A Rotation-Invariant Secure Image Watermarking Algorithm Incorporating Steerable Pyramid Transform

Jiangqun Ni*, Rongyue Zhang, Jiwu Huang, Chuntao Wang, and Quanbo Li

Department of Electronic and Communication Engineering, Sun Yat-Sen University
Guangzhou 510275, P.R. China
Phn: 86-20-84036167
issjqni@mail.sysu.edu.cn

Abstract. Robustness and security are the key issues in the development of image watermarking algorithm. A new rotation invariant security image watermarking algorithm based on steerable pyramid transform is proposed in this paper. The algorithm is characterized as follows: (1) the rotation invariance and robust watermarking are achieved concurrently on the same transform domain; (2) the rotation synchronization is obtained through template matching by using steerable pyramid transform, which satisfies the shiftability in orientation condition; (3) the watermarks are embedded into an oriented subband at angle θ, which can be interpolated with base filter kernels and used as a key in watermark detection to increase the security of watermark; (4) the watermark detector is designed based on the steerable vector HMM model. High robustness is observed against StirMark attacks and their joint attacks.

1 Introduction

With the popularity of Internet, the copyright protection, authentication and tamper proofing of digital media are becoming increasingly important. And thus digital watermarking, especially for image and video, has become the domain of extensive research. The DWT is playing an increasingly important role in the development of watermarking algorithm [1][2], due to its good spatial-frequency characteristics and its wide applications in image/video coding standards. One of the drawbacks of standard wavelet transforms is in that they are sensitive to the orientation of the input image. If the image is rotated, then in the wavelet domain, the wavelet coefficients change completely. Actually, the wavelet coefficients of the rotated image are not just be simply rotated, but are also modified. One way to remedy this situation is to replace the standard wavelet decomposition with the steerable pyramid transform proposed by Simoncelli and Freeman [3][4]. The steerable pyramid is a linear multiscale, multi-orientation image decomposition where the basis functions are directional derivative operators. One can convolve the image with a range of oriented filter kernels tuned to cover all orientations of interests in the image, where the oriented filter kernels can be interpolated with a fixed set of basis kennels to avoid high computational cost[4].

* Corresponding author.

Y.Q. Shi and B. Jeon (Eds.): IWDW 2006, LNCS 4283, pp. 446 – 460, 2006.

According to J.Cox[2], there exists two fundamental attributes for watermarking system, i.e., robustness and security. Robustness means the resistance against common signal distortions, such as geometrical distortions and other signal processing operations. While the security means the resistance against malicious and intentional modification of the watermark signal.

For robustness of watermarking, one of the major challenges is to increase its performance to resist against geometrical attacks such as rotation, scaling, translation, cropping and shearing. These geometrical distortions cause the loss of geometrical synchronization that is necessary in watermark detection and decoding [2]. Although some significant progresses have been made recently [5][6][7], the existing approaches generally require an extensive computational load, or need to work in multiple domains (such as DWT and DFT) and are not robust to JPEG compression. There exist two different approaches to resisting geometrical attacks, i.e., the blind and non-blind ones. For the non-blind approach, due to the availability of the original image, the loss of synchronization caused by geometrical distortions can be recovered efficiently. While the blind one, which does not use the original image in watermark extraction, has wider applications but is obviously more challenging. Three major approaches for the blind solutions have been reported in the literatures. The first approach hides the watermark signal in the invariant domain of the host signal (invariant with respect to rotation, scaling, translation and etc.). In [8], Ruanaidh *et al.* proposed a watermarking scheme based on transform invariants via applying Fourier-Mellin transform to the magnitude spectrum of the original image. However, the resulting stego-image quality is poor due to interpolation errors. The second approach exploits the self-reference principle based on an auto-correlation function (ACF) or the Fourier magnitude spectrum of a periodical watermark [9]. Unfortunately, the proposed watermarking scheme is generally vulnerable to loss coding operation such as JPEG compression. The third approach incorporates the template for watermark synchronization. In [7], Kang and Huang proposed a DWT-DFT composite watermarking scheme, where the messages and templates are embedded into DWT and DFT domain, respectively. Relatively high robustness is observed against both affine transformation and JPEG compression. However the proposed watermarking scheme is required to work in multiple domains.

In this paper, a new robust image watermarking algorithm based on the steerable pyramid transform is proposed, where the rotation synchronization and robust watermarking against JPEG compression are concurrently obtained on the same transform domain. The rotation synchronization is achieved through the template matching, which is just the operation of interpolation with greatly reduced complexity of computation. Under the framework of steerable pyramid, the watermarks can be embedded into an oriented subband at angle θ, which can also be interpolated with base filter kernels and used as a key in watermark detection to increase the security of watermark.

The vector HMM model developed in [10] is also extended to steerable wavelet domain, and the resulting HMM based watermark detector achieves significant improvement in performance compared to the conventional correlation detector. Simulation results demonstrate that the proposed watermarking algorithm is robust against joint Stirmark attacks (the joint attacks of rotation and JPEG compression, additive noise, median cut, etc).

The remainder of the paper is organized as follows. In section 2, the framework of steerable pyramid is briefly reviewed. And the theory behind efficient rotation

synchronization and watermark security in steerable pyramid transform domain is established. By replacing the standard wavelet transform with steerable pyramid, the WD-HMM model is extended and reviewed in section 3. Section 4 gives the overall framework of the proposed rotation invariant secure image watermarking algorithm. The simulation results and analysis are presented in section 5. Finally, we draw the conclusion in section 6.

2 The Steerable Pyramid Transform for Image Watermarking

The standard wavelet transforms have only limited oriented resolution. If the image is rotated, then in the wavelet domain the wavelet coefficients change completely. To solve these problems, a variant on standard wavelet transform, i.e., the steerable pyramid, was proposed by Simoncelli [3]. This transform satisfies the shiftability in orientation.

2.1 The Steerable Pyramid

The steerable pyramid is based on a set of steerable filter kernels which could be tuned to cover all orientations of interest in the image. Given the 2-D, circularly symmetric Gaussian function G:

$$G(x, y) = e^{-(x^2+y^2)} \tag{1}$$

where the scaling and normalization constants have been set to 1 for convenience.

The first partial derivatives in x and y of the Gaussian function constitute a set of filter kernels, i.e.,

$$\begin{aligned} G^0(x, y) &= \frac{\partial}{\partial x} G(x, y) = -2xe^{-(x^2+y^2)}, \\ G^{90}(x, y) &= \frac{\partial}{\partial y} G(x, y) = -2ye^{-(x^2+y^2)}. \end{aligned} \tag{2}$$

It is straight to show that a filter $G^\theta(x, y)$ at arbitrary orientation θ can be interpolated with G^0 and G^{90}:

$$G^\theta(x, y) = \cos(\theta)G^0(x, y) + \sin(\theta)G^{90}(x, y) \tag{3}$$

Let $f(x, y)$ denotes the original image, then

$$R^0(x, y) = (f * G^0)(x, y) \tag{4}$$

is the image filtered for vertical features and

$$R^{90}(x, y) = (f * G^{90})(x, y) \tag{5}$$

for horizontal features. For image features at orientation θ, we further have

$$R^\theta(x, y) = \cos(\theta)R^0(x, y) + \sin(\theta)R^{90}(x, y) \tag{6}$$

For large number of orientations, Eq. (6) is computationally far less expensive than filtering with $G^\theta(x, y)$ directly for an equal number of orientations.

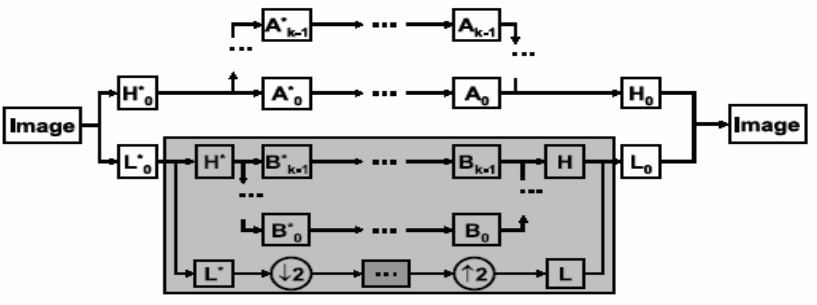


Fig. 1. Block diagram of steerable pyramid

Steerable pyramid is a recursive multi-scale and multi-orientation decomposition. Fig.1 shows its block diagram, where H and L are high-pass and low-pass filters, respectively. And the B_k 's are the oriented steerable filters for a resolution scale. As a bonus, the steerable pyramid representation is also translation-invariant. It is noted that second and third derivatives of Gaussian function give rise to 3 and 4 oriented subbands Without loss of generality, we use two oriented subbands per resolution scale in this paper, i.e., $k = 2$ (unless mentioned otherwise).

2.2 Rotation Synchronization Using Steerable Pyramid

Using the steerable pyramid above, we now develop the theory and framework for rotation synchronization.

***Proposition 1*:** Suppose that $f(x, y)$ and $f^{\theta}(x, y)$ are the original image and its rotated version by θ, respectively. $G^{\theta}(x, y)$ and $R^{\theta}(x, y)$ are the filter kernel and response at angle θ. R^{θ_1,θ_2} represents the response of $G^{\theta_2}(x, y)$ to $f^{\theta_1}(x, y)$. And $T[\circ,\theta]$ denotes the rotation operator such that for any image $f(x, y)$, $T[f(x, y),\theta]$ is $f(x, y)$ rotated by θ anti-clockwise. Then for $\forall\theta$ and a steerable pyramid with two oriented subbands, $R^{0,0}(x, y) = T\left[R^{\theta,\theta}(x, y),-\theta\right]$ and $R^{0,90}(x, y) = T\left[R^{\theta,\theta+90}(x, y),-\theta\right]$.

***Proof*:** Recall that the first derivative of Gaussian function results in a set of steerable filter, i.e., $G^{0}(x, y)$ and $G^{90}(x, y)$.

$$\begin{aligned} R^{\theta,\theta}(x, y) &= f^{\theta}(x, y) * G^{\theta}(x, y) = f^{\theta}(x, y) * \left[G^{0}(x, y)\cos(\theta) + G^{90}(x, y)\sin(\theta)\right] \\ &= f\left[x\cos(\theta) + y\sin(\theta), y\cos(\theta) - x\sin(\theta)\right] * \left[-2xe^{-(x^2+y^2)}\cos(\theta) - 2ye^{-(x^2+y^2)}\sin(\theta)\right]. \end{aligned} \tag{7}$$

Rotate the $R^{\theta,\theta}(x, y)$ by $(-\theta)$, we have

$$\begin{aligned} x &= x'\cos(-\theta) + y'\sin(-\theta), \\ y &= y'\cos(-\theta) - x'\sin(-\theta). \end{aligned} \tag{8}$$

Substitute (8) into (7) and have some trigonometric manipulations, we further have

$$T\left[R^{\theta,\theta}(x, y), -\theta\right] = f(x', y')\left[-2x'e^{-(x'^2+y'^2)} - 2y'e^{-(x'^2+y'^2)}\right]. \tag{9}$$

Therefore, we obtain $T(R^{\theta,\theta}(x, y), -\theta) = R^{0,0}(x, y)$. Similarly, we have $T(R^{\theta,90+\theta}(x, y), -\theta) = R^{0,90}(x, y)$. The result can also be extended to the cases where 3 or 4 steerable filters are used [3].

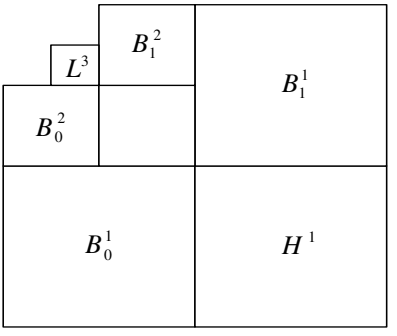


Fig. 2. Two scale steerable pyramid model decomposition for *k*=2

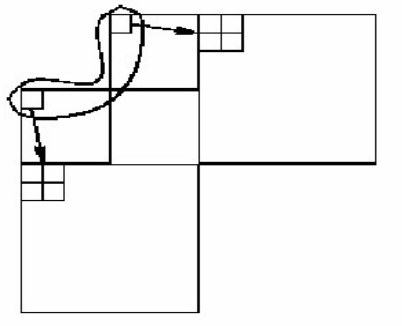


Fig. 3. Steerable wavelet vector HMM (two levels)

Fig.2 shows a two-stage steerable pyramid decomposition for *k*=2, where the L^j and H^1 denote the low-pass bank at scale *j* and high-pass band at scale 1, respectively; and B_k^j represents the *k*'s ($k = 0,1$; 0 and 1 corresponds to the oriented subband at 0^0 and 90^0) seeable pass-band at scale *j*. **Proposition 1 implies the principle for rotation synchronization using steerable pyramid.** The designed template is placed in B_0^1 for highest oriented resolution. For a rotated image $f^{\theta}(x, y)$, if the template is detected in BT, where $BT = T\left[B_0^1\cos(\theta) + B_1^1\sin(\theta), \quad -\theta\right]$, then the rotated image is recovered with angle θ. The detailed template design and efficient matching scheme are included in section 4.

2.3 The Security of Watermarking

One of the objectives for watermarking systems design is security, i.e., the embedded watermark should only be accessible by authorized parties, and be undetectable by

unauthorized users in general. The framework of steerable pyramid provides the necessary security for watermarking system design to some extent.

For a *J*-level decomposition of steerable pyramid $\left\{H^1, L^{J+1}, B_0^j, B_1^j, j = 1 \cdots J\right\}$, rather than the subband B_0^j and B_1^j at scale *j*, two oriented subband at angle θ_1 and θ_2 are randomly selected:

$$\begin{aligned} B_{\theta_1}^j &= B_0^j \cos(\theta_1) + B_1^j \sin(\theta_1), \\ B_{\theta_2}^j &= B_0^j \cos(\theta_2) + B_1^j \sin(\theta_2). \end{aligned} \tag{10}$$

The watermark signals are embedded according to:

$$\hat{B}_{\theta_1}^j = B_{\theta_1}^j + \alpha_1 w_1^j \ and \ \hat{B}_{\theta_2}^j = B_{\theta_2}^j + \alpha_2 w_2^j \tag{11}$$

According to (10), the $\hat{B}_0^j$ and $\hat{B}_1^j$ can be reconstructed from $B_{\theta_1}^j$ and $B_{\theta_2}^j$ via

$$\begin{aligned} \hat{B}_0^j &= \left[\hat{B}_{\theta_1}^j \sin(\theta_2) - \hat{B}_{\theta_2}^j \sin(\theta_1)\right] \Big/ \left[\cos(\theta_1)\sin(\theta_2) - \cos(\theta_2)\sin(\theta_1)\right], \\ \hat{B}_1^j &= \left[\hat{B}_{\theta_1}^j \cos(\theta_2) - \hat{B}_{\theta_2}^j \cos(\theta_1)\right] \Big/ \left[\sin(\theta_1)\cos(\theta_2) - \sin(\theta_2)\cos(\theta_1)\right]. \end{aligned} \tag{12}$$

where $j = 1, \cdots, J$. And finally based on $\left\{H^1, L^{J+1}, \hat{B}_0^j, \hat{B}_1^j, j = 1 \cdots J\right\}$ the watermarked image is obtained via inverse steerable pyramid transform.

The angle θ for oriented subband can be randomly selected from a large space, ranging from $0 \sim 2\pi$. Combined with other secure schemes, such as the random selection of vector tree and Direct Sequence Spread Spectrum (DSSS) [10], the watermark signal can be hidden in a secret multi-scale and multi-orientation pyramid transform domain, making it difficult for the hostile attack that seeks to remove or destroy the watermark at specific locations.

3 The Steerable Wavelet HMM Model

The approach in [10] can be extended to develop the steerable wavelet domain vector HMM for robust watermarking system design. For a steerable pyramid with two oriented subband as shown in Fig.2, each coefficient $w_{j,i}$ in B_k^j has its hidden state $s_{j,i}$ ($1 \le j \le J$, $j = J$ denotes the coarsest scale). Given $s_{j,i} = m$, $w_{j,i}$ is modeled with a zero-mean Gaussian $g(0, \sigma_{j,i}^{(m)})$. Also if a two-states HMM is adopted, the pdf of $w_{j,i}$ is given by

$$f_j(w) = p_j^{(1)} g(w; \sigma_j^{(1)}) + p_j^{(2)} g(w; \sigma_j^{(2)}) \tag{13}$$

where $p_j^{(1)} + p_j^{(2)} = 1$, and $p_j^{(1)}, p_j^{(2)}$ in (13) represent the probability that $w_{j,i}$ is small or large (in statistical sense), respectively.

The steerable pyramid HMM model captures the energy dependency across scale by using Markov chain to describe the probability of hidden state transition from the parent node to its four child nodes, i.e.,

$$A_j = \begin{pmatrix} p_j^{1\to 1} p_j^{1\to 2} \\ p_j^{2\to 1} p_j^{2\to 2} \end{pmatrix}, \; j = 1, 2, \cdots, J-1. \tag{14}$$

where $p_j^{m'\to m}$ represents the probability that child node is in state m given that its parent node is in state m'. Let $\mathrm{p}_j = \left(p_j^{(1)} p_j^{(2)}\right)$ and $\mathrm{p}_j = \mathrm{p}_{j+1}\mathrm{A}_j$, then

$$\mathrm{p}_j = \mathrm{p}_J \mathrm{A}_{J-1}\mathrm{A}_{J-2}...\mathrm{A}_j, \; j = 1, 2, \cdots, J-1. \tag{15}$$

Therefore, the steerable wavelet HMM model is completely defined by a set of parameters:

$$\theta = \{\mathrm{p}_J, \mathrm{A}_{J-1}, ..., \mathrm{A}_1; \sigma_j^{(m)}, (j = 1, ..., J, m = 1, 2)\}. \tag{16}$$

Taking into account the cross-orientation dependency of steerable wavelet coefficients, the steerable vector HMM model is developed as shown in Fig.3. Denote the subband coefficients at orientation d (d =0,1), scale j and location i as $w_{j,i}^d$, the grouping operation results in vectors of coefficients: $\mathbf{w}_{j,i} = \left(w_{j,i}^{(0)} w_{j,i}^{(1)}\right)^T$. For vector WD-HMM model, we have

$$f_j(\mathbf{w}) = p_j^{(1)} g(\mathbf{w}, \mathbf{C}_j^{(1)}) + p_j^{(2)} g(\mathbf{w}; \mathbf{C}_j^{(2)}) \tag{17}$$

where $g(\mathbf{w}; \mathbf{C})$ denotes the zero-mean multivariate Gaussian density with covariance matrix $\mathbf{C}$, i.e.,

$$g(\mathbf{w}; \mathbf{C}) = \frac{1}{\sqrt{(2\pi)^n \left|\det(\mathbf{C})\right|}} \exp(-\mathbf{w}^T \mathbf{C}^{-1} \mathbf{w}), \tag{18}$$

where n is the numbers of orientations (in this case n=2).

Therefore, the steerable pyramid coefficients of image can be modeled by a vector HMM model with a set of parameters:

$$\Theta = \{\mathrm{p}_J, \mathrm{A}_{J-1}, ..., \mathrm{A}_1; \mathbf{C}_j^{(m)}, (j = 1, ..., J, m = 1, 2)\} \tag{19}$$

4 Watermarking Embedding and Detection

The rotation-invariant secure image watermarking scheme based on steerable pyramid transform (SPT) is given in this section, which includes the efficient template matching for rotation synchronization, the strategy of watermarking security, and the steerable vector HMM based watermarking scheme.

4.1 Embedding of Template and Watermark

Fig.4 shows the overall structure for the proposed template and watermark embedding scheme.

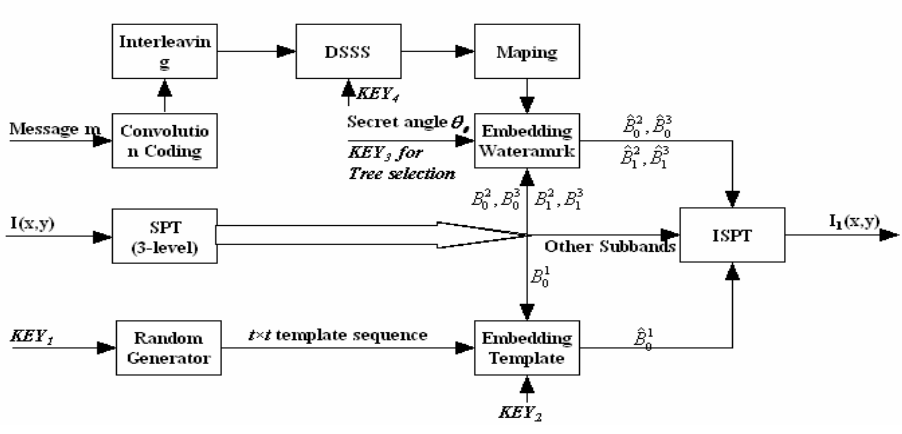


Fig. 4. Embedding scheme of the template and watermark

4.1.1 Watermark Coding

For watermark message **m** , the watermark coding includes:

1. Convolution coding for watermark **m**: let $\mathbf{m} = \{m_i; i = 1,2,...,L, m_i \in [0,1]\}$ be the watermark message, where L is the length of the message. Then **m** is coded with the 1/3 convolution code to generate a sequence $\mathbf{m}_c$ with the length of L_c;
2. Interleaving of $\mathbf{m}_c$ to generate $\mathbf{m}_I$;
3. DSSS for $\mathbf{m}_I$: The interleaved message $\mathbf{m}_I$ is DSSS (Direct Sequence Spread Spectrum) with PN sequence **p** of length N_p, which is generated with a secret key KEY_4. The coded watermark message is $\mathbf{w}=\{w_i; w_i \in \{-1,+1\}, i = 1,2,..., L_c * N_p\}$.

4.1.2 Template Design and Embedding

As the filter bank in Fig.1 is non-orthogonal and near PR (perfect reconstruction), and uses a set of non-separated filters of 9×9 for the steerable band-pass filter B_k , there exists some error spreading around its neighbor if some coefficients in oriented subband B_j^k are modified. Fig.5 shows the effect of error spreading, where (1) the image is decomposed with 4 scale steerable pyramid and the coefficient at (32,32) in B_0^1 is modified by –50; (2) the image is reconstructed with the modified coefficients; (3) the image is decomposed into pyramid again and the coefficients around (32,32) is more or less modified. As the radius of the region where the coefficients are significantly affected is about 6 pixels, we design a template of 32×32 with lattice structure. The lattice points of the template are spaced apart with 10 pixel alone x and y axis to alleviate the effect of error spreading.

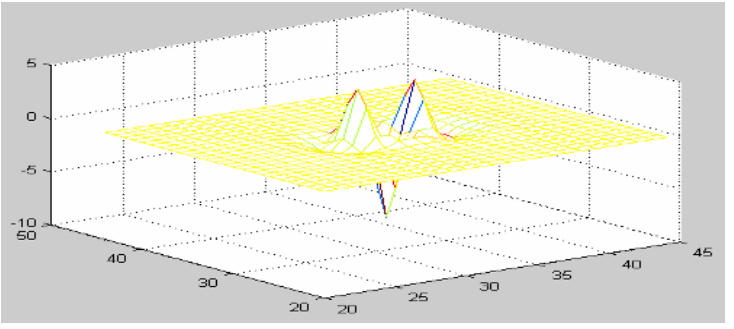


Fig. 5. The effect of error spreading in oriented subband

A PN sequence $\{t(i)\}$ of length 32×32 is generated with key KEY_1, and used to construct the template described above. Also the template is place in the center of B_0^1 to avoid the cropping attack. Let $w(u_i, v_i)$ be the coefficient in B_0^1 which is used to host the template bit $t[i]$, then the template are embedded according to:

$$w'(u_i, v_i) = w(u_i, v_i) + \beta * t(i), t(i) \in \{+1.-1\} \text{ and } i \in [1,1024] \subset Z . \tag{20}$$

where β is a global parameter to adjust the embedding strength.

4.1.3 Watermark Embedding

For the coded watermark message $\mathbf{w} = [w_i]$ of length $L_c * N_p$, the watermark embedding process is as follows:

1. The original image $I(x, y)$ is decomposed into L-level steerable pyramids (L=3 in our scheme), where scale 1 for template and scale 2-3 for watermark message;
2. As described in section 2.3, rather than the band $\{B_0^j, B_1^j; j = 2,3\}$, the watermark messages are embedded into randomly selected oriented subband $\{B_{\theta_1}^j, B_{\theta_2}^j; j = 2,3\}$ to increase the security of watermarking. The θ_1 and θ_2 are assigned to be θ_0 and $(\theta_0 + 90)$ in our work for good visual quality and high capacity. And θ_0 is used as the key in watermark detection;
3. Under the framework of HMM model, the carrier of watermark signal is vector tree. In the interest of resisting against JPEG attack, the watermark is only embedded into the coarsest 2 scales ($j = 2,3$). The resulting vector tree includes 10-nodes as shown in Fig.3;
4. Each vector tree is used to embedded 1 bit for the coded message $\mathbf{w} = [w_i]$, and the optimal strategy for 1-to-10 mapping $\mathbf{k}$ is designed based on the principle given in [10]. Fig.6 shows the mapping rule, where the dot and circle stand for same and inverse version of the to-be-embedded bit w_i, respectively;

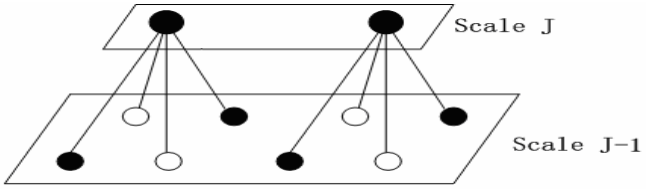


Fig. 6. Optimal mapping strategy for each vector tree

5. The t^{th} mapped pattern $\mathbf{k}(t)$ for w_t is embedded into the vector tree according to

$$\mathbf{x}'(t,i) = \mathbf{x}(t,i) + \beta * a(t,i) * \mathbf{k}(t,i) \tag{21}$$

where $\mathbf{x}(t,i)$ is the i^{th} node of the t^{th} vector tree, $a(t,i)$ is its corresponding HVS masking weight and β is the global adjustment factor for embedding strength [10].

6. After all coded message bits are embedded into $L_c * N_p$ vector trees which are randomly selected with the secret key KEY_3, the inverse steerable pyramid transform is performed to obtain the watermarked image $I'(x, y)$.

4.2 Rotation Synchronization Via Template Matching

For a rotated watermarked image, the rotation synchronization should be achieved before the watermark can be extracted. Let $I^{\theta}(x, y)$ be the rotated image, and the template $t[i]$ generated with key KEY_1 is contained in the oriented subband B_0^1 of original image $I(x, y)$, if the template can be detected via a correlation detector in $T\left[B_{\theta}^1, \ -\theta\right]$, then the rotated image is synchronized with angle θ. Incorporating the steerable pyramid transform, two optimized strategies are developed for efficient template matching, which are described as follows:

A. Efficient template matching

1. For a matching angle α and the template $t[i]$ of 32×32, the correlation can be computed via (22):

$$t'[i] = B_{\alpha}^1\left[u_i \cos(\alpha) + v_i \sin(\alpha), \quad v_i \cos(\alpha) - u_i \sin(\alpha)\right], i = 1, 2, \cdots, 1024.$$

$$Cor(\alpha) = \frac{\sum_{i=1}^{1024} t'[i]t[i]}{\sqrt{\sum_{i=1}^{1024} t'^2[i]}\sqrt{\sum_{i=1}^{1024} t^2[i]}} \tag{22}$$

where (u_i, v_i) is the location of $t[i]$ in B_0^1.

2. It is noted that, instead of rotating each pixel of B_{α}^1 by $-\alpha$, only 32×32 pixels in B_{α}^1 are accessed to compute the $Cor(\alpha)$ using Eq. (22). Therefore the computation load is greatly reduced.

B. Coarse to fine template searching

1. The template searching is begun with a coarse stage, where a relatively large step $\Delta\alpha_c$ (e.g., $\Delta\alpha_c = 0.5$) is used to compute the $Cor(\alpha)$ with $\alpha = \alpha + \Delta\alpha_c$. A coarsely recognized rotation angle θ_c is obtained.
2. Based on the roughly estimated θ_c , a fine searching is carried out with an accurate step $\Delta\alpha_f$ (say, $\Delta\alpha_f = 0.1$) around the neighbor of θ_c .

4.3 Steerable HMM-Based Watermark Detection

Assume the watermark signal is embedded into secure oriented subband $\left\{B_{\theta_0}^j, B_{\theta_0+90}^j\right\}_{j=2,3}$ with key θ_0 .

1. Generate the secure oriented subbands $\left\{B_{\theta_0}^j, B_{\theta_0+90}^j\right\}_{j=2,3}$ of $I(x, y)$ from the oriented subbands $\left\{B_0^j, B_1^j\right\}_{j=2,3}$ of $I^\theta(x, y)$ according to

$$\begin{aligned} B_{\theta_0}^j &= T[B_0^j \cos(\theta+\theta_0) + B_1^j \sin(\theta+\theta_0), -\theta]_{j=2,3} , \\ B_{\theta_0+90}^j &= T[B_0^j \cos(90+\theta+\theta_0) + B_1^j \sin(90+\theta+\theta_0), -\theta]_{j=2,3} . \end{aligned} \tag{23}$$

2. The recovered oriented subbands $\left\{B_{\theta_0}^j, B_{\theta_0+90}^j\right\}_{j=2,3}$ are used to construct the posterior vector HMM model with parameters set Θ . The vector trees to carry the watermark signal are determined with the key KEY_3.
3. The watermark is detected with a vector HMM detector as described in [10]

$$\ln f_x(\mathbf{T}_Z^t - \mathbf{a}^t * \mathbf{k}_0 \mid \Theta) > \ln f_x(\mathbf{T}_z^t - \mathbf{a}^t * \mathbf{k}_1 \mid \Theta) , \tag{24}$$

   where $f_x(\circ)$ is the likelihood function, $\mathbf{T}_z^t$ stands for the selected vector tree, and $\mathbf{k}_0$ and $\mathbf{k}_1$ are the mapping pattern for bit 0 and 1, respectively (only 1 bit message is embedded into each selected tree). Eq.(24) implies that the HMM detector outputs the pattern with maximum likelihood, which is taken as the detected watermark;
4. Based on the detected sequence, the operations of de-mapping, de-DSSS, and convolution decoding are implemented to get the decoded watermark signal $\hat{\mathrm{w}}$.

5 Simulation Results and Analysis

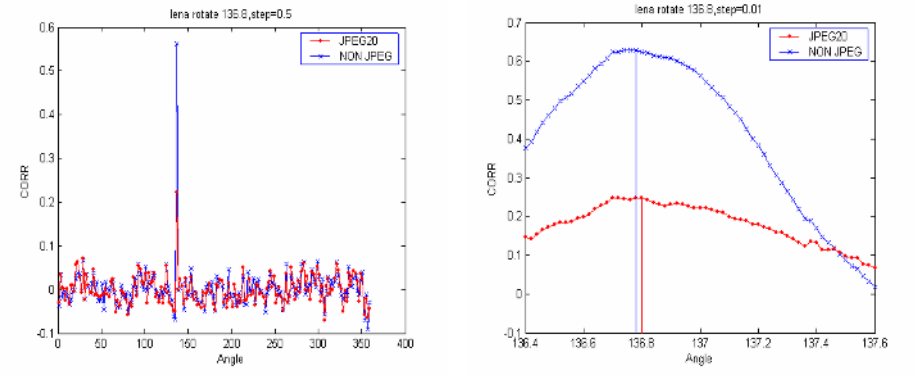
In our experiments, 5 standard 512*512*8b images with different texture characteristic are tested. The images are firstly decomposed into 3-level pyramids with the steerable pyramid transform; the 32*32 template and 60-bit meaningful watermark messages are embedded in the B_0^1 and $\left\{B_\theta^j, B_{\theta+90}^j\right\}_{j=2,3}$, respectively. Here, θ is the parameter to describe the secure oriented subband. Fig.7 shows the steerable pyramid based watermarked image with template.

Fig. 7. Watermarked images with template: (a) baboon (PSNR=35.91dB); (b) fishingboat (PSNR=38.98dB); (c) f16 (PSNR=37.38dB); (d) lena (PSNR=40.60dB); (e) peppers (PSNR=37.86dB)

Fig.8 shows the performance of rotation synchronization under JPEG attacks with steerable pyramid transform, where the watermarked image "lena" in Fig.7 is rotated by 136.8^o and the coarse to fine template matching scheme developed in section 4.2 is employed. For the case without JPEG attack ("x" mark line), the searching step is set to be 0.5^o at the coarse stage and the estimated angle is 137^o, as shown in Fig.8 (a). Then based on the roughly estimated angle, the fine searching is implemented with step of 0.01^o, and the finally recognized rotation angle is 137.78^o, as shown in Fig.8 (b). The 2-stage searching process needs only 820 searching operations and takes 0.5s when it is implemented with Matlab6.5 on a P4-2.4G PC, which shows good searching resolution and efficiency. The searching process under JPEG20 attack ("$\bullet$" mark line) is also given in Fig.8, which demonstrates that the proposed rotation synchronization scheme is robust to deep JPEG attack. Similar results are observed with other test images.

To evaluate the secure watermarking strategy described in section 2.3, the secret angle θ is set to 12.36^o, and two oriented subband at 12.36^o and 102.36^o ($=\theta+90^0$) are generated to embed watermark signal. Fig.9 gives the security performance under different orientation angle θ, where the "x" mark, "$\bullet$" mark and "o" mark line stand for BER performance after HMM detector, De-DSSS and Viterbi decoding, respectively. Fig.9 shows that the farther away the oriented subband derivates from the secure angle θ, the higher the detection BER would be. The watermark signal can only be recovered from those oriented subbands near the secret angle θ ($\Delta\theta \approx 15^o$). Considering the fact that the secure angle θ used in watermark detection runs from 0 to 2π, when combined with other strategies such as the random selection of vector tree and the key to generate the PN for DSSS, the proposed scheme greatly increases the security of watermarking to hostile attacks.

The watermarked images in Fig.7 are attacked with StirMark4.0 [12], and then the proposed steerable HMM based detectors are employed to detect the watermark signals. Table 1 shows the performance under Stirmark attacks, which are very robust against Stirmark attacks. Due to the fact that the steerable pyramid transform is near PR with a reconstruction PSNR of 50dB, the objective quality (PSNR) of the watermarked image with steerable pyramid is relatively lower than that when other PR transforms, such as DCT and 9/7 biorthogonal wavelet, are used.



(a) Estimation at coarse stage (b) Estimation at fine stage

Fig. 8. Template matching

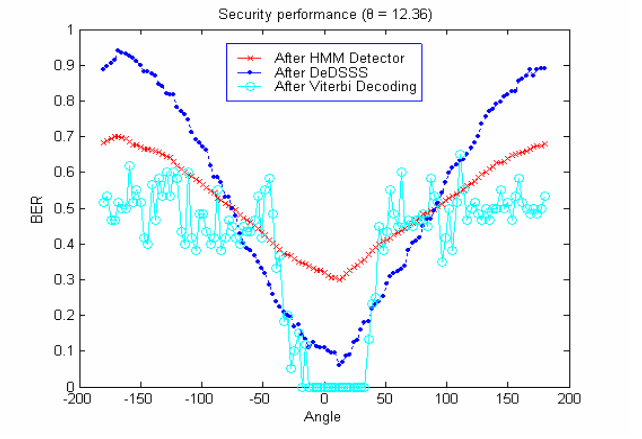


Fig. 9. Security performance under different orientation angle θ

Table 1. Performance of steerable vector HMM-based detector under StriMark attack

Images / Attacks	lena	baboon	F16	fishingboat	peppers
PSNR(dB)	40.60	35.91	37.38	38.98	37.86
JPEG	10~100	15~100	12~100	13~100	10~100
AddNoise	1~5	1~3	1~3	1~2	1~6
MedianCut	2~5	Fail	2~5	2~3	2~5
Gaussian	Ok	Ok	Ok	Ok	Ok
Sharpening	Ok	Ok	Ok	Ok	Ok

Table 2. Performance under joint StriMark attacks: Rotation 30.5° + (JPEG, Additive noise, MedianCut, or filter)

Attacks \ Images	lena	baboon	f16	fishingboat	peppers
PSNR(dB)	40.60	35.91	37.38	38.98	37.86
JPEG	13~100	22~100	19~100	20~100	17~100
Additive noise	1~4	Fail	1	Fail	1~4
MedianCut	2~3	Fail	2~3	Fail	2~3
Gaussian	Ok	Ok	Ok	Ok	Ok
Sharpening	Ok	Fail	Ok	Fail	Ok

In addition, the performance against the joint attacks is also investigated. The images in Fig.7 are first rotated by 30.5° and then attacked with the StirMark4.0 such as JPEG compression, addtitive noise, median cut, and filter (Gaussian and sharpening). After the rotation synchronization is obtained with template matching, the watermark is extracted from the secure oriented subbands based on steerable HMM model. The performance with the proposed watermarking algorithm is given in Table 2, which demonstrates high robustness against joint Stirmark attacks.

6 Conclusion

In this paper, we present a rotation-invariant secure image watermarking algorithm based on the steerable pyramid transform. The rotation synchronization is obtained through efficient template matching via steerable pyramid transform, which satisfies shiftability in orientation condition. By embedding the watermark signal into randomly selected oriented subband at angle θ, which can be interpolated with base filter kernels and used as a key in watermark detection, the security of the proposed watermarking system is greatly increased. The HMM model is also extended to develop a steerable wavelet HMM model for robust watermarking system design. Under the framework of steerable pyramid transform, the rotation synchronization, robustness and security of watermarking are concurrently obtained in the same transform domain. And simulation results with the proposed algorithm demonstrate high robustness against StirMark attacks (rotation, JPEG compression, additive noise, median cut, etc.) and Joint StirMark attacks (the Joint attack of rotation and JPEG compression, etc).

Acknowledgments

The authors appreciate the supports received from NSFC (60325208, 90604008), 973 Program (2006CB303104) and NSF of Guangdong (04205407).

References

1. P.Meerwald and A.Uhl, "A Survey of Wavelet-Domain Watermarking Algorithms," *Proceeding of SPIE*, Security and Watermarking of Multimedia Contents III, Vol.4314, San. Jose, CA, USA, Jan. 2001.
2. J.Cox, M.L.Miller and J.A.Bloom, Digital Watermarking, *Morgan Kaufmann*, 2001
3. E.P.Simoncelli, W.T.Freeman, E.H.Adelson and D.J.Heeger, "Shiftable Multi-scale Transform," *IEEE Trans. on Information Theory*, Vol.38(2), pp.587-607, March 1992.
4. W.T.Freeman and E.H.Adelson, "The Design and Use of Steerable Filters," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol.13, No.9, pp.891-906, Sep.1991.
5. F.Hartung and M.Kutter, "Multimedia Watermarking Techniques," *Proc. of IEEE*, Vol.87, pp.1079-1107, July 1999.
6. C.Y.Lin, M.Wu, J.A.Bloom, J.Cox, M.L.Miller and Y.M.Lui, "Rotation, Scale and Translation Resilient Watermarking for Images," *IEEE Trans. on Image Processing*, ol.10, pp.767-782, May 2001.
7. X.G. Kang, J.W. Huang, Y.Q.Shi and Y.Lin, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression," *IEEE Trans. on Circuits and Systems for Video Technology*, Vol.13, No.8, pp: 776-786, Aug. 2003.
8. J.Ruanaidh and T.Pun, "Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking," *Signal Processing*, Vol.6, No.3, pp.303-317, 1998.
9. M.Kutter, "Watermarking Resistance to Translation, Rotation and Scaling," *Proc. of SPIE: Media Systems Applications*, Vol.3528, pp:423-431, 1998.
10. J.Ni, R.Zhang, J.Huang and C.Wang, "A Robust Multi-bit Image Watermarking Algorithm Based on HMM in Wavelet Domain," *Lecture Notes in Computer Science: Proc.of IWDW 2005*, Vol. 3710, pp: 110-123, Springer-Verlag.
11. C. Fei, D. Kundur and R. H. Kwong, "Analysis and Design of Watermarking Algorithms for Improved Resistance to Compression," *IEEE Trans. on Image Processing*, Vol. 13, No. 2, pp. 126-144, Feb. 2004.
12. StirMark, [Online], Available: http://www.cl.cam.ac.uk/~fapp2/watermarking /stirmark/.