable of locating individual tampered pixels," *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 727–730, Oct. 2007.

[8] E. C. Ifeachor and B. W. Jervis, *Digital Signal Processing: A Practical Approach*. Wokingham, U.K.: Addison-Wesley, 1993.

[9] R. H. T. Bates, B. K. Quek, and C. R. Parker, "Some implications of zero sheets for blind deconvolution and phase retrieval," *J. Opt. Soc. Amer. A, Opt. Image Sci.*., vol. 7, no. 3, pp. 468–479, Mar. 1990.

[10] R. Vich, *z-Transform Theory and Applications*. Dordrecht, The Netherlands: Reidel, 1987.

# On the Assumption of Equal Contributions in Fingerprinting

Hans Georg Schaathun

***Abstract*—With a digital fingerprinting scheme, a vendor of digital copies of copyrighted material marks each individual copy with a unique fingerprint. If an illegal copy appears, it can be traced back to one or more guilty pirates due to this fingerprint. A coalition of pirates may combine their copies to produce an unauthorized copy with a false, hybrid fingerprint. It is often assumed in the literature that the members of the collusion will make equal contributions to the hybrid fingerprint, because nobody will accept an increased risk of being caught. We argue that no such assumption is valid *a priori*, and we show that a published solution by Sebé and Domingo–Ferrer can be broken by breaking the assumption.**

***Index Terms*—Collusion-attack, collusion-secure code (CSC), digital fingerprinting, scattering codes.**

I. Background

The problem of digital fingerprinting was introduced in [1] and has received quite some attention following [2]. A vendor of digital copies of copyrighted material wants to prevent unauthorized copying. Digital fingerprinting makes it possible to trace the guilty user (pirate) when an illegal copy is found. This is done by embedding a secret identification mark (fingerprint) in each copy, making every copy unique.

Typically, a robust watermarking (WM) scheme is used to hide the fingerprint in the file. WM schemes are designed to hide any message in a file in such a way that they can be recovered, even after being subject to noise, signal-processing operations, or even malicious attacks.

If a single pirate distributes unauthorized copies, they will carry his or her fingerprint. If the vendor discovers the illegal copies, he or she can trace them back to the pirate and prosecute him or her. However, a collusion of users can compare their copies, and thereby find regions

Manuscript received July 28, 2007; revised May 8, 2008. This work was supported in part by the Norwegian Research Council under Grant 146874/420, conducted under employment with the University of Bergen, Norway. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Upamanyu Madhow.

The author is with the Department of Computing, University of Surrey, Guildford GU2 7XH, U.K. (e-mail: h.schaathun@surrey.ac.uk).

Digital Object Identifier 10.1109/TIFS.2008.926991