Data Duplication Prevention and Detection

B. Vijay Vamshi

Asst Professor, Department of Electronics and Communication Engineering
Christu Jyothi Institute of Technology and Science, Jangoan, Warangal -AP-India.

Abstract: In this project, an image watermarking technique based upon a z transform is proposed and analyzes that, how it is resistant to attacks. The redundant transform provides an over complete representation of the image which facilitates the identification of significant image features via a simple correlation operation across scales. Although the watermarking algorithm is image adaptive, it is not necessary for the original image to be available for successful detection of the watermark. The performance and robustness of the proposed technique is tested by applying common image-processing operations such as filtering, re-quantization, and JPEG compression. A quantitative measure is proposed to objectify performance; under this measure.

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 semi fragile watermark, 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. Unfortunately, these methods are somewhat unsecured as the use of LSBs could be easily detected and manipulated. In 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. 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.

In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values. There are many spatial and frequency domain techniques available for authentication watermarking.

Literatures on Previous Analysis

Previous methods have failed in providing robust behavior under many commonly considered attacks mainly, because they attempted to face the image, audio or video signal in a global sense, without

exploiting their local characteristics. In the case of image watermarking, employing spatial characteristics is essential for ensuring immunity to geometric transformations. When a watermark is embedded on the entire image, scaling, rotation or cropping will result in the destruction of the watermark because no reference points exist that would lead in finding the amount of scaling, rotation or cropping. The use of an image transform, with the exception of the Fourier transform, will suffer the same problems. The Fourier transform is theoretically rotation, translation and scale invariant, but the robustness to filtering or compression depends on the range of frequencies that are used for watermarking.

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. 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.

Fragile Watermarking

It checks and detects even a small change in the host image. In other words it is a mark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation. Fragile marks are not suited for enforcing copyright ownership of digital images; an attacker would attempt to destroy the embedded mark and fragile marks are, by definition, easily destroyed. The sensitivity of fragile marks to modification leads to their use in image authentication. That is, it may be of interest for parties to verify that an image has not been edited, damaged, or altered since it was marked. Fragile or semi-fragile watermarking schemes based on conventional DWT have been reported during the last few years. Tamper detection at multi-resolution had been achieved. But it violates the nature of the human visual system. It brings perceptible distortion to the watermarked images. Inoue et al. embedded fragile watermark by threshold and quantize wavelet coefficients at the coarser scales and gave a measurement for tamper proofing. Yu et al. modeled the DWT coefficient's changes caused by tamper as Gaussian distribution. Malicious tamper has large variance while incidental tamper has small variance. They embedded mark based on modulating the mean of some coefficients instead of individual coefficients.

Most conventional DWT based fragile or semi-fragile watermarking schemes reported in the literature have three shortcomings: (1) Insecurity. The schemes used only one wavelet base to perform the DWT. Once the algorithm was stolen by an attacker, the hidden information bits may be exposed or changed easily. (2) Low robustness to JPEG. (3) High computational complexity. Compared to DCT (discrete cosine transform), conventional DWT has less computational cost. But in the case of images having large size, it is still a problem when DWT applied to a whole image.

Background on Z-Transform

In signal processing, the Z-transform converts a discrete time domain signal (a sequence of real numbers), into a complex frequency domain representation. The Z-transform is to discrete time domain signals what the Laplace transform is to continuous time domain signals.

Definition: If we discrete a time series with a constant sampling interval T, we can write the time series in the following manner: $[x_k] = x_0, x_1, x_2, \ldots, x_k, \ldots$

Where each x_k represents the value (number) of the variable x (t) at time t = k T. We can represent this data in the following form: $x_0 + x_1 z^{-1} + x_2 z^{-2} + \ldots + x_k z^{-k} \ldots$

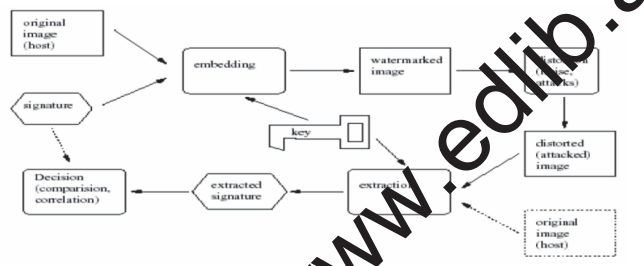
This form is a (symbolic) power series in the variable z–1. We can also write it in the following more compact form:

$$Z[x_k] = \sum_{k=0}^{\infty} x_k z^{-k}.$$

In mathematics and signal processing, the **Z-transform** converts a discrete time-domain signal, which is a sequence of real or complex numbers, into a complex frequency-domain representation. It can be considered as a discrete equivalent of the Laplace transform. This similarity is explored in the theory of time scale calculus. The z-transform was introduced, under this name, by Ragazzini and Zadeh in 1952. The modified or advanced Z-transform was later developed by E. I. Jury, and presented in his book *Sampled-Data Control Systems* (John Wiley & Sons 1958). The idea contained within the Z-transform was previously known as the "generating function method".

Existing Method of Watermarking

Watermarking is previously done by using the wavelet transform, DCT, etc.



The image from the data base is taken using a user friendly menu selection. The image is then read using imread function available in Matlab image processing tool box. Then the content to be water marked is also read and stored in a variable. The block ztrans sub routine is called to perform z transforms operation. After the water marked image is returned from the block ztrans function, both the original and water marked image is shown in the screen using imshow function. In addition to the above we show the watermark which we added to the image. The PSNR is calculated using the formula as shown given below.

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

PSNR = 20 * log10 (255 / sqrt (MSE))

Problem Identified

Most current image-watermarking research focuses on invisible watermarks, those which are imperceptible under normal viewing conditions. The different techniques that are used for invisible image watermarks can be categorized into two classes: spatial-domain watermarks and transform-domain watermarks. The embedding of the image-watermark data into the least-significant bits of image pixels is a typical approach employed by spatial-domain watermarking methods. For transform domain techniques, an image transform, such as the discrete cosine transform (DCT) or discrete wavelet transform (DWT), is employed, the watermark is added to the transform coefficients, and the corresponding inverse transform is taken.

As opposed to spatial-domain techniques which have relatively low bit capacity, transform-domain techniques can embed a large amount of watermark data without incurring noticeable visual artifacts, and they tend to be more robust than spatial-domain methods to attacks on the watermark. The problem with both spatial and frequency domain watermarking techniques is that they modify some pixels of the host

image directly or indirectly, which decreases the image quality. In addition, both of the techniques perform poorly when noise is added to the image. Apart from this most of the watermark techniques are not resistant to attacks.

Embedding strength in conventional method of water marking is low. Quantity of watermark data is low in conventional methods.

Proposed System

In this project we design and development for the fragile watermarking for digital image authentication by using the zeros of the z-transform. 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, 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. Unfortunately, these methods are somewhat unsecured as the use of LSBs could be easily detected and manipulated. 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. 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.

Watermark Embedding and Detecting

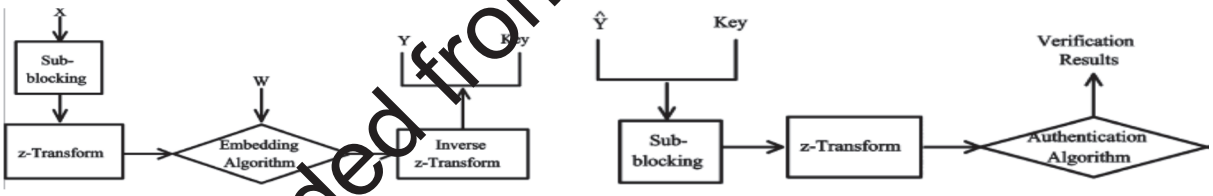


Image Authentication Algorithm for Watermarking Process

Watermarking process

1. The original image X is divided into non overlapping blocks of size NxN, where N is an even positive integer.
2. By viewing it row by row, each block can be expressed as a sequence of vectors.
3. We then perform the z-transform and obtain the zeroes.
4. We embed the watermark w by slightly perturbing the locations of the zeroes, where 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.
5. After the watermark embedding process, we transform the zeroes back to the sequence using the inverse z-transform. We then obtain another vector X'
6. The output of this work is nothing but the Water marked image Y and the key generated k.

Algorithm for Authentication Process

Authentication process

1. In the authentication process, we need the watermarked image and the secret key to identify the watermark.
2. Let the watermarked image after passing through variant communication channels be Y'. The watermark sequence w is generated using the initial state number contained in the key.
3. The authentication process also starts by dividing the image into small blocks of size N x N. In every block, by applying the z-transform to every row, we obtain the zeroes.
4. We find the values of p from the hash functions and the watermarked image block after z transform

Strengths and Limitations

In this project we did the watermarking and authentication process by taking z-transform to the given image. Generally watermarking is done by using Fourier transform and the wavelet transform. The advantages of using the z-transform in watermarking are no need to have the host image. We do the fragility check without the host image. Everything was done with the key and the watermarked image.

Results & Analysis

In this project we introduce the new idea for watermarking generally watermarking is done by using the wavelet transform but in this project we prefer z-transform for fragile watermarking for digital image authentication. The original image X is divided into non overlapping blocks of size N _ N, where N is an even positive integer. By viewing it row by row, each block can be expressed as a sequence of vectors $\{x_m\}$, m = 0; 1; . . . ; N-1, where $x_m = \{x_m[n]\}$, n = 0; 1; . . . ; N-1. We then perform the z-transform and obtain the zeroes, which are denoted as $\{z_{m;i}\}$ i = 1; . . . ; N-1, and m = 0; . . . ; N-1.

We embed the watermark w by slightly perturbing the locations of the zeroes, where 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). The small positive offset € 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 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 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 Ý. The watermark sequence 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*N.

Simulation Results

In this project we introduce the new idea for watermarking generally watermarking is done by using the wavelet transform but in this project we prefer z-transform for fragile watermarking for digital image

authentication. The original image X is divided into non overlapping blocks of size N _ N, where N is an even positive integer. By viewing it row by row, each block can be expressed as a sequence of vectors $\{x_m\}$, m = 0; 1; . . . N-1, where $x_m = \{x_m[n]\}$, n = 0; 1; . . . ; N-1. We then perform the z-transform and obtain the zeroes, which are denoted as $\{z_{m;i}\}$ i = 1; . . . ; N-1, and m = 0; . . . ; N-1.

We embed the watermark w by slightly perturbing the locations of the zeroes, where 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, 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). The small positive offset € 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 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 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 various communication channels be Ý. The watermark sequence 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*N.

Fig: authenticated image

Fig: Tampered image

Fig: authenticated image

Fig: Tampered image

Conclusion

No need to have the host image. We do the fragility check without the host image. Everything is done with the key and the watermarked image. The project can be extended further with some other techniques like wavelet and DCT combined with z-transform for digital image authentication process. The computation time can be reduced by using high end processors. The same work can be extended for visible watermarking also.

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.