The Journal of Systems and Software 86 (2013) 222–232

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

# A lossless copyright authentication scheme based on Bessel–Fourier moment and extreme learning machine in curvature-feature domain

Guangyong Gao [a,b], Guoping Jiang [a,*]

[a] College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[b] School of Information Science & Technology, Jiujiang University, Jiujiang 332005, China

ARTICLE INFO

*Article history:*
Received 10 January 2012
Received in revised form 26 July 2012
Accepted 28 July 2012
Available online 4 August 2012

*Keywords:*
Multiple zero-watermarking
Copyright authentication
Bessel–Fourier moment
Extreme learning machine (ELM)
Curvature feature

ABSTRACT

To overcome some drawbacks existing in current zero-watermarking methods, a lossless copyright authentication scheme is proposed in this paper. This scheme designs a multiple zero-watermarking algorithm based on Bessel–Fourier moment and extreme learning machine (ELM) in curvature-feature domain, develops a method for image feature enhancement and noise suppression in curvature-feature domain, and presents a simple algorithm which uses Bessel–Fourier moment phase to estimate the rotation angle of the rotation-attacked image. The experimental results, involving five types of images, indicate the proposed scheme has better overall performance compared to other five current methods, especially in the aspects of resisting high ratio cropping and large angle rotation attacks. Finally, some related factors including phase and magnitude components, feature vector dimension and ELM optimization are considered in the algorithm performance evaluation.



## 1. Introduction

At present, digital watermarking technology is broadly adopted in the copyright authentication of digital images to avoid pirating behavior. Most of the existing watermarking schemes modify image contents in spatial domain or frequency domain (Akhaee et al., 2010; Cui and Li, 2011; Gao and Jiang, 2010; Lou et al., 2006; Mohanty and Bhargava, 2008; Mohanty et al., 2006), which cannot be directly applied to protect the remote sensing images and medical images because these images do not permit alteration. Recently, a lossless watermarking method called zero-watermarking, which does not change the image information, is presented to enhance the visual quality of protected images. This method is very suitable to prove the copyrights of this kind of image (Chang and Lin, 2008; Chen et al., 2005; Furon, 2007; Sang et al., 2006; Tsai et al., 2010; Wen et al., 2003; Rawat and Raman, 2012).

Wen et al. (2003) presented the notion of zero-watermarking, and utilized high-order cumulants, which can reflect the global feature of an image, to construct zero-watermarking. The proposed scheme is robust to common signal processing and some global geometric attacks such as slight rotation and scaling. Chen et al. (2005) proposed a wavelet-based zero-watermarking scheme that does not require the original image for logo verification, and cryptographic tools, such as digital signature and timestamp, are introduced to make copyright proving publicly verifiable. In Furon (2007), an unifying framework for zero-watermarking scheme was constructed using partial differential equation. Chang and Lin (2008) proposed an adaptive copyright protection scheme in the spatial domain. The approach uses Sobel operator to extract the edge feature of an image as watermarking and allows the image owner to enhance the robustness of watermarking through the adjustment of the watermarking strength using a threshold, and the rest of this method is also like Chen's method. Sang et al. (2006) proposed a zero-watermarking scheme using the spatial domain-based neural network (NN). The differences between the intensity values of the selected pixels and the corresponding output values of the neural network model are calculated to generate a binary pattern, which is regarded as watermarking. Tsai et al. (2010) presented a robust lossless watermarking technique based on $\alpha$-trimmed mean algorithm and support vector machine (SVM). The scheme trained SVM to memorize the relationship between the watermarking and the image-dependent watermarking, and the robustness to malicious manipulations is enhanced using the $\alpha$-trimmed mean operator. Rawat and Raman (2012) proposed a lossless copyright protection algorithm based on fractional Fourier transform and visual cryptography (VC). The algorithm uses the visual secret sharing scheme to construct master share and ownership share. The extracted features of the original image by singular value decomposition (SVD) are utilized to generate the master share, and using VC technique, ownership share is generated with

* Corresponding author at: College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210003, China.
*E-mail addresses:* gaoguangyong@163.com (G. Gao), jianggp@njupt.edu.cn (G. Jiang).

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.07.070

the help of secret image and master share. In the phase of ownership identification, the copyright can be proved using the revealed secret image by stacking the master share and the ownership share.

The above methods for zero-watermarking still have some drawbacks as follows: (1) They are resistant to common signal processing and some geometrical attacks such as noise, filter, compression, scaling, etc. but they are still sensitive to high ratio cropping and large angle rotation attacks. At present, the studies robust to high ratio cropping and large angle rotation attacks mainly focus on embedding watermarking, while rarely touch on zero-watermarking. (2) They do not give the test and analysis for false alarm, while the false alarm is an important issue in zero-watermarking schemes. (3) They only provide the experiment results for common images, for example, Lena image, but seldom involve other types of images including cartoon image, medical image, remote-sensing image and artistic image.

Aiming at these problems, a lossless copyright authentication scheme is presented in this paper. The scheme is based on Bessel–Fourier moment and extreme learning machine (ELM) in curvature-feature domain, which is mainly due to three reasons: (1) The improved multi-scale corner detector based on curvature scale space (CSS) (He and Yung, 2008) has better detection performance for feature points than some popular detectors such as Harris, SUSAN and original CSS. (2) Bessel–Fourier moment (Xiao et al., 2010), proposed recently as a new image moment, has better performance than Zernike and orthogonal Fourier-Mellin moments defined in the polar coordinate in terms of invariant recognition accuracy due to its good orthogonality, and has been successfully applied to the pattern recognition field. (3) Compared with NN and SVM, ELM improves tremendously the generalization ability and learning speed of learning network (Huang et al., 2004, 2006).

The followings are our main contributions:

(1) Design a multiple zero-watermarking scheme based on Bessel–Fourier moment vector and ELM in curvature-feature domain.
(2) Develop a method for image feature enhancement and noise suppression in curvature-feature domain, and present a simple estimation algorithm for the rotation angle of the rotation-attacked image using Bessel–Fourier moment phase.
(3) Show the proposed multiple zero-watermarking scheme has better overall performance compared to the five current methods, especially in the aspects of resisting high ratio cropping and large angle rotation attacks.

The rest of the paper is organized as follows. In Section 2, a brief background about curvature corner detector, Bessel–Fourier moment and extreme learning machine is provided. Section 3 describes a robust multiple zero-watermarking scheme for image copyright authentication using Bessel–Fourier moment feature vector and ELM model in curvature-feature domain. Simulation and performance analysis are given in Section 4. Finally, Section 5 concludes the presentation.

## 2. Related knowledge

### 2.1. Curvature corner detector

The definiton of curvature $\kappa$ is given by (Mokhtarian and Mackworth, 1992)

$$\kappa(u,\sigma)=\frac{X_u(u,\sigma)Y_{uu}(u,\sigma)-X_{uu}(u,\sigma)Y_u(u,\sigma)}{\left(X_u(u,\sigma)^2+Y_u(u,\sigma)^2\right)^{1.5}} \tag{1}$$

where $X_u=x(u)\otimes g_u(u,\sigma)$, $X_{uu}=x(u)\otimes g_{uu}(u,\sigma)$, $Y_u=y(u)\otimes g_u(u,\sigma)$, $Y_{uu}=y(u)\otimes g_{uu}(u,\sigma)$, $\otimes$ is the convolution operator, $g_u(u,\sigma)$, $g_{uu}(u,\sigma)$ are the first and second derivatives of $g(u,\sigma)$, respectively, and $g(u,\sigma)$ denotes a Gaussian function with deviation $\sigma$.

The basic idea of an improved multi-scale corner detection algorithm based on CSS with adaptive threshold and dynamic region of support (ROS) is summarized as follows (He and Yung, 2008).

(1) The edge contours are obtained from the gray level image by Canny edge detector, then the T-junctions are found after the gaps in the contours are filled.
(2) The curvatures are computed at a fixed low scale, $\sigma_{low}$, for each contour to retain all true corners.
(3) All of the curvature local maxima are considered as corner candidates. These candidates include the false corners, which can be removed by using an adaptive local curvature threshold and dynamic ROS. The adaptive threshold is given by

$$T(u)=C\times\bar{\kappa}=C\times\frac{1}{L_1+L_2+1}\sum_{i=u-L_2}^{u+L_1}\kappa(i) \tag{2}$$

where the mean value, $\bar{\kappa}$, is used to represent the curvature of a neighborhood region. The dynamic ROS is defined as from one of the neighboring local curvature minima to the next, $u$ in the equation above is the position of corner candidate in the curve, $L_1$ and $L_2$ are the sizes of ROS, and $C$ is a coefficient.
(4) The corners are tracked from the highest scale to the lowest scale to improve localization, the T-junction and other corners are compared and one of two closely spaced corners is removed.

### 2.2. Bessel–Fourier moments

#### 2.2.1. Definition of Bessel–Fourier moments

In the polar coordinate, the Bessel–Fourier moments using the first kind of Bessel function are defined as (Xiao et al., 2010)

$$B_{nm}=\frac{1}{2\pi a_n}\int_0^{2\pi}\int_0^1 f(r,\theta)J_v(\lambda_n r)\exp(-jm\theta)r\,dr\,d\theta \tag{3}$$

where $n=0,1,2,\ldots$, $m=0,1,2,\ldots,n+m$ is the moment order, $a_n=[J_{v+1}(\lambda_n)]^2/2$ is the normalization constant, and $f(r,\theta)$ is the image. $J_v(\lambda_n r)$ is the Bessel polynomial in $r$ of degree $n$, $\lambda_n$ is the $n$-th zero of $J_v(r)$. $J_v(x)$ is the first kind of Bessel function with integer order (Amos, 1986).

#### 2.2.2. Rotation invariance

In terms of Eq. (3), the Bessel–Fourier moment of the rotated image is given by

$$\begin{aligned}B'_{nm}&=\frac{1}{2\pi a_n}\int_0^{2\pi}\int_0^1 f'(r,\theta)J_v(\lambda_n r)\exp(-jm\theta)r\,dr\,d\theta\\&=\frac{1}{2\pi a_n}\int_0^{2\pi}\int_0^1 f(r,\theta-\alpha)J_v(\lambda_n r)\exp(-jm\theta)r\,dr\,d\theta\end{aligned} \tag{4}$$

where $f'(r,\theta)$ is the rotated version of an image $f(r,\theta)$ with the rotation angle $\alpha$, and $f'(r,\theta)=f(r,\theta-\alpha)$. Let $\phi=\theta-\alpha$, Eq. (4) can be written as

$$\begin{aligned}B'_{nm}&=\frac{1}{2\pi a_n}\int_0^{2\pi}\int_0^1 f(r,\phi)J_v(\lambda_n r)\exp(-jm(\phi+\alpha))r\,dr\,d\phi\\&=\left[\frac{1}{2\pi a_n}\int_0^{2\pi}\int_0^1 f(r,\phi)J_v(\lambda_n r)\exp(-jm\phi)r\,dr\,d\phi\right]\exp(-jm\alpha)\\&=B_{nm}\exp(-jm\alpha)\end{aligned} \tag{5}$$

It is concluded by Eq. (5) that the rotation of an image with the rotation angle $\alpha$ only leads to a phase shift of Bessel–Fourier moments. So we have

$$|B_{nm}| = |B'_{nm}| \tag{6}$$

where $|\cdot|$ denotes the magnitude operator. Hence, the magnitudes of the Bessel–Fourier moments have rotation invariance.

### 2.3. Extreme learning machine

Extreme learning machine (ELM) is a new algorithm of machine learning using Moore–Penrose (MP) generalized inverse theory, which can solve the output weight value of learning network by a step calculation (Huang et al., 2004, 2006). Compared with NN and SVM, ELM vastly boosts generalization ability and learning speed of a network.

The training model of ELM adopts single hidden layer feedforward networks (SLFNs). Let $m$, $M$, $n$ be the node numbers of input layer, hidden layer and output layer, respectively, $g(x)$ is activation function of hidden layer neuron, $b_i$ is the threshold of the $i$th hidden node, $o_j = [o_{j1}, o_{j2}, \ldots, o_{jn}]^T$ denotes the network output, for $N$ arbitrary distinct samples $(x_i, t_i)$, where $x_i = [x_{i1}, x_{i2}, \ldots, x_{im}]^T \in R^m$ and $t_i = [t_{i1}, t_{i2}, \ldots, t_{in}]^T \in R^n$, the network model of ELM is mathematically modeled as

$$\sum_{i=1}^{M} \beta_i g(w_i \cdot x_i + b_i) = o_j, \quad j = 1, 2, \ldots, N \tag{7}$$

where $w_i = [w_{1i}, w_{2i}, \ldots, w_{mi}]$ is the weight vector connecting the input nodes and the $i$th hidden node, $\beta_i = [\beta_{i1}, \beta_{i2}, \ldots, \beta_{in}]$ is the weight vector connecting the $i$th hidden node and the output nodes.

The training object of ELM is to seek a set of $w_i$, $\beta_i$ and $b_i$ for meeting $\sum_{j=1}^{N} ||o_j - t_j|| = 0$, i.e.,

$$\sum_{i=1}^{M} \beta_i g(w_i \cdot x_i + b_i) = t_j, \quad j = 1, 2, \ldots, N \tag{8}$$

## 3. Proposed zero-watermarking scheme

Using Bessel–Fourier moment feature vector and ELM model in curvature-feature domain, we propose a robust multiple zero-watermarking scheme for image copyright authentication. Firstly, for strengthening the image feature and suppressing the noise, a method is developed based on lifting wavelet transform, which can meanwhile make the distribution of feature domains more uniform. Then rotation angle estimation between an original image and its rotated version is presented using Bessel–Fourier moment phase. Finally, a multiple zero-watermarking detection scheme is designed based on ELM training model, multiple watermarkings are embedded into the extracted feature regions and the test image is classified as watermarked when the number of correctly detected watermarkings marked as $\eta$ from all feature regions satisfies the condition of $\eta \geq 2$.

### 3.1. Feature enhancement and noise suppression

Firstly, the original $N \times N$ size image is devided into non-overlapping sub-blocks with the size of $M \times M$ noted as $S_i$, $i = 1, 2, 3, \ldots, \lfloor N/M \rfloor^2$. Then $L$-level db1 lifting wavelet transform is executed on every sub-block and the size of generated low-frequency approximate sub-band is $1 \times 1$, subsequently, an approximate image marked as *appimg* is reconstructed by all low-frequency coefficients. Since $L$-level low-frequency coefficients concentrate the most of energy of original image, which reflects the most important content feature of original image, thus compared with original image, the approximate image *appimg* contains more intensive feature information.

Considering simultaneously both the feature point number and size of the feature domain, for original $512 \times 512$ size image, parameters $M$, $L$ are set as 4, 2, respectively, and thus the size of the obtained *appimg* is $128 \times 128$. Fig. 1 shows extracted contour and curvature-feature point images of the original image Lena and corresponding approximate image *appimg* of Lena, respectively, where curvature-feature points are extracted by the improved multi-scale corner detector based on CSS. It is easy known from Fig. 1 that the contour of *appimg* is more obvious and uniformly distributed than original image due to the strengthening of image feature, which further leads to the generation of significant and well-distributed feature points with better image representativeness and higher resisting ability to cropping attacks. Moreover, *appimg* is created by deleting the high-frequency ingredient of original image, which is similar to a low-pass filtering process with noise suppression, and thus *appimg* is more robust to noise attacks than the original image.

### 3.2. Rotation angle estimation

Let the Bessel–Fourier moments of an original image and its rotated version be $B^{ori}_{nm}$, $B^{rot}_{nm}$, respectively. $\varphi^{ori}_{nm}$, $\varphi^{rot}_{nm}$ denote Bessel–Fourier moment phases of an original image and its rotated version, respectively. According to Eqs. (5) and (6), we have

$$\begin{aligned} B^{rot}_{nm} &= B^{ori}_{nm} \exp(-jm\alpha) \\ &= |B^{ori}_{nm}| \exp(j\varphi^{ori}_{nm}) \exp(-jm\alpha) \\ &= |B^{ori}_{nm}| \exp(j(\varphi^{ori}_{nm} - m\alpha)) \\ &= |B^{rot}_{nm}| \exp(j(\varphi^{ori}_{nm} - m\alpha)) \end{aligned} \tag{9}$$

Combining $B^{rot}_{nm} = |B^{rot}_{nm}| \exp(j\varphi^{rot}_{nm})$ with Eq. (9), we can infer the following equation.

$$\varphi^{rot}_{nm} = \varphi^{ori}_{nm} - m\alpha \tag{10}$$

where $\alpha \in [0, 2\pi]$ is the rotation angle. When $n = 1$, $m = 1$, $\varphi^{rot}_{11} = \varphi^{ori}_{11} - \alpha$, namely,

$$\alpha = \varphi^{ori}_{11} - \varphi^{rot}_{11} \tag{11}$$

Therefore, we can firstly solve $\varphi^{rot}_{11}$ of rotated image, then utilize $\varphi^{ori}_{11}$ as a key $k_1$ and Eq. (11) to obtain the rotation angle $\alpha$.

### 3.3. The watermarking embedding procedure

The watermarking embedding procedure is demonstrated in Fig. 2 and summarized as follows.

**Step 1**. The original image is normalized to prescribed standard size of $W \times W$, then $L$-level db1 lifting wavelet transform is executed on the normalized image according to the method developed in Section 3.1 and the approximate image *appimg* is obtained.

**Step 2**. Extract the curvature-feature points from *appimg*, then the feature regions are generated by expanding the feature points to the disk regions with the radius of $R$, here, $R$ is set to 10. Some of the disk regions overlap with others, in order to maintain the independence of feature regions, all feature regions must be non-overlapped. For overlapped feature regions, we only select a feature region whose corresponding feature point has biggest curvature, thus the reversed feature regions are non-overlapped and better embody the image characteristic.

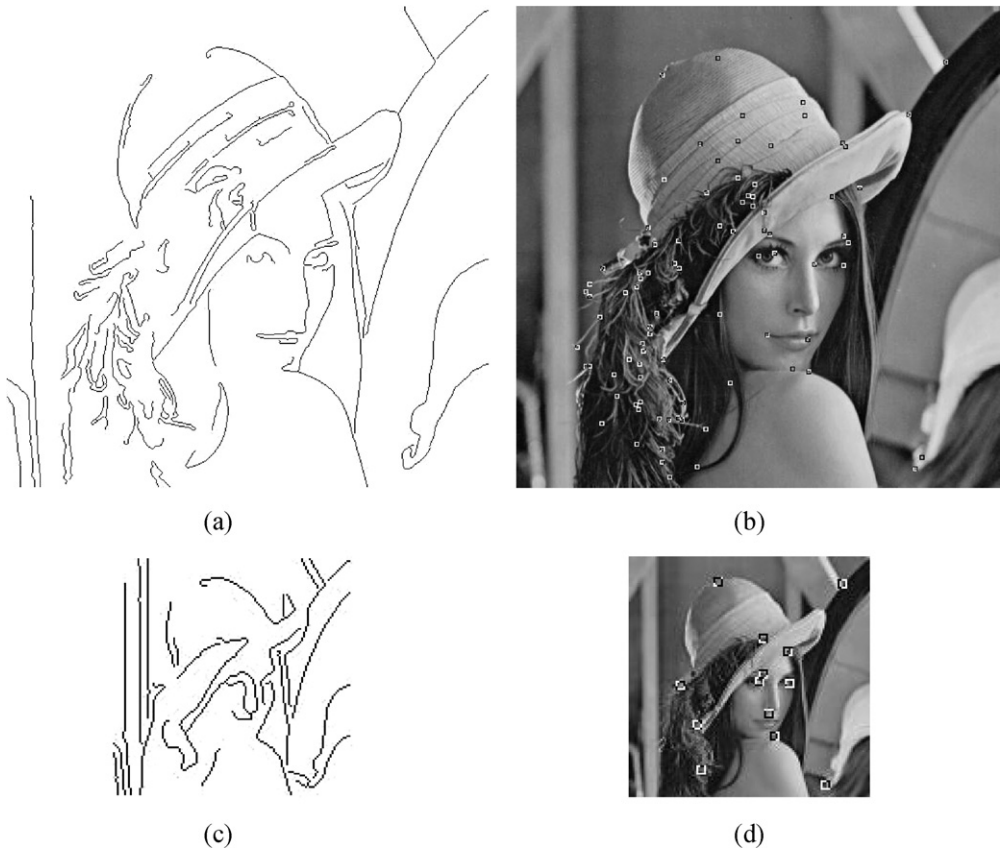


**Fig. 1.** Extracted contour and curvature-feature point images of original 512 × 512 size Lena and corresponding 128 × 128 size *appimg*. (a) Extracted contour of Lena; (b) curvature-feature point image of Lena; (c) extracted contour of *appimg*; (d) curvature-feature point image of *appimg*.

**Step 3**. The phases of Bessel–Fourier moments of every feature region are computed to construct feature vectors as follows:

$$\vec{p}_i = [p_{i1}, p_{i2}, \ldots, p_{iN}]^T = [\varphi_{i01}, \varphi_{i02}, \varphi_{i11}, \ldots, \varphi_{i0n\max}, \ldots, \varphi_{i(n\max-1)1}]^T \quad (12)$$

where $i \in [1, Q]$, $Q$ is the feature region number, $\vec{p}_i$ is the feature vector of the $i$th feature region, $N$ is the dimension of feature vector, *nmax* denotes the maximum order of Bessel–Fourier moment, which is set to 5 in our experiment. Here, the Bessel–Fourier moment phases $\varphi_{inm}$ with $m = 0$ are not included, since they are always equivalent to 0 or $\pi$ and provide no information regarding the image feature, thus $N = 15$. Moreover, we do not adopt the Bessel–Fourier moment magnitudes to construct feature vector, because the magnitude components have less discriminative ability for image feature than the phase components, which is analyzed in detail in Section 4.4.1.

**Step 4**. All feature vector components are normalized according to the following formula.

$$\varphi_{norm\_inm} = \frac{\varphi_{inm} - k_2}{k_3 - k_2} \quad (13)$$

where $\varphi_{inm}$, $\varphi_{norm\_inm}$ denote initial and normalized feature vector components of the $i$th feature region, respectively, and $\varphi_{norm\_inm} \in [0, 1]$. $k_2$ and $k_3$, as keys, are the minimum and maximum in all of $\varphi_{inm}$, respectively. The normalized feature vectors are marked as $\vec{p}_{norm\_i}$.

**Step 5**. Calculate the phases of Bessel–Fourier moments of a binary logo image up to *nmax*th order, then similar to step 4, the normalized feature vector is obtained, which is denoted as $\vec{q}_{norm}$ with same dimension $N$ as $\vec{p}_{norm\_i}$. The combination of $Q$ copies of $\vec{q}_{norm}$ is marked as $\vec{q}_{norm\_i}$, $i \in [1, Q]$.

**Step 6**. $\vec{p}_{norm\_i}$ and $\vec{q}_{norm\_i}$, as the input and output of ELM, respectively, are utilized to train ELM model, here, the number of hidden

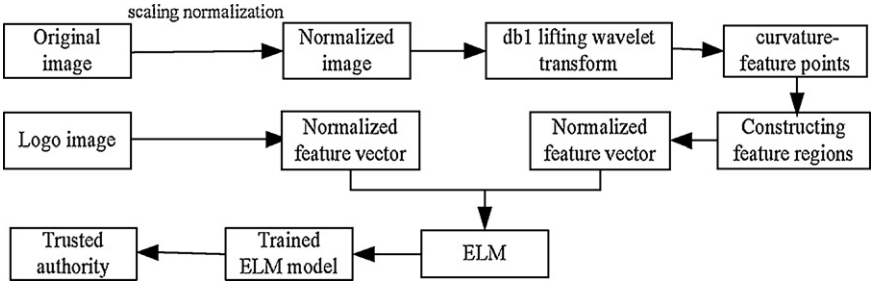


**Fig. 2.** The block diagram of watermarking embedding procedure.

**Table 1**
Keys of five kinds of test images.

| Test images | $k_1$ | $k_2$ | $k_3$ |
|---|---|---|---|
| Lena | 0.8705 | 3.1281 | −3.0400 |
| Cartoon image | 1.3002 | 3.1240 | −3.1309 |
| Medical image | 2.6899 | 3.1123 | −3.1305 |
| Remote-sensing image | 1.2529 | 3.1197 | −3.1375 |
| Artistic image | 1.8997 | 3.1271 | −3.0844 |

neurons of ELM is set to 20, and sine function is used as the activation function of ELM.

**Step 7**. The signer sends the trained ELM model *elmmod* and extra information $\{k_1||k_2||k_3||\mathrm{ID}_{\mathrm{signer}}||t\}$ to Trusted Authority (TA) through a secure channel, where $k_1$ is original image phase $\varphi_{11}^{ori}$, $k_2, k_3$ denote the minimum and maximum of original image phase $\varphi_{nm}$, respectively, $\mathrm{ID}_{\mathrm{signer}}$ represents the identity of signer, and $t$ is timestamp. After TA receives the message, a digest of the message is made as a certificate, which is defined as

$$h_{TA} = H_{TA}(k_1||k_2||k_3||\mathrm{ID}_{\mathrm{signer}}||t) \tag{14}$$

where $H_{TA}(\cdot)$ stands for a kind of one-way hash function.

It is noted that the keys $k_1$, $k_2$, $k_3$ of different images are not same, for example, the keys of five kinds of test images listed in Fig. 4 are diverse, which are shown in Table 1.

### 3.4. The watermarking verification procedure

The watermarking verification procedure is demonstrated in Fig. 3 and summarized as follows.

**Step 1**. Gain $h_{TA}$, $t$, $H_{TA}(\cdot)$ from TA and calculate a new message digest $h'_{TA} = H_{TA}(k_1||k_2||k_3||\mathrm{ID}_{\mathrm{signer}}||t)$, then compare the $h'_{TA}$ with $h_{TA}$ to confirm the integrity and validity of the information $\{k_1||k_2||k_3||\mathrm{ID}_{\mathrm{signer}}||t\}$. If $h_{TA}$ and $h'_{TA}$ are not equal, the verification procedure is terminated in this step, otherwise, we set the rotation flag $rot\_flag = 0$ and the verification procedure is continued.

**Step 2**. Similar to the watermarking generation procedure, the test image is normalized to prescribed standard size of $W \times W$, then $L$-level db1 lifting wavelet transform is executed on the normalized image and the approximate image $appimg'$ is obtained.

**Step 3**. Extract the curvature-feature points from $appimg'$ and construct $Q'$ non-overlapped feature regions. Then phases of Bessel–Fourier moments of every feature region are computed with key $k_2$, $k_3$ to form normalized feature vectors $\vec{p}'_{norm\_i}$, which are input into the trained ELM model *elmmod* from TA to obtain the output vectors $\vec{O}'_i$ with $N$ dimensions, here $i \in [1, Q']$.

**Step 4**. Calculate the normalized feature vector $\vec{q}'_{norm}$ of the logo image from TA, and the dimension of $\vec{q}'_{norm}$ is $N$. The combination of $Q'$ copies of $\vec{q}'_{norm}$ is marked as $\vec{q}'_{norm\_i}$.

**Step 5**. The detection distances $d_i$ are defined by Eq. (15) for measuring the difference between $\vec{q}'_{norm\_i}$ and $\vec{O}'_i$, if $d_i \le \lambda$, we consider a watermarking is correctly detected from a feature region of the test image, where $\lambda$ is a detection threshold set to 0.005. Let $\eta$ express the number of correctly detected watermarkings, considering the false-alarm probability, we deem that the test image is under the protection of watermarking when $\eta \ge 2$. If $\eta < 2$ and $rot\_flag == 1$, the test image is regarded as no watermarking. If $\eta < 2$ and $rot\_flag == 0$, the test image is inversely rotated in terms of the estimation angle which is generated according to the method proposed by Section 3.2 with key $k_1$, then we set $rot\_flag = 1$ and skip to step 2 to execute iteratively.

$$d_i = \frac{1}{N}\sum_{j=1}^{N}|\vec{O}'_{i,j} - \vec{q}'_{norm\_i,j}| \tag{15}$$

**Table 2**
Test for true images under free-attack and false images.

| Test images | False images | | | | |
|---|---|---|---|---|---|
| | Lena | Cartoon image | Medical image | Remote-sensing image | Artistic image |
| Lena | 8 | 1 | 1 | 0 | 0 |
| Cartoon image | 0 | 16 | 0 | 0 | 0 |
| Medical image | 0 | 0 | 8 | 0 | 0 |
| Remote-sensing image | 0 | 0 | 1 | 13 | 0 |
| Artistic image | 0 | 0 | 0 | 0 | 9 |

## 4. Simulation and performance analysis

For verifying the validity of proposed scheme, all types of gray images with size of $512 \times 512$ are selected as cover images in our experiments. These images are standard common image Lena, cartoon image, medical image, remote-sensing image and artistic image, respectively (see Fig. 4a–e), and the corresponding numbers of feature regions are 8, 16, 8, 13 and 9, respectively. A binary image (see Fig. 4f) with the size of $64 \times 64$ is used as the logo image. The robustness tests under various attacks are implemented by Stirmark.

### 4.1. Test for true images under free-attack and false images

Table 2 shows the correctly detected feature numbers for true images under free-attack and false images. For instance, the correctly detected feature number is 8 for true medical image under free-attack, and for corresponding false images, such as Lena, cartoon image, remote-sensing image and artistic image, the correctly detected feature numbers are 0, 0, 0 and 0, respectively. It is easy to know from Table 2 that all feature-regions of true images can be detected under free-attack and the forgeries prove no copyrights.

### 4.2. Robustness test under various attacks

In our experiments, the adopted attack methods include common signal processing, geometrical attacks and combining attacks. Figs. 5 and 6 show the attacked images of Lean and corresponding extracted feature regions, and the local feature regions marked by "*white point*" denote that they are detected exactly. Tables 3 and 4 list the test results of all detected images under various attacks. It is clear that the proposed scheme is robust to various attacks.

### 4.3. Comparison with other schemes

Table 5 displays the robustness to kinds of attacks of proposed method compared with that of other existing methods including Chen et al.'s (2005), Sang et al.'s (2006), Chang and Lin's (2008), Tsai

**Table 3**
The test results of all detected images under common signal processings.

| Attack methods | Test images | | | | |
|---|---|---|---|---|---|
| | Lena | Cartoon image | Medical image | Remote-sensing image | Artistic image |
| JPEG 50 | 7 | 6 | 4 | 5 | 5 |
| Median filter ($3 \times 3$) | 7 | 10 | 4 | 3 | 5 |
| Mosaic ($2 \times 2$) | 6 | 11 | 3 | 6 | 7 |
| Average filter ($3 \times 3$) | 5 | 4 | 5 | 3 | 5 |
| Gaussian noise (0.001) | 5 | 15 | 4 | 3 | 3 |
| Gaussian noise (0.005) | 3 | 11 | 3 | 2 | 3 |
| Salt-pepper noise (0.008) | 3 | 7 | 4 | 3 | 3 |
| Average filter + JPEG 70 | 8 | 3 | 6 | 2 | 3 |
| Mosaic + median filter | 5 | 8 | 5 | 2 | 3 |

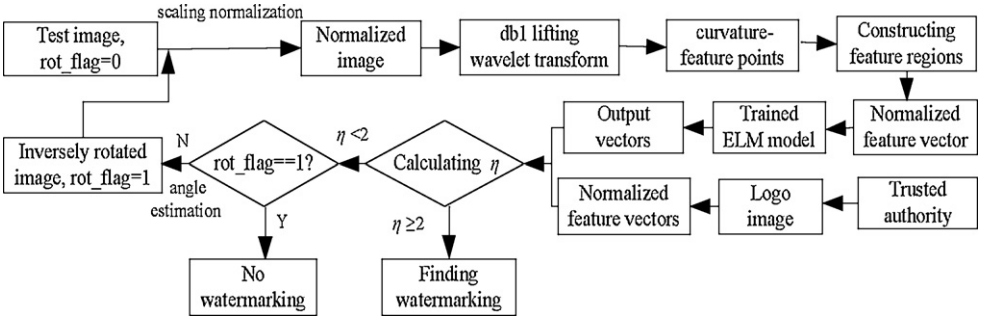


**Fig. 3.** The block diagram of watermarking verification procedure.

**Table 4**
The test results of all detected images under geometrical attacks.

| Attack methods | Test images | | | | |
|---|---|---|---|---|---|
| | Lena | Cartoon image | Medical image | Remote-sensing image | Artistic image |
| Top-left cropping (1/4) | 3 | 11 | 5 | 6 | 3 |
| Center cropping (1/4) | 3 | 7 | 2 | 5 | 3 |
| Surround cropping (1/4) | 5 | 7 | 8 | 2 | 6 |
| Rotation 5° | 7 | 7 | 6 | 2 | 4 |
| Rotation 240° | 6 | 5 | 5 | 5 | 4 |
| Scaling (1.2, 1.5) | 5 | 7 | 4 | 6 | 3 |
| Translation (20, 20) | 6 | 12 | 8 | 4 | 9 |
| Stirmark RBA(0.1) | 5 | 5 | 3 | 2 | 3 |
| Rotation 2° + JPEG 70 | 5 | 4 | 3 | 4 | 5 |
| Translation (20, 0) + top-left cropping (1/4) | 5 | 8 | 5 | 3 | 3 |

et al.'s (2010) and Rawat and Raman's methods (2012). Because the detection criterions of zero-watermarking of all compared schemes are diverse, thus we only offer qualitative comparison. From Table 5, it is concluded that the proposed scheme outperforms other five methods, especially on resisting cropping attacks, big angle rotation and RBA attacks, which mainly profits from the adopting of multiple zero-watermarking, rotation estimation and ELM model. Then Table 6 gives the contrast results of image types for test among Chen et al.'s (2005), Sang et al.'s (2006), Chang and Lin's (2008), Tsai et al.'s (2010), Rawat and Raman's (2012) and the proposed methods. Moreover, some test results and analysis for false images are shown in Sections 4.1, 4.4.1 and 4.4.2, respectively, however, similar test and analysis are not provided by Chen et al.'s (2005), Sang et al.'s (2006), Chang and Lin's (2008), Tsai et al.'s (2010) and Rawat and Raman's methods (2012).

**Table 5**
The robustness to kinds of attacks of proposed method in comparison with other existing methods.

| Attack methods | Robustness | | | | | |
|---|---|---|---|---|---|---|
| | Chen | Sang | Chang | Tsai | Rawat | Proposed method |
| Median filter (3 × 3) | Yes | Yes | Yes | Yes | Yes | Yes |
| JPEG compression | Yes | Yes | Yes | Yes | Yes | Yes |
| Gaussian noise (0.005) | Yes | No | Yes | Yes | Yes | Yes |
| Average filter (3 × 3) | Yes | Yes | Yes | Yes | Yes | Yes |
| Small angle rotation | Yes | Yes | Yes | No | Yes | Yes |
| Big angle rotation | No | No | No | No | No | Yes |
| Scaling | Yes | Yes | Yes | Yes | Yes | Yes |
| Translation | Yes | Yes | Yes | Yes | No | Yes |
| Stirmark RBA | Yes | No | Yes | No | No | Yes |
| Top-left cropping (1/8) | Yes | Yes | Yes | Yes | No | Yes |
| Center cropping (1/4) | Yes | No | Yes | No | No | Yes |
| Surround cropping (1/4) | Yes | No | Yes | Yes | No | Yes |

### 4.4. Analysis of performance evaluation

#### 4.4.1. Effects of phase and magnitude components on the algorithm performance

Considering the effects of Bessel–Fourier moment magnitudes and phases used to construct feature vector on the algorithm performance, we analyze the discriminative abilities of magnitude and phase components for the feature regions of image. Firstly, normalized magnitudes and normalized phases of Bessel–Fourier moments of two arbitrarily extracted feature regions from Lean image are calculated, which are used to construct the feature vectors shown in Figs. 7 and 8. Then we arbitrarily select one feature region respectively from Lean image and from cartoon image, Figs. 9 and 10 show the feature vectors composed by normalized magnitudes or normalized phases of the two selected feature regions, respectively. From Figs. 7–10, it is known that normalized magnitudes of two different regions are close, however, the differences of normalized phases of two different regions are obvious. Next, we utilize an objective criterion to evaluate the differences of normalized magnitudes or phases of two different regions as follows.

$$magdiff = \frac{1}{N}\sum_{i=1}^{N}|mag_i - mag_i'| \tag{16}$$

$$phadiff = \frac{1}{N}\sum_{i=1}^{N}|pha_i - pha_i'| \tag{17}$$

where $mag_i$, $mag_i'$ are normalized magnitudes of two different regions, respectively, $magdiff$ is the average distance between $mag_i$ and $mag_i'$. $pha_i$, $pha_i'$ are normalized phases of two different regions, respectively, $phadiff$ is the average distance between $pha_i$ and $pha_i'$. The $magdiff$, $phadiff$ corresponding to Fig. 7, Fig. 8 are 0.1176 and 0.4267, respectively. The $magdiff$, $phadiff$ corresponding to Fig. 9, Fig. 10 are 0.1320 and 0.3530, respectively.

**Table 6**
The image types tested by proposed method in comparison with other existing methods.

| Image types | Chen | Sang | Chang | Tsai | Rawat | Proposed method |
|---|---|---|---|---|---|---|
| Common image | Tested | Tested | Tested | Tested | Tested | Tested |
| Cartoon image | No | No | No | No | No | Tested |
| Medical image | No | No | Tested | No | No | Tested |
| Remote-sensing image | No | No | No | No | No | Tested |
| Artistic image | No | No | No | No | No | Tested |

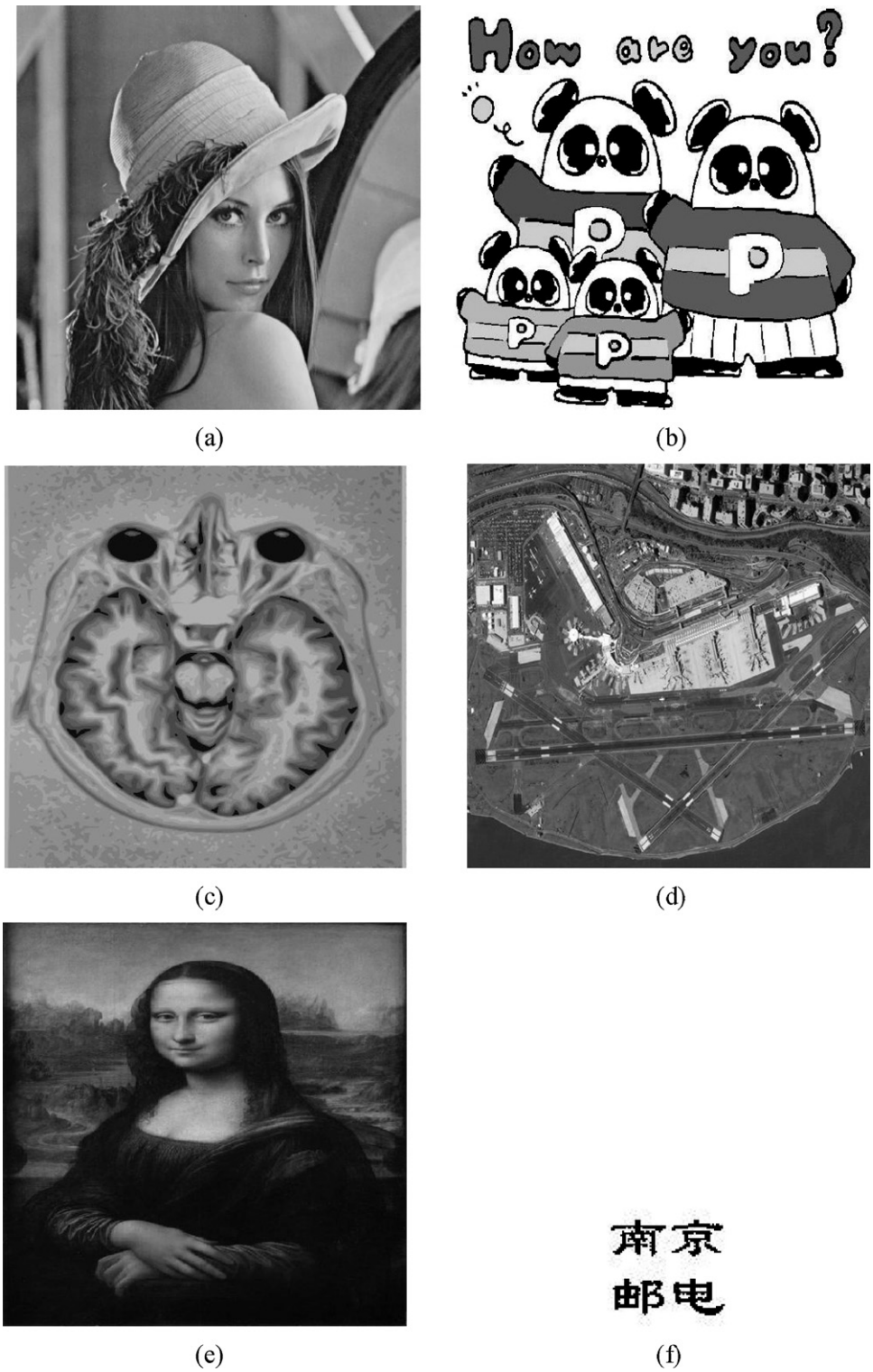


**Fig. 4.** All types of gray images used for test and a binary logo image. (a) Lena; (b) cartoon image; (c) medical image; (d) remote-sensing image; (e) artistic image; (f) logo image.

Consequently, the phase components have a better discrimination ability and can better represent the image feature than the magnitude components, meanwhile, it is easily inferred that compared with the magnitude components the phase components have less false probability for copyright authentication of an image using the proposed algorithm. Thus the phase components adopted to form the feature vector in the presented scheme have better performance than the magnitude components.

*4.4.2. Effect of feature vector dimension on the algorithm performance*

Fig. 11 describes the test results of common Lena image under various attacks where the feature vector utilizes Bessel–Fourier moments of order $N$ up to 3, 5 and 7, respectively, and the corresponding feature dimensions are 6, 15 and 28, respectively. The homologous attack modes with indices of horizontal ordinate are JPEG 50, median filter ($3 \times 3$), mosaic ($2 \times 2$), average filter ($3 \times 3$),


**Fig. 5.** The attacked images of Lean and corresponding extracted feature regions under common signal processings. (a) JPEG 50; (b) median filter ($3 \times 3$); (c) mosaic ($2 \times 2$); (d) average filter ($3 \times 3$); (e) salt-pepper noise (0.008); (f) Gaussian noise (0.005); (g) average filter + JPEG 70; (h) mosaic + median filter.

Gaussian noise (0.001), Gaussian noise (0.005), salt-pepper noise (0.008), top-left cropping (1/4), center cropping (1/4), surround cropping (1/4), rotation 5°, rotation 240°, scaling (1.2, 1.5), translation (20, 20) and Stirmark RBA(0.1), respectively. Fig. 12 shows the test results of Lena image for false images with different orders of Bessel–Fourier moments, and the indices of horizontal ordinate correspond to cartoon image, medical image, remote-sensing image and artistic image, respectively.

It can be concluded that the robustness to attacks gets worse along with the increasing of feature dimension in Fig. 11, meanwhile, the corresponding detection ability for false images becomes better in Fig. 12. This is because that the high-dimensional feature vector with a high order of Bessel–Fourier moments owns generally a better representation power to distinguish the different images at the cost of time and memory space, which leads to a high sensitivity to the tiny difference between original image and attacked

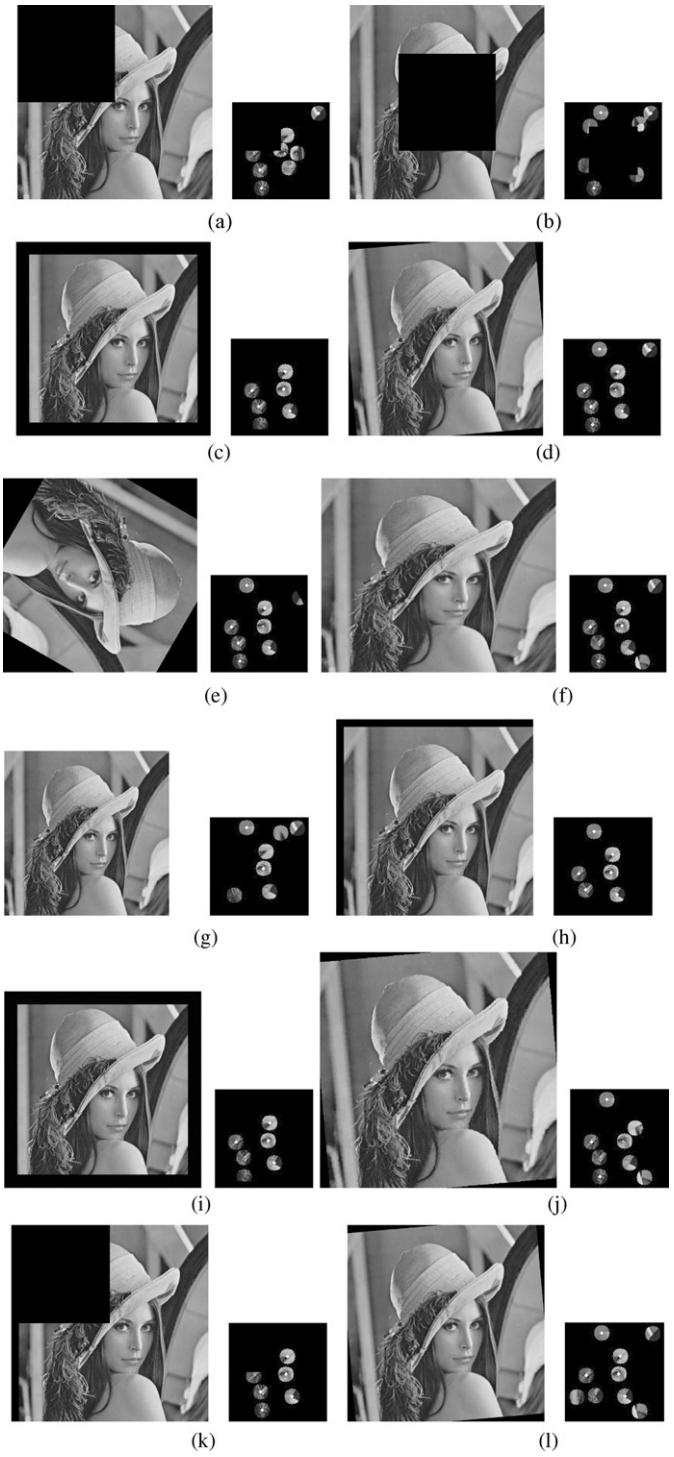


**Fig. 6.** The attacked images of Lean and corresponding extracted feature regions under geometrical attacks. (a) Top-left cropping (1/4); (b) center cropping (1/4); (c) surround cropping (1/4); (d) rotation 5°; (e) rotation 240°; (f) scaling (1.2, 1.5); (g) scaling 0.5; (h) translation (20, 20); (i) surround cropping (1/4) + JPEG 70; (j) rotation 5° + scaling 1.2; (k) translation(20, 0) + top-left cropping (1/4); (l) rotation 2° + JPEG 70.

image and a strong discernment to false images. The selection of order $N = 5$ with the feature dimension of 15 is a tradeoff between robustness to attacks and ability against false images.

### 4.4.3. Optimization for ELM

The proposed scheme employs the strong generalization ability of ELM to enhance the robustness to various malicious attacks.

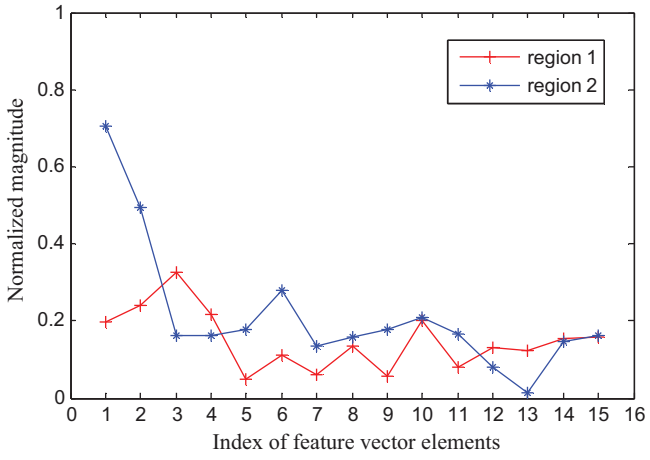


**Fig. 7.** Feature vectors composed by normalized magnitudes of arbitrary two extracted feature regions from Lean image.

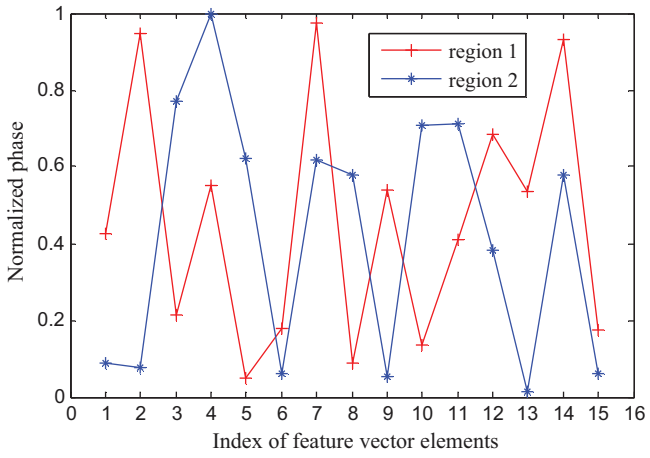


**Fig. 8.** Feature vectors composed by normalized phases of arbitrary two extracted feature regions from Lean image.

Furthermore, by optimizing ELM, we can improve further the performance of proposed scheme. Currently, the main optimization methods of ELM include evolutionary extreme learning machine (E-ELM) (Zhu et al., 2005) and optimally pruned extreme learning

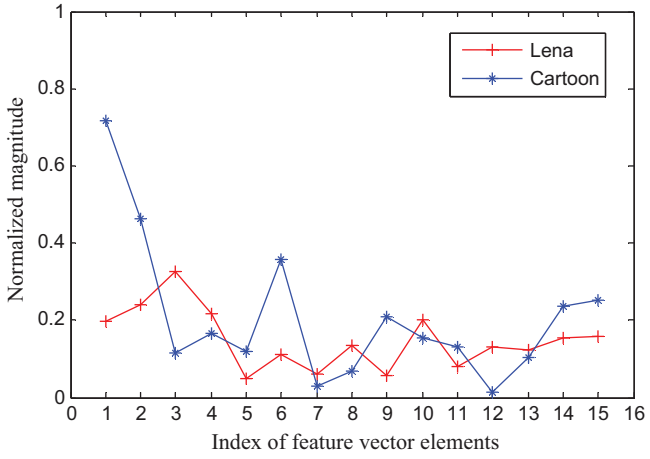


**Fig. 9.** Feature vectors composed by normalized magnitudes of two arbitrary feature regions respectively from Lean and from cartoon image.

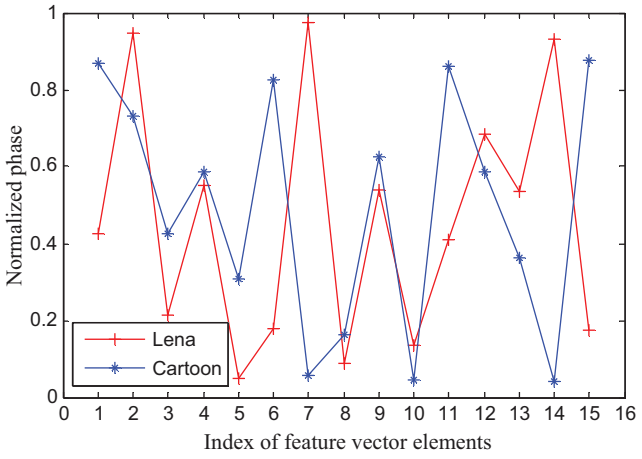


**Fig. 10.** Feature vectors composed by normalized phases of two arbitrary feature regions respectively from Lean and from cartoon image.

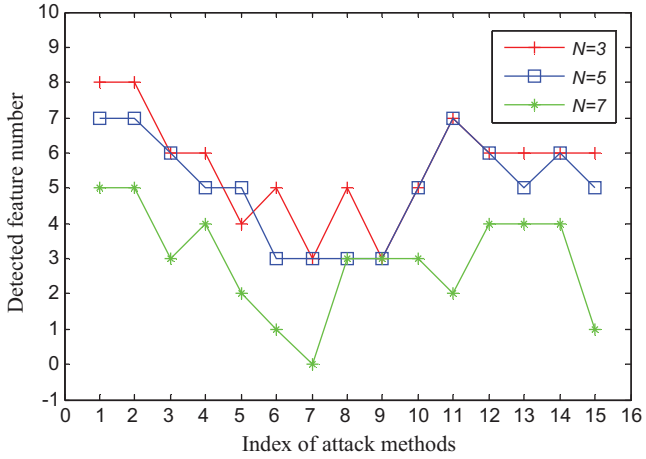


**Fig. 11.** The test results of Lena under various attacks with order $N$ up to 3, 5 and 7.

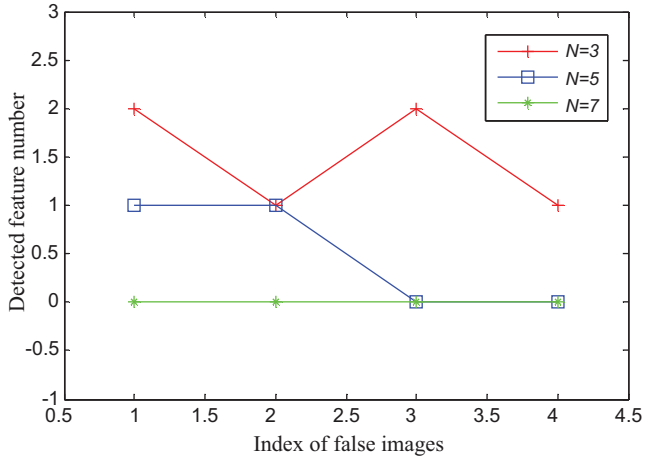


**Fig. 12.** The test results of Lena for false images with order $N$ up to 3, 5 and 7.

machine (OP-ELM) (Miche et al., 2010), which will be applied to our scheme in future research.

## 5. Conclusion

A drawback of current zero-watermarking methods is weak robustness to high ratio cropping and large angle rotation attacks. To solve this problem, this paper presents a multiple zero-watermarking scheme, which obtains a better performance than other five existing algorithms due to the superiorities of improved CSS corner detector, Bessel–Fourier moment and ELM. A method for image feature enhancement and a simple rotation estimation algorithm are provided in proposed scheme. Moreover, the tests and analyses for false alarm and five types of images, seldom mentioned in other literatures for lossless authentication, are presented in this paper. Finally, the effects of phase and magnitude components and feature vector dimension on the algorithm performance are discussed, and it is pointed out that the performance of proposed scheme can be improved further by the optimization of ELM.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 60874091), the Six Projects Sponsoring Talent Summits of Jiangsu Province, China (Grant No. SJ209006), the Research Fund for the Doctoral Program of Higher Education of China (20103223110003), the Natural Science Foundation of Jiangsu Province, China (Grant No. BK2010526), the Project for Introduced Talent in Nanjing University of Posts and Telecommunications, China (Grant No. NY209021), the Natural Science Foundation of Educational Commission of Jiangxi Province, China (Grant No. GJJ12614) and the Scientific Research Innovation Program for the Graduat Students in Jiangsu Province, China (Grant No. CXZZ11_0400).

## References

Akhaee, M.A., Sahraeian, S., Marvasti, F., 2010. Contourlet-based image watermarking using optimum detector in a noisy environment. IEEE Transactions on Image Processing 19 (4), 967–980.
Amos, D.E., 1986. A portable package for Bessel functions of a complex argument and nonnegative order. ACM Transactions on Mathematical Software 12 (3), 265–273.
Chang, C.C., Lin, P.Y., 2008. Adaptive watermark mechanism for rightful ownership protection. Journal of System and Software 81, 1118–1129.
Chen, T., Horng, G., Leew, B., 2005. A publicly verifiable copyright proving scheme resistant to malicious attacks. IEEE Transactions on Industrial Electronics 52 (1), 327–334.
Cui, L.H., Li, W.G., 2011. Adaptive multiwavelet-based watermarking through JPW masking. IEEE Transactions on Image Processing 20 (4), 1047–1060.
Furon, T., 2007. A constructive and unifying framework for zero-bit watermarking. IEEE Transactions on Information Forensics and Security 2 (2), 149–163.
Gao, G.Y., Jiang, G.P., 2010. Grayscale watermarking resistant to geometric attacks based on lifting wavelet transform and neural network. In: Proceedings of the 8th World Congress on Intelligent Control and Automation, Jinan, China, pp. 1305–1310.
He, X.C., Yung, N.H.C., 2008. Corner detector based on global and local curvature properties. Optical Engineering 47 (5), 057008-1–057008-12.
Huang, G.B., Zhu, Q.Y., Siew, C.K., 2004. Extreme learning machine: a new learning scheme of feedforward neural networks. In: Proceedings of the International Joint Conference on Neural Networks, Budapest, Hungary, pp. 25–29.
Huang, G.B., Zhu, Q.Y., Siew, C.K., 2006. Extreme learning machine: theory and applications. Neurocomputing 70, 489–501.
Lou, D.C., Shieh, J.M., Tso, H.K., 2006. A robust buyer-seller watermarking scheme based on DWT. International Journal of Pattern Recognition and Artificial Intelligence 20 (1), 79–90.
Miche, Y., Sorjamaa, A., Bas, P., 2010. OP-ELM: optimally pruned extreme learning machine. IEEE Transactions on Neural Networks 21 (1), 158–162.
Mohanty, S.P., Bhargava, B.K., 2008. Invisible watermarking based on creation and robust insertion-extraction of image adaptive watermarks. ACM Transactions on Multimedia Computing, Communications, and Applications 5 (2), 12:1–12:22.
Mohanty, S.P., Guturu, P., Kougianos, E., Pati, N., 2006. A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion–extraction. In: Proceedings of the IEEE International Symposium on Multimedia, pp. 153–160.
Mokhtarian, F., Mackworth, A.K., 1992. A theory of multi-scale curvature-based shape representation for planar curves. IEEE Transactions on Pattern Analysis and Machine Intelligence 14 (8), 789–805.
Rawat, S., Raman, B., 2012. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. Signal Processing 92, 1480–1491.
Sang, J., Liao, X., Alam, M.S., 2006. Neural-network-based zerowatermark scheme for digital images. Optical Engineering 45 (9), 097006-1–097006-9.

Tsai, H.H., Tseng, H.C., Lai, Y.S., 2010. Robust lossless image watermarking based on α-trimmed mean algorithm and support vector machine. Journal of System and Software 83 (1), 1015–1028.
Wen, Q., Sun, T., Wang, S., 2003. Concept and application of zero-watermark. Acta Electronic Sinica 31 (2), 214–216 (in Chinese).
Xiao, B., Ma, J.F., Wang, X., 2010. Image analysis by Bessel–Fourier moments. Pattern Recognition 43, 2620–2629.
Zhu, Q.Y., Qin, A.K., Suganthan, P.N., Huang, G.B., 2005. Evolutionary extreme learning machine. Pattern Recognition 38, 1759–1763.

**Guangyong Gao** is Associate Professor, Ph.D., and is working in School of Information Science & Technology, Jiujiang University, China. His research interests include Digital Watermarking, Image Processing and Information Security.

**Guoping Jiang** received the B.E. degree in electrical engineering from Hohai University, Nanjing, China, in 1988 and the Ph.D. degree in control theory and engineering from Southeast University, Nanjing, in 1997.

From 1988 to 1992, he was an Assistant Teacher with the Department of Electrical Engineering, Hohai University, Nanjing. From March 1997 to July 2005, he was with the Department of Electronic Engineering, Nanjing University of Posts and Telecommunications, Nanjing, first as a Lecturer and then as an Associate Professor and a Professor. From June to September 2001, January to April 2002, and July to August 2005, he was with the Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong, first as a Research Assistant and then as a Research Fellow. From August to December 2003, he was with the School of Quantitative Methods and Mathematical Sciences (QMMS), University of Western Sydney, Sydney, Australia, as a Visiting Fellow. He is the Founding Director of the Center for Control and Intelligence Technology, Nanjing University of Posts and Telecommunications, where he has also been a Professor and the Dean of the College of Automation since August 2005. He has authored or coauthored more than 100 published articles in the area of system and control. His current research interests include chaos synchronization and control, chaos-based communication, and complex dynamical networks.