Journal of Zhejiang University SCIENCE A
ISSN 1009-3095
http://www.zju.edu.cn/jzus
E-mail: jzus@zju.edu.cn

Science Letters:

A new asymmetric watermarking scheme based on a real fractional DCT-I transform*

GUI Guo-fu (桂国富)†, JIANG Ling-ge (蒋铃鸽), HE Chen (何 晨)

(*Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*)

†E-mail: gf_gui@sjtu.edu.cn

Received Aug. 25, 2005; revision accepted Dec. 28, 2005

Abstract: A new asymmetric watermarking scheme is proposed in this letter. In the proposed scheme, a secret real fractional DCT-I transform and a primitive watermark are employed to generate an asymmetric watermark. The secret watermark for embedding is derived from the primitive watermark, and is embedded in the large fractional DCT-I transformation coefficients of a cover signal. The asymmetric detection procedure is performed using a correlation test. Simulation results showed that the asymmetric detection is reliable, and that the scheme can provide minimum security.

Key words: Asymmetric watermarking, DCT-I, Fractional transforms
doi:10.1631/jzus.2006.A0285 **Document code:** A **CLC number:** TP309

INTRODUCTION

Due to the ease of transmitting digital data and copying without loss of quality, the unauthorized distribution of digital multimedia contents has become easy and popular. Digital watermarking is the most promising technique to protect the copyright of digital multimedia contents (Cox *et al*., 2001). Most of the proposed watermarking schemes are symmetric, in which keys for watermark detecting are identical to those for watermark embedding. Therefore, symmetric watermarking schemes are not secure when the detector is publicly available to an attacker (Eggers *et al*., 2000).

In recent years, some researchers began to study asymmetric watermarking schemes, wherein detection keys are different from watermarking keys. The asymmetric scheme can provide public detection, and the embedded watermark cannot be deduced from the public detection key. Some new asymmetric watermarking schemes were proposed recently (Kim *et al*., 2004; Choi *et al*., 2004). In these schemes, embedded watermarks are independent of cover signals, and are inserted in each coefficient of the cover signals, which will degrade the quality of cover signals greatly. In this letter, we propose a new asymmetric watermarking scheme. The embedded watermark is derived from a primitive watermark and the cover signal, and is embedded in the large coefficients of a fractional DCT-I transformation of the cover signal. The key for asymmetric detection is the inverse fractional DCT-I transformation of the primitive watermark.

REAL FRACTIONAL DCT-I TRANSFORM

The kernel matrix of the DCT-I transform (Pei and Yeh, 2001) is shown as

$$\boldsymbol{M}=\left[\sqrt{\frac{2}{N}}k_m k_n \cos\left(\frac{mn\pi}{N}\right)\right]$$

for $m,n=0,1,\ldots,N-1$, where k_m is defined as

$$k_m=\begin{cases}1/\sqrt{2}, & m=0 \text{ and } m=N;\\ 1, & \text{otherwise.}\end{cases}$$

* Project (Nos. 60372076 and 60272082) supported by the National Natural Science Foundation of China

The eigenvalues of DCT-I transform matrix, λ_i, are 1 or –1, and the unique eigenvectors $\boldsymbol{v}_i$ can be obtained from the even Hermite-Gaussian eigenvectors of the Fourier matrix in the cosine case. The eigendecomposition of an $N\times N$ DCT-I transform matrix $\boldsymbol{M}$ can be expressed by

$$\boldsymbol{M}=\boldsymbol{V}\boldsymbol{\Lambda}\boldsymbol{V}^{\mathrm{T}},$$

where, $\boldsymbol{V}=[\boldsymbol{v}_1|\boldsymbol{v}_2|\ldots|\boldsymbol{v}_N]$, $\boldsymbol{\Lambda}=\mathrm{diag}(\lambda_1,\lambda_2,\ldots,\lambda_N)$. With these eigenvalues and eigenvectors, the fractional transform matrix $\boldsymbol{M}_\alpha$ is constructed by

$$\boldsymbol{M}_\alpha=\boldsymbol{V}\boldsymbol{\Lambda}_\alpha\boldsymbol{V}^{\mathrm{T}}. \tag{1}$$

To design a real fractional transform matrix, a method is presented (Venturini and Duhamel, 2004). Set $N=2^b$ (b is an integer and $b\geq 2$) and $\lambda_1=\ldots=\lambda_{N/2}=-1$, a block-diagonal matrix $\boldsymbol{\Lambda}_\alpha$ is computed by

$$\boldsymbol{\Lambda}_\alpha=\begin{bmatrix}\boldsymbol{G1}_{N/2}(\theta(\alpha)) & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{G2}_{N/2}(\eta(\alpha))\end{bmatrix},$$

where, $\boldsymbol{G1}$ and $\boldsymbol{G2}$ are block-diagonal Givens matrices whose blocks are

$$\boldsymbol{G1}_2(\theta(\alpha))=\begin{bmatrix}\cos(\theta(\alpha)) & \sin(\theta(\alpha))\\ -\sin(\theta(\alpha)) & \cos(\theta(\alpha))\end{bmatrix}$$

and analogously for $\boldsymbol{G2}$ with the angle η. θ and η are functions of the real fraction α. Among the choices for θ and η, we consider the one with $\theta(\alpha)=2\pi\alpha$ and $\eta(\alpha)=\pi\alpha$.

THE PROPOSED SCHEME

An embedded watermark and an asymmetric watermark (a key for asymmetric detection) are generated using the following method.

(1) Generate a primitive watermark $\boldsymbol{u}$ with length N. Each element of $\boldsymbol{u}$ is a binary number of {1, –1}.

(2) Construct a fractional DCT-I transform matrix $\boldsymbol{M}_\alpha$ using Eq.(1), where the parameter α is selected randomly and it is a real fractional parameter.

(3) Compute the asymmetric watermark $\boldsymbol{w}_\mathrm{p}$ by

$$\boldsymbol{w}_\mathrm{p}=\boldsymbol{M}_\alpha^{\mathrm{T}}\boldsymbol{u}. \tag{2}$$

(4) Obtain a transformed signal $\boldsymbol{x}_\mathrm{T}$ as follows

$$\boldsymbol{x}_\mathrm{T}=\boldsymbol{M}_\alpha\boldsymbol{x}, \tag{3}$$

where $\boldsymbol{x}$ is the cover signal.

(5) Generate a secret binary sequence $\boldsymbol{t}$ according to the following rule

$$t(i)=\begin{cases}1, & x_\mathrm{T}(i)>T,\\ 0, & \text{otherwise},\end{cases}$$

where $t(i)$ and $x_\mathrm{T}(i)$ are the ith element of $\boldsymbol{t}$ and $\boldsymbol{x}_\mathrm{T}$, respectively, and assuming that there are M elements of $\boldsymbol{t}$ whose value is 1.

(6) Compute the embedded watermark $\boldsymbol{w}_\mathrm{e}$ by

$$w_\mathrm{e}(i)=u(i)t(i), \tag{4}$$

where, $w_\mathrm{e}(i)$, $u(i)$ and $t(i)$ are the ith element of $\boldsymbol{w}_\mathrm{e}$, $\boldsymbol{u}$ and $\boldsymbol{t}$, respectively.

In the proposed scheme, the asymmetric watermark, the watermark generation algorithm, the embedding and detection algorithms can be public. If an attacker obtains the fraction α, he can construct the fractional DCT-I transform, and then derive $\boldsymbol{u}$, $\boldsymbol{t}$ and $\boldsymbol{w}_\mathrm{e}$ from the public information using Eqs.(2), (3) and (4), respectively. Therefore, the fractional parameter α should be secret, and only the content owner holds them.

The watermark $\boldsymbol{w}_\mathrm{e}$ is embedded in the fractional transformed domain, and the watermarked signal $\boldsymbol{y}$ is computed by

$$\boldsymbol{y}=\boldsymbol{M}_\alpha^{\mathrm{T}}\left(\boldsymbol{M}_\alpha\boldsymbol{x}+\gamma\boldsymbol{w}_\mathrm{e}\right)=\boldsymbol{x}+\gamma\boldsymbol{M}_\alpha^{\mathrm{T}}\boldsymbol{w}_\mathrm{e}, \tag{5}$$

where γ is the watermarking strength.

The user can perform an asymmetric detection using a correlation test between the asymmetric watermark $\boldsymbol{w}_\mathrm{p}$ and the received signal $\hat{\boldsymbol{y}}=\boldsymbol{y}+\boldsymbol{n}$, where $\boldsymbol{n}$ represents the possible attacking noise. The correlation coefficient is computed as follows

$$\begin{aligned} c_{\mathrm{p}} &= \frac{1}{N\gamma}\boldsymbol{w}_{\mathrm{p}}^{\mathrm{T}}\hat{\boldsymbol{y}} = \frac{1}{N\gamma}\boldsymbol{w}_{\mathrm{p}}^{\mathrm{T}}(\boldsymbol{x}+\boldsymbol{n}+\gamma\boldsymbol{M}_{\alpha}^{\mathrm{T}}\boldsymbol{w}_{\mathrm{e}}) \\ &= \frac{1}{N\gamma}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{M}_{\alpha}(\boldsymbol{x}+\boldsymbol{n}+\gamma\boldsymbol{M}_{\alpha}^{\mathrm{T}}\boldsymbol{w}_{\mathrm{e}}) \\ &= \frac{1}{N\gamma}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{M}_{\alpha}(\boldsymbol{x}+\boldsymbol{n}) + \frac{1}{N}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{w}_{\mathrm{e}} \\ &= \frac{1}{N\gamma}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{M}_{\alpha}(\boldsymbol{x}+\boldsymbol{n}) + \frac{M}{N}. \end{aligned} \tag{6}$$

Assuming that $\boldsymbol{x}$ and $\boldsymbol{n}$ are Gaussian distributed, we have $c_{\mathrm{p}}\approx M/N$. After selecting an appropriate decision threshold, the asymmetric detection can be realized.

The content owner can perform a symmetric detection as follows. The received signal $\hat{\boldsymbol{y}}$ is first transformed through the matrix Eq.(1), and then a correlation test is performed between the watermark $\boldsymbol{w}_{\mathrm{e}}$ and the transformed signal $\boldsymbol{M}_{\alpha}\hat{\boldsymbol{y}}$ as follows

$$\begin{aligned} c_{\mathrm{s}} &= \frac{1}{M\gamma}\boldsymbol{w}_{\mathrm{e}}^{\mathrm{T}}\boldsymbol{M}_{\alpha}\hat{\boldsymbol{y}} = \frac{1}{M\gamma}\boldsymbol{w}_{\mathrm{e}}^{\mathrm{T}}\boldsymbol{M}_{\alpha}(\boldsymbol{x}+\boldsymbol{n}+\gamma\boldsymbol{M}_{\alpha}^{\mathrm{T}}\boldsymbol{w}_{\mathrm{e}}) \\ &= \frac{1}{M\gamma}\boldsymbol{w}_{\mathrm{e}}^{\mathrm{T}}\boldsymbol{M}_{\alpha}(\boldsymbol{x}+\boldsymbol{n}) + 1 \approx 1. \end{aligned} \tag{7}$$

In the end, the symmetric detection statistic c_{s} is compared with a predefined decision threshold, and then we can determine the presence or absence of the watermark $\boldsymbol{w}_{\mathrm{e}}$.

Since the asymmetric watermark is public, and the proposed scheme is based on the correlation detection, subtraction attack (Kim *et al*., 2004) can disable the public detection. But it cannot disable the symmetric detection, which will be demonstrated in the simulation. Therefore, the proposed scheme can provide the minimum security (Kim *et al*., 2004).

SIMULATION RESULTS

We apply our scheme to image watermarking. The test image shown in Fig.1a is a gray-level Lena of size 128×128. One thousand asymmetric watermarks and the corresponding embedded watermarks are generated using the method described in Section 3, and their length is 1024. The watermarks are embedded as follows. The test image is first decomposed with 2-level wavelet transform. Then the mid-frequency coefficients of the decomposed image are transformed by a fractional DCT-I transform defined as Eq.(1). After that, an embedded watermark is inserted in the transformed coefficients. In the end, inverse fractional DCT-I transform and inverse wavelet transform are performed on the watermarked coefficients. The watermarked image of PSNR 43.26 shown in Fig.1b has good perceptual quality. The detection probability and the false positive probability with different decision thresholds are shown in Fig.2 and Fig.3 showing that the asymmetric detections are highly reliable.

(a) (b)

Fig.1 Original (a) and watermarked (b) images

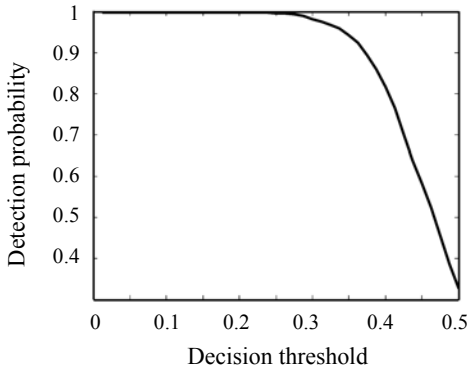

Fig.2 The asymmetric detection probability with different decision thresholds

The subtraction attack is one of the most important public attacks in asymmetric watermarking schemes. For correlation-based asymmetric watermarking schemes, this attack can disable the asymmetric detection. However, asymmetric watermarking schemes should be able to provide a successful symmetric detection when an asymmetric detection is disabled by the subtraction attack. In the proposed scheme, an attacker can disable the asymmetric de-

tection using the subtraction attack: $\boldsymbol{y}_a=\boldsymbol{y}-\beta\boldsymbol{w}_p$, where β is the attacking strength. In the simulation, we set $\beta=\gamma$, and perform the subtraction attack on the 1000 watermarked images. The asymmetric and symmetric detection statistics are shown in Fig.4. The first 1~1000 watermark detections are asymmetric, and the 1001~2000 ones are symmetric. From Fig.4, we can clearly see that the symmetric detections are successful even if the asymmetric detections are disabled.

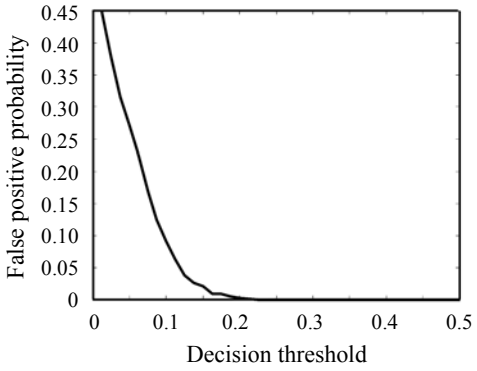

Fig.3 The asymmetric false positive probability with different decision thresholds

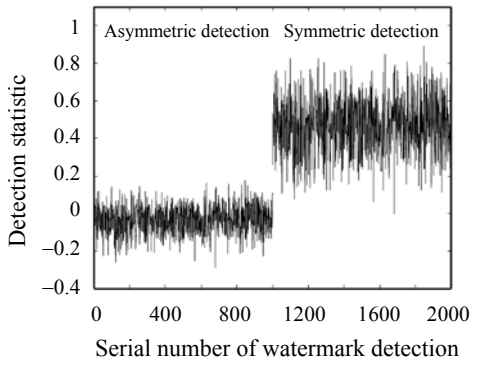

Fig.4 Asymmetric and symmetric detection statistics under subtraction attacks

CONCLUSION

In this letter, we present a new asymmetric watermarking scheme, in which the fractional DCT-I transform is used to construct the asymmetric watermark. The embedded watermark is inserted in large coefficients of the transformed cover signal, and the watermarked signal has good perceptual quality. In the simulations, we apply the scheme to image watermarking, with the simulation results demonstrating that the scheme can provide reliable asymmetric detections. Moreover, symmetric detections have been performed on the images that suffered subtraction attack. The results showed that the scheme can provide the minimum security.

References

Choi, H., Lee, K., Kim, T., 2004. Transformed-key asymmetric watermarking system. *IEEE Signal Process Lett.*, **11**(2):251-254. [doi:10.1109/LSP.2003.819873]

Cox, J., Miller, M.L., Bloom, J.A., 2001. Digital Watermarking. Morgan Kaufmann Publishers, San Francisco, CA, USA.

Eggers, J.J., Su, J.K., Girod, B., 2000. Asymmetric Watermarking Schemes. Tagungsband Des GI Workshops Sicherheit in Mediendaten. Berlin, Germany, p.107-123.

Kim, T.Y., Choi, H., Lee, K., Kim, T., 2004. An asymmetric watermarking system with many embedding watermarks corresponding to one detection watermark. *IEEE Signal Process Lett.*, **11**(3):375-377. [doi:10.1109/LSP.2003.822923]

Pei, S.C., Yeh, M.H., 2001. The discrete fractional cosine and sine transforms. *IEEE Trans. Signal Processing*, **49**(6):1198-1207. [doi:10.1109/78.923302]

Venturini, I., Duhamel, P., 2004. Reality preserving fractional transforms. *IEEE Int. Conf. Acoustics, Speech, and Signal Process*, **5**:205-208.