A NOVEL FRACTAL WATERMARKING TECHNIQUE

Ming Hong Pi and Chun-Hung Li

Department of Computer Science
Hong Kong Baptist University, Kowloon Tong, Hong Kong
Email: minghong@cs.ualberta.ca, chli@comp.hkbu.edu.hk

ABSTRACT

The paper describes a novel watermarking method to hide binary watermark into the image files compressed by fractal block coding. This watermarking method utilize a special type of orthogonalization fractal coding method where the fractal affine transform is determined by range block mean and contrast scaling. Such orthonalization fractal decoding has the unique mean-invariant property for each range block where the mean of a range block of the decoding series is invariant. The proposed watermark embedding procedure inserts an m-sequence into the quantized code of the range block means. The watermark detection is statistically determined by computing the correlation coefficient. Experimental results show that the watermark is robust against image processing operations such as JPEG compression, low-pass filtering, rescaling and clipping.

1. INTRODUCTION

With the extensive distribution of multimedia data, there is an urgent need for ownership identification and copyright protection. A variety of watermarking methods have been proposed to meet an increasing demand. Digital watermarking is a process of hiding a watermark in multimedia object without perceptually degradation such that the watermark can be detected or extracted later for copyright ownership identification. Early watermarking techniques are directly implemented in the pixel domain. For instance, Schyndel et al. [1, 2] proposed to insert a watermark (an m-sequence) into the least significant bits (LSB) of an image by bit-plane manipulation of LSBs or adding the watermark and the image. The watermark is detected by the correlation coefficient between the original m-sequence and the watermarked image. However, any watermark embedded in the LSBs is susceptible to destroy.

Most watermarking techniques embed a watermark in the transform domain, such as Discrete Cosine Transform (DCT) and discrete wavelet transform. Cox et al [3] asserted that a watermark should be placed in perceptually significant component to deter intentional and unintentional attacks, and hided a watermark into the 1000 highest magnitude AC coefficients. Zhu et al. [4] inserted the watermark into all high-pass wavelet coefficients, and multi-resolution detection can be allowed because of wavelet pyramid structure. A spectrum of watermarking techniques has been investigated in the survey on watermarking [5].

Since Jacquin presented a block-based fractal compression scheme by partition iterated function system, also known as fractal block coding [10], fractal theory has widely been applied into image compression [10-14], image segmentation [15], image retrieval [16], and image watermarking [6-9]. Based on the fractal codes, a few watermarking techniques have been proposed recently [6-9].

All existing watermarking techniques are developed from classification of the fractal codes, and a watermark is often hidden indirectly as a function of the fractal codes [6-9]. Davern and Scott [6] split domain block pool into two halves and the watermark is hidden in those range blocks according to which half the best-pair domain block belongs to. Similarly, Puate and Jordan [7] proposed hiding an 32-bits binary signature into the fractal codes with a redundancy *U* based on that the original and decoding images possess the same fractal codes. Each range block is encoded by search of the Local Search Region (LSR) (a square region around the range block). LSR is divided into two sub-regions: A and B, and all range blocks are classified into two categories according to whether the best-pair domain belongs to A or B. Each bit is hidden with U randomly selected range blocks so that the embedded bit can survive even though the fractal codes of some range blocks are altered by attacks. The analogous fractal watermarking technique was proposed by Li and Wang [8], but each bit is hidden by the isometric transforms, instead of the geometric position of the best-pair domain block [7]. In addition, Bas et al. [9] proposed a binary watermarking technique based on classification of the fractal codes (or the maps). A portion of the original maps are replaced by the redefined maps, and as a result, a binary watermark is hidden.

The aforementioned watermarks have limited information capacity, typically 32 bits. With such a small size, it is easy to cause ambiguity and is also more vulnerable to attack. In addition, since contrast scaling and luminance offset depend on the domain block pool, the contrast scaling and luminance offset obtained from the watermarked image deviate from those obtained from the original image if the watermarked image is altered by common signal and geometric distortion. As a result, the watermark is susceptible to destroy. This is the reason why the existing fractal watermarking techniques hide the watermark by classification, instead of directly embedding a watermark into fractal parameters.

In a new type of orthogonalized fractal coding [12], range block mean substitutes luminance offset as one of the two affine parameters. Range block mean is a stable fractal parameter and a secure place to hide a watermark. Using range block means, a watermark can be embedded in the fractal transform domain. The watermark insertion add an m-sequence binary watermark to the range block means, followed by fractal decoding, As a result, the watermark diffuse throughout the whole pixel domain without any visual degradation. The digital watermark can be detected by evaluating correlation coefficients between the original watermark and the extracted watermark. Experimental results show that the watermark is robust against common signal and geometric distortion, such as lossy compression, median filter, scaling, clipping, etc.

The remainder of the paper is organized as follows. Section 2 introduces the orthogonalization fractal coding. The proposed fractal watermarking technique is described in Section 3. Experimental results are presented in Section 4, which is followed by the conclusions.

2. THE ORTHOGONAL FRACTAL CODING

Jacquin-styled fractal coding (non-orthogonalization) is a block-based fractal compression scheme [10, 11]. The parameters of affine transform are contrast scaling and luminance offset. Through orthogonalization, luminance offset is replaced by range block mean [12, 14].

Given an image I of size $2^m \times 2^n$, it first is partitioned into N $(=2^{m+n-2b})$ non-overlapping square range blocks of size $2^b \times 2^b$. A domain block pool Ω is then obtained from the original image by sliding a window of size $2^{b+1} \times 2^{b+1}$ within the image, starting at the top left corner of the image, in step-size of δ, along the horizontal or vertical direction.

For each range block $R=\{r_{ij}\}$, we search the domain block pool Ω to find a domain block $D=\{d_{ij}\}$ and an affine transformation τ (i.e., $\tau(D)=s*\sigma(D)+g$) such that $\tau(D)$ provides the best matching for R in the least squares sense. The parameters s and g are the scaling and luminous offset, respectively, and $\sigma(\cdot)$ is a contractive operator to contract the $2^{b+1} \times 2^{b+1}$ domain blocks into the same size as the $2^b \times 2^b$ range blocks.

Although the scaling and luminous offset are the most obvious parameterization of the affine transform, it has been shown that they strongly depends upon domain block pool Ω. Øien and Lepsøy [12] proposed applying Gram-Schmidt orthogonalization to the non-orthogonal basis in Jacquin's mappings for faster decoding: as a result, the model parameters for their fractal encoding become scaling and the range block mean, instead of the luminous offset. In terms of decoding, the two different parameterization leads to different decoding algorithms, namely:

$$R_{old}^{(n)} = s\sigma\left(D^{(n-1)}\right) + gU = \overline{R}U + s\sigma\left(D^{(n-1)} - \overline{D}U\right) \tag{1}$$

for the conventional parameterization, and

$$R_{new}^{(n)} = \overline{R}U + s\sigma\left(D^{(n-1)} - \overline{D^{(n-1)}}U\right) \tag{2}$$

for the orthogonalized parameterization. Here, U denotes a square block with all entries equal to 1, and $\overline{R}$ and $\overline{D}$ are the mean of range block R and domain block D. By (2), we can easily derive

$$\overline{R_{new}^{(n)}} = \overline{R_{new}^{(n-1)}} = \cdots = \overline{R_{new}^{(1)}} = \overline{R} \tag{3}$$

(3) means the orthogonalized decoding algorithm is a mean-invariant, in other words, the mean of R of the decoding image always equals the mean of R of the original image.

In practice, after-quantization to the optimal parameters increases collage error, and degrades the image fidelity. Hence, after $\overline{R}$ is quantized to $\overline{r}$ using quantization table $\{\overline{r}_i\}$, we consider the minimization as follows [13]

$$\hat{E}(R,D) = \left\| R - \overline{r}U - s_j\sigma(D - \overline{D}U) \right\|^2 \tag{4}$$

over $D=\{d_{ij}\} \in \Omega$ and a set of the pre-quantized fractal parameters $\{s_j\}$. The fractal code of R is then calculated as

$$\{\overline{r}, s, x, y\} = \arg\min_{D\in\Omega}\min_{s_j} \hat{E}(R,D) \tag{5}$$

where (x,y) is the coordinate of the top-left corner of the best-pair domain block.

3. FRACTAL WATERMARKING

A watermark placed in the transform domain is harder to be deciphered than one placed in the pixel domain. Cox et al. [3] assert a watermark should be placed over perceptually significant components (1000 highest magnitude DCT coefficients). Fractal block coding is a block-based transform, which maps a block into its fractal code $\{\overline{r}, s, x, y\}$. We have shown that the mean of range block is invariant for orthogonalization fractal decoding algorithm, and hence, range block means provides the secure places to hide a watermark. Since range block means correspond to low frequency components, and hence the embedded watermark is very difficult to remove and destroy by common signal and geometric distortion. After fractal decoding, the embedded watermark diffuses throughout the decoding image, and it is harder to decipher from the pixel domain without knowing the watermark extraction scheme.

Because range block means are quantized to small integers, we select an m-sequence for generating the binary watermark [1]. Next, we introduce how to measure the similarity between two watermarks, and then describe watermark embedding and detecting procedure.

3.1 Similarity Measurement of Watermarks

Given an image I of size $2^m \times 2^n$, if it is encoded with range blocks of size $2^b \times 2^b$, then the fractal codes of the image I consist of the fractal codes of N ($= 2^{m+n-2b}$) range blocks, i.e., $\{\bar{r}_u, s_u, x_u, y_u\}_{u=1}^N$. $\{\bar{r}_u\}_{u=1}^N$ are the means of N range blocks of the original image. A binary watermark of the size N is generated by an m-sequence with $l = m+n-2b$ stages, appended zero at the end, and is denoted by $\{w_u\}_{u=1}^N$ [1-2]. The watermarked image may be altered by common signal and geometric distortion, as a result, range block means $\{\bar{r}_u^*\}_{u=1}^N$ of the attacked image is different from $\{\bar{r}_u\}_{u=1}^N$ of the original image, in turn, the extracted watermark $\{w_u^*\}_{u=1}^N$ by differencing $\{\bar{r}_u^*\}_{u=1}^N$ and $\{\bar{r}_u\}_{u=1}^N$ is different from the original $\{w_u\}_{u=1}^N$. We measure the similarity of $\{w_u\}_{u=1}^N$ and $\{w_u^*\}_{u=1}^N$ by the correlation coefficient:

$$\rho(\{w_u\}_{u=1}^N, \{w_u^*\}_{u=1}^N) = \sum_{u=1}^{N} w_u * w_u^* \Bigg/ \sqrt{\left(\sum_{u=1}^{N} w_u^2\right)\left(\sum_{u=1}^{N} (w_u^*)^2\right)} \quad (6)$$

3.2 Watermark Insertion

A watermark $\{w_u\}_{u=1}^N$ is embedded using the following steps:

Step 1: Fractal encoding

Step 2: Add the binary watermark into the quantized code of range block means $\{\bar{r}_u + w_u\}_{u=1}^N$.

Step 3: Hiding watermark by fractal decoding of $\{\bar{r}_u + w_u, s_u, x_u, y_u\}_{u=1}^N$.

3.3 Watermark Detection

The watermark is identified as follows:

Step 1: Compute the average of all range blocks $\{\bar{r}_u^*\}_{u=1}^N$ from the attacked image.

Step 2: Obtain the attacked watermark $\{w_u^*\} = \{\bar{r}_u^* - \bar{r}_u\}$.

Step 3: Compute correlation coefficient according to (6), and identify existence of the watermark by a threshold T.

4. EXPERIMENTAL RESULTS

Because the proposed watermarking is image-independent, we take 512x512 "Barbara" as an example. The size of range block is 4x4, as a result, the "Barbara" image is partitioned into 128x128(=16384) range blocks. $\bar{R}$ and S are uniformly quantized to 7 bits and 2 bits, respectively. The fractal code of each range block is obtained according to (5) by searching the global domain block pool Ω.

Peak-Signal-Noise-Ratio (PSNR) is 45.53 dB between the watermarked and unwatermarked image, no visual difference is observed. The decoded watermark is similar to white noise image. Even if the original image is given, it is unlikely to decipher the watermark without the watermark extraction procedure.

The pseudorandom sequence $\{w_u\}_{u=1}^N$ is an m-sequence of the period N, $\{w_{u+k}\}_{u=1}^N$ is the $k-$shift of $\{w_u\}_{u=1}^N$. The autocorrelation function defined according to (6)

$$\rho(k) = \rho(\{w_u\}_{u=1}^N, \{w_{u+k}\}_{u=1}^N) = \begin{cases} 1 & k = lN \\ -1/N & k \neq lN \end{cases}$$

is two-valued. Since *m-sequences* have good auto-correlation property, they are suitable as a binary watermark [1-2]. N shifted *m-sequences* may be used as different watermarks for different users.

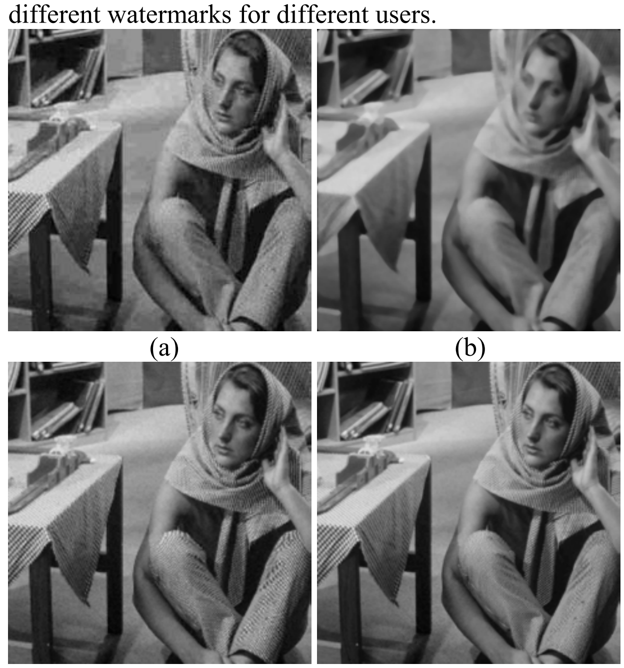
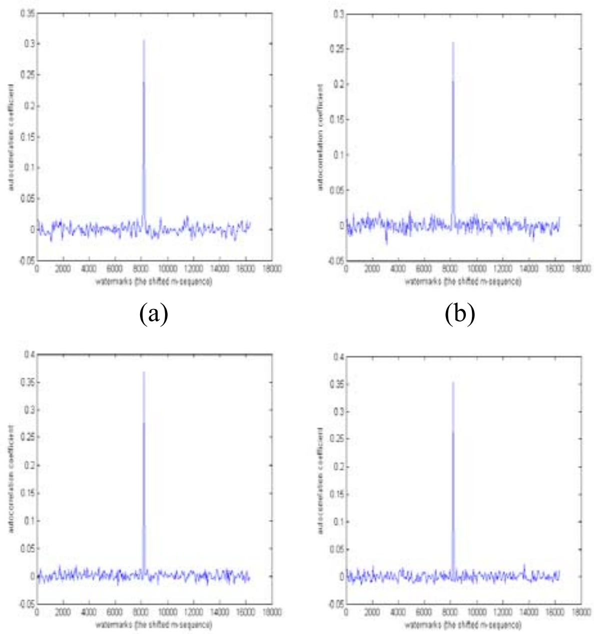


Fig. 1 The attacked watermarked images: (a) Compressed by JPEG (quality factor is 10); (b) Median filtering (5x5 window); (c) Scaling; (d) Clipping.

If the watermarked image is not attacked at all, then the embedded watermark can be retrieved without loss. When the watermark is perturbed, the correlation function still has a strong unique pulse, which corresponds to the embeded watermark. The correlation values from other random synthetic watermarks are close to zero. In general, when the peak is larger than a threshold *T*, we infer that the watermark exists in the image. In the paper, *T* is set at 0.2.

To test robustness of the proposed watermarking against common signal and geometric distortion, assume the embedded watermark is $\{w_{u+8192}\}_{u=1}^N$. Fig. 1 shows the attacked watermarked images, which are distorted by JPEG compression, median filtering, scaling, and clipping (about scaling and clipping process, see Cox [3]), and Fig. 2 shows the correlation functions between the retrieved watermark and N=16384 watermarks (shifted m-sequences). The correlation functions have the unique pulse at k=8192, and the corresponding peaks are larger than the threshold (T=0.2). This demonstrates that the embedded watermark can be detected and uniquely identified.



(a) (b) (c) (d)

Fig. 2 The correlation functions: the correlation coefficients between the retrieved watermark from Fig. 1 and N=16384 watermarks (shifted m-sequences). The peaks at k=8192 are 0.31, 0.26, 0.37 and 0.35 for (a), (b), (c) and (d), respectively.

5. CONCLUSION

In the paper, we propose a novel watermarking technique to hide a binary watermark into the compressed image files by fractal coding. The watermark insertion procedure adds a pseudorandom binary watermark to the quantized code of the range block means. The watermark is detected and uniquely identified by correlation function. Our experiments show that the proposed watermarking is very robust against signal and geometric distortion.

REFERENCES

[1] R.G. Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermarking,” in *Proc. ICIP94*, 1994, vol. 2,pp. 86-90.

[2] A.Z.Tirkel, R.G.van Schyndel, C.F.Osborne. "A Two Dimensional Digital Watermark,” *DICTA'95*, University of Queensland, Brisbane, pp.378-383, December 6-8, 1995.

[3] I. Cox, J. Killian, F. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Trans. IP*, vol. 6, no. 12, pp. 1673-1687, 1997.

[4] W. Zhu, Z. Xiong, and Y. Zhang, “Multiresolution watermarking for Image and Video”, *IEEE Trans. IP*, vol. 9, no. 4, 1999.

[5] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information Hiding---A Survey,” *Proceedings of IEEE, special issue on protection of multimedia content*, vol. 87, no.7, pp. 1062-1078, July 1999.

[6] Paul Davern, Michael Scott. “Fractal Based Image Steganography,” *Information hiding: first international workshop*, Cambridge, UK. Springer Lecture Notes, no. 1174, pp. 279-294, 1996.

[7] J. Puate and F. Jordan, “using fractal compression scheme to embed a digital signature into image,” *Proc. SPIE Photonics East Symposium*, Boston, USA, Nov. 18-22, 1996.

[8] C. H. Li and S. S. Wang, “Digital Watermarking using Fractal Image Coding,” *IEICE Trans. Fundamentals*, vol. E83-A, no. 6, pp. 1286-1288.

[9] P. Bas, J. M. Chassery, and F. Davoine, “Using the Fractal Code to Watermark Images,” in *Proc ICIP98*, vol. 1, pp. 469-473.

[10]A. E. Jacquin, “Fractal image coding: A review”, *Proc. IEEE*, vol. 81, no.10, pp. 1451-1465, 1993.

[11]E. W. Jacobs, Y. Fisher, and R. D. Boss, “Image Compression: A Study of Iterated Transform Method,” *Signal Processing*, vol. 29, pp. 251-263, Dec. 1992.

[12]G. E. Øien and S. Lepsøy, “A Class of Fractal Image coders with Fast Decoder Convergence,” *Fractal Image Compression: Theory and Application*, Springer-Verlag, 1995 (in Chapter 8)

[13]C. Tong and M. Pi, “Fast Fractal Image compression using Adaptive Search,” *IEEE Trans. on IP*, vol.10, pp.1269-1277, Sep. 2001.

[14]M. Pi, A. Basu, and M. Mandal, “A new decoding algorithm based on range block mean and contrast scaling”, Proc. of *ICIP2003*, Barcelona, Spain, September 14-17, 2003.

[15]T. Ida and Y. Sambonsugi, “Image Segmentation Using Fractal Coding,” *IEEE Trans. Circuits and System for Video Technology*, vol. 5, no. 6, pp.567-570, Dec. 1995.

[16]M. Pi, M. Mandal and A. Basu, “Image Retrieval Based on Histogram of New Fractal Parameters,” *Proceeding of ICASSP 2003*, Hong Kong