文章编号：2095-4980(2022)07-0722-10

基于Tchebichef矩与颜色矢量角度的鲁棒图像哈希算法

王　瑶[1]，陈文宇[2]

(1.重庆城市职业学院 信息与智能工程学院，重庆 402160；2.电子科技大学 计算机科学与工程学院，四川 成都 611731)

摘　要：为了改善哈希算法对旋转等内容修改的鲁棒性，设计了径向Tchebichef矩耦合颜色矢量角度的鲁棒图像哈希算法。引入2D离散小波变换(DWT)，对图像的颜色矢量角度实施分解，获取对应的4个子带，将其低频系数作为结构特征。采用径向Tchebichef矩计算预处理图像的Tchebichef矩，提取全局特征。通过组合这2种特征，以形成中间哈希序列。设计加密函数，对中间哈希完成加密，得到目标哈希序列。计算初始目标与待识别图像的哈希序列之间的l_2范数距离，并将其与预设阈值作比较，完成图像内容的真伪判别。测试数据表明：相对于已有的哈希算法而言，所提算法具备更高的鲁棒性，可以对旋转、颜色与缩放等内容修改做出准确识别。

关键词：图像哈希；径向Tchebichef矩；颜色矢量角度；全变分；离散小波变换；非线性复合混沌系统；范数距离

中图分类号：TP391　　**文献标志码：**A　　**doi：**10.11805/TKYDA2020291

Robust image Hashing algorithm based on Tchebichef moments and Color Vector Angle

WANG Yao[1]，CHEN Wenyu[2]

(1.School of Information and Intelligent Engineering，Chongqing City Vocational College，Chognqing 402160，China；
2.School of Computer Science and Engineering，University of Electronic Science and Technology，Chengdu Sichuan 611731，China)

Abstract：In order to improve the robustness of the Hashing algorithm for the content modification such as rotation, a robust image Hashing algorithm based on radial Tchebichef moment and Color Vector Angle(CVA) is designed in this paper. The 2D Discrete Wavelet Transform(DWT) is introduced to decompose the color vector angle of image for obtaining four sub-bands, and the low frequency coefficients are taken as structural features. The Tchebichef moments of pre-processing image are calculated based on radial Tchebichef moments to extract global features. And an intermediate Hash sequence is got by combining the two features. The encryption function is designed to encrypt the intermediate Hash for obtaining the target Hash sequence. Finally, the l_2 norm distance between the initial target and the Hash sequence of the recognized image is calculated, and the authenticity discrimination of the image content is finished by comparing it with the preset threshold. The test data shows that this proposed Hashing algorithm is more robust than the existing Hashing algorithm, which can accurately identify the modifications of rotation, color and scaling.

Keywords：image Hash；radial Tchebichef moment；Color Vector Angle；total variation；discrete wavelet transform；nonlinear composite chaotic system；norm distance

图像中存在丰富的用户信息，已是目前用户实施表达与交流的重要介质，但是，图像在网络中传输时，会碰到外部的恶意攻击，导致其信息被篡改与泄露，难以对其真实性实施判别[1-2]。图像哈希作为一种对图像真实性进行认证的重要方法，被国内外人员广泛研究，其对图像内容的变化非常敏感，对常规的几何攻击具有较强的感知鲁棒性[2]。

收稿日期：2020-06-25；**修回日期：**2020-09-03

基金项目：国家重点研发计划参与课题(2018YFC0808304；201807-202106)；2019电子科技大学“双一流”学科建设研究支持计划基金资助项目(SYLYJ2019101)；重庆市教委科学技术重点研究基金资助项目(KJZD-K201903901)

哈希算法包含3个阶段：图像预处理、特征提取与哈希形成，在这三者之中，特征提取是其最为关键的过程，对哈希算法的识别能力影响较大[3−7]。近年来，学者们设计了诸多新颖的哈希算法，如王彦超等[3]借助块截断编码机制，输出二次图像的高、低电平矩和二进制位图，设计邻域空间局部二值模式(Local Binary Patterns，LBP)，得到位图的特征矩阵，通过对其实施量化，输出对应的二值序列，采用主成分分析处理特征矩阵，从而形成了紧凑哈希。但是这种邻域空间LBP算子对旋转等攻击缺乏鲁棒性，且其没有考虑图像的结构特征，导致其哈希算法的感知鲁棒性有待提升。Tang等[4]通过计算预处理图像的颜色矢量角度，并从其归一化图像内的最大内切圆里的颜色矢量角度中提取直方图，将其作为中间哈希，最后通过压缩方法，输出紧凑哈希。但是，该哈希算法无法提取图像中抗旋转特征，限制了其感知鲁棒性。Nilesh等[5]首先生成图像对应的的颜色直方图，该特征对大多数内容保持攻击是不变的，而且借助优化的调谐因子来确定合适的直方图单元，以增强哈希算法的鲁棒性，并且该算法还对模糊颜色直方图进行归一化处理。但是，该算法对旋转与亮度调整的鲁棒性不理想。为了提高对旋转操作的稳健性，陈勇昌等[6]设计了基于形状不变矩的图像感知哈希算法，首先提取预处理图像的亮度分量，再计算其径向Tchebichef矩，将该矩视为哈希特征，并对其进行量化与二值映射操作，形成中间哈希序列，最后，基于混沌置乱方法，实现哈希加密，得到最终的目标哈希。Chen等[7]提出了基于径向Tchebichef矩的图像哈希生成算法，该方法利用Tchebichef矩来表示正交核下的图像，从而使其具有良好的正交性和鲁棒性，并通过对径向Tchebichef矩的自适应量化来得到Hash值，然后在离散二进制转换阶段应用随机Gay码来增强分辨性。这2种技术虽然采用了径向Tchebichef矩，对旋转与尺度等变换具有较好的鲁棒性，但其仅利用了图像的形状特征，忽略了颜色信息，使其难以有效描述图像中的颜色特征，导致其对颜色变换的鲁棒性较低。

为了改善哈希序列对旋转、颜色等变换的鲁棒性，本文设计了径向Tchebichef矩耦合颜色矢量角度的鲁棒图像哈希算法。通过线性插值运算来规范图像的尺寸，并借助基于全变分的非线性滤波器，消除噪声的影响，有效增强哈希序列对缩放与噪声的鲁棒性。提取滤波图像的颜色矢量角度，利用DWT方法来实现分解，将其输出的低频系数作为结构特征，有效改善其对颜色变换的识别性；再计算滤波图像的Tchebichef矩，作为全局特征，将其与结构特征组合，得到中间哈希序列，增强其对任意角度旋转的鲁棒性。通过对中间哈希完成加密，获取最终的哈希序列。引入l_2范数距离，对图像内容的真伪进行判别。最后，测试了所提哈希算法的鲁棒性与认证能力。

1　所提鲁棒哈希算法

所提的鲁棒哈希生成过程见图1，其包括3个阶段：基于插值运算与非线性滤波的图像预处理；基于颜色矢量角度与Tchebichef矩的鲁棒特征提取；哈希加密与认证。

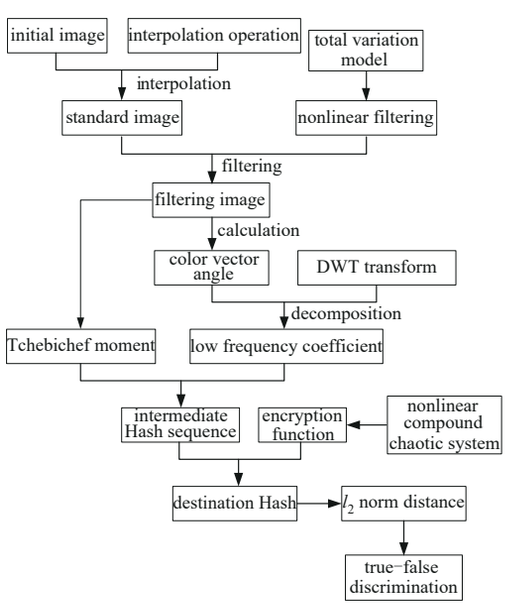


Fig.1 Process of the proposed robust Hashing algorithm
图1 所提的鲁棒哈希算法的过程

1.1 基于插值运算与非线性滤波的图像预处理

令输入图像为I，其大小为$M\times N$，借助插值运算[5]来规范其尺寸，以固定哈希序列：

$$z_X=y_0+\frac{y_1-y_0}{x_1-x_0}\left(z_Y-x_0\right) \tag{1}$$

$$z_Y=x_0+\frac{x_1-x_0}{y_1-y_0}\left(z_X-y_0\right) \tag{2}$$

式中：x_0、y_0分别是x、y维度最初状态的起始值；x_1、y_1分别是x、y维度插值前的原始值；z_X、z_Y分别是x、y维度插值后的插值结果。$x_0\leqslant z_X\leqslant x_1$；$y_0\leqslant z_Y\leqslant y_1$。

通过插值运算处理，可以将任意尺寸的图像转变成规范尺寸为$Z\times Z$的图像I_1，从而使其具备固定长度的哈希序列，增强其对尺度修改的稳健性[1]。再引入基于全变分[8]的非线性滤波器来处理I_1，避免噪声干扰。这种滤波器主要是通过最小化能量函数来实现：

$$E_\lambda(I)=\int|\nabla I|\mathrm{d}x\mathrm{d}y+\frac{\lambda}{2}\int\left|I-I_0\right|^2\mathrm{d}x\mathrm{d}y \tag{3}$$

式中：λ为约束变分问题的拉格朗日乘子[8]；I_0为输入图像。

根据文献[9]发现，与式(3)有关的最小化问题可演变为偏微分方程(Partial Differential Equation，PDE)：

$$\frac{\delta_{I_2}}{\delta t}=div\left[\frac{\nabla I_2}{|\nabla I_2|}\right]+\lambda\left(I_1-I_2\right) \tag{4}$$

式中：I_2为滤波结果；t为时间引擎；div为散度算子；∇为梯度算子。

将图2(a)所示的图像当成测试样本，根据上述过程，输出数据分别见图2(b)~2(c)。基于测试图像发现，源图像被插值后，可获取一个尺寸规范的图像；且经过滤波后，能输出一幅不含噪声干扰的图像。

(a) initial color image (b) dimension specification image (c) filtered image

Fig.2 Preprocessing results of images

图2 图像的预处理结果

1.2 基于颜色矢量角度与Tchebichef矩的鲁棒特征提取

亮度(Lightness，L)、色相(Hue，H)与饱和度(Saturation，S)是彩色图像的重要信息[10]。为了充分提取图像的颜色特征，计算其颜色矢量角度(CVA)[10-11]。就RGB(Red Green Blue)空间而言，相对于Eulidean距离，CVA更能充分反映出2种不同颜色间的视觉差异，见图3。

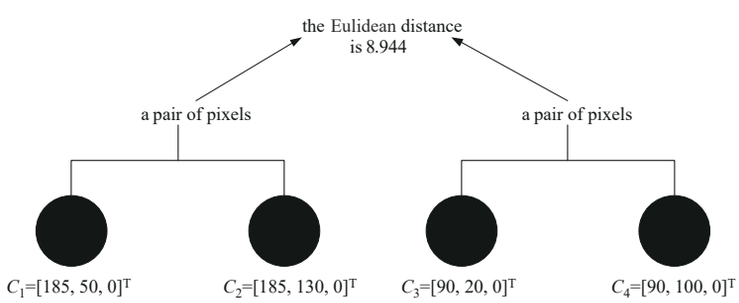


Fig.3 Eulidean distance and Color Vector Angle

图3 Eulidean距离与颜色矢量角度

令$\boldsymbol{P}_1=\left[R_1,G_1,B_1\right]^{\mathrm{T}}$,$\boldsymbol{P}_2=\left[R_2,G_2,B_2\right]^{\mathrm{T}}$是图像中的2个颜色矢量，则其颜色矢量角度$\theta$为[11]：

$$\theta=\arcsin\left(1-\frac{\left(\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{P}_2\right)^2}{\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{P}_1\boldsymbol{P}_2{}^{\mathrm{T}}\boldsymbol{P}_2}\right)^{1/2} \tag{5}$$

在所提哈希算法中，为了简化计算，用$\sin\theta$来替换θ，则式(5)变为[11]：

$$\sin\theta=\left(1-\frac{\left(\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{P}_2\right)^2}{\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{P}_1\boldsymbol{P}_2{}^{\mathrm{T}}\boldsymbol{P}_2}\right)^{1/2} \tag{6}$$

借助式(6)来计算图像中所有像素的$\sin\theta$值，通过排列组合，可得到颜色矩阵：

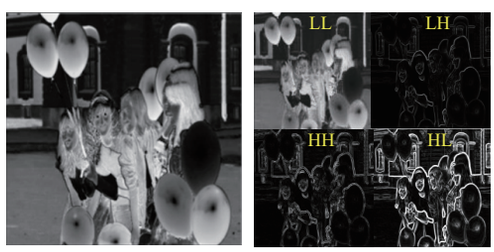
$$\boldsymbol{A}_{\text{color}}=\begin{bmatrix}\sin\theta_{1,1} & \sin\theta_{1,2}\cdots\sin\theta_{1,Z}\\ \sin\theta_{2,1} & \sin\theta_{2,2}\cdots\sin\theta_{2,Z}\\ \vdots & \vdots\ \ \vdots\ \ \vdots\\ \sin\theta_{Z,1} & \sin\theta_{Z,2}\cdots\sin\theta_{Z,Z}\end{bmatrix} \tag{7}$$

式中Z是滤波图像的高度。

随后，为了压缩哈希序列的长度，本文引入2D离散小波变换[12](DWT)来分解颜色矢量角度，输出LL,LH,HH,HL等子带信息。首先，提取LL子带中的DWT系数，并将其随机排列，组合成一个紧凑表示。显然，通过采用DWT分解方法，能够减少图像的75%的信息，从而大幅压缩哈希长度。令S是LL子带中的DWT系数的总量，则$S=\left(\lceil Z/2\rceil\right)^2$，其中$\lceil\ \rceil$是向下取整运算，则形成紧凑表示$\boldsymbol{e}=\left[e(1),e(2),\cdots,e(S)\right]$。

以图2(c)为对象，通过上述过程，形成的颜色矢量角度见图4(a)。再借助DWT方法对其分解后，形成4个子带，见图4(b)。由图4(b)发现，左上角的LL子带包含了图4(a)的主要信息，可提供近似描述。

然而，提取颜色矢量角度对旋转攻击缺乏鲁棒性。因此，本文引入径向Tchebichef矩[13]，以充分提取图像中的抗旋转特征。对于尺寸为$Z\times Z$的图像$I_2(x,y)$，本文根据文献[14]提供的映射方法，将方形图像平面映射到圆形的内部，以计算图像矩的不变性，其坐标转换函数为：



(a) color vector angle　　(b) DWT decomposition

Fig.4 Angle of color vector and its decomposition
图4 颜色矢量角度及其分解

$$r_{ij}=\frac{Z\sqrt{\left[2/(Z-1)i-1\right]^2+\left[2/(Z-1)j-1\right]^2}}{2} \tag{8}$$

$$\theta_{ij}=\arctan\left(\frac{(2/Z-1)j-1}{(2/Z-1)i-1}\right) \tag{9}$$

式中：r_{ij}是圆形半径；θ_{ij}为旋转角度。

根据式(8)和式(9)，将图像$I_2(x,y)$转换为$f(r,\theta)$，此时的一致性采样过程见图5。图中的$N=Z/2$和M分别是沿着图5所示的圆周上的最大像素数量。则计算阶数为n、重复次数为m的径向Tchebichef矩为[13-14]：

$$S_{mn}=\frac{1}{M}\sum_{r=0}^{N-1}\sum_{k=1}^{M-1}\tilde{t}_n(r)\exp\left(-\mathrm{j}m\frac{2\pi\theta_k}{M}\right)f\left(r,\theta_k\right) \tag{10}$$

式中：$\tilde{t}_n$为径向Tchebichef多项式[14]；$\theta_k=2\pi k/M$是第k个圆对应的旋转角度。

在本文哈希算法中，通过反复实验，取最大阶数n=5，最大重复次数m=5，那么对于$Z\times Z$的图像$I_2(x,y)$而言，可以获取36个径向Tchebichef矩不变量，记为$\boldsymbol{F}=\left[\left|S_{01}\right|,\left|S_{02}\right|,\left|S_{03}\right|,\cdots,\left|S_{55}\right|\right]$。然后将$\boldsymbol{e}=\left[e(1),e(2),\cdots,e(S)\right]$与$\boldsymbol{F}=\left[\left|S_{01}\right|,\left|S_{02}\right|,\left|S_{03}\right|,\cdots,\left|S_{55}\right|\right]$实施组合，形成中间哈希序列$\boldsymbol{Z}=\left[z(1),e(2),\cdots z(S),\left|S_{01}\right|,\cdots,\left|S_{55}\right|\right]$。

1.3 哈希加密与认证

为了改善所提哈希算法的防碰撞性，引入非线性复合混沌系统[15]，设计哈希元素加密方法，对$\boldsymbol{Z}=\left[z(1),e(2)\cdots z(S),z(S+1),\cdots,z(S+36)\right]$实施加密。非线性复合混沌系统的函数为[15]：

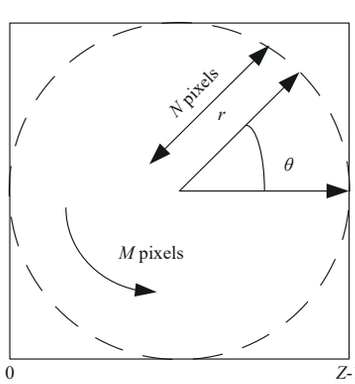


Fig.5 Uniform sampling processes of radial Tchebichef moments
图5 径向Tchebichef矩的一致采样过程

$$\begin{cases}x_{i+1}=\sin\left(\pi\mu\left(y_i+3\right)x_i\left(1-x_i\right)\right)\\ y_{i+1}=\sin\left(\pi\mu\left(x_{i+i}+3\right)y_i\left(1-y_i\right)\right)\end{cases} \tag{11}$$

通过设置该系统的初始条件u,x_0与y_0，对式(11)完成迭代$(S+36)$次，得到2个随机数组：

$$\begin{cases}X'_1=\left\{x'_{11},x'_{12},x'_{13}\cdots x'_{1(S+36)}\right\}\\ Y'_1=\left\{y'_{11},y'_{12},y'_{13}\cdots y'_{1(S+36)}\right\}\end{cases} \tag{12}$$

由于混沌系统在迭代过程存在周期性[16]，因此，本文定义了非线性运算，用来消除式(12)的周期性：

$$\begin{cases} x''_{1i}=\left\lfloor abs\left(x'_{1i}\right)-\left\lfloor x'_{1i}\right\rfloor\times 10^{14}\right\rfloor \bmod 2^{10} \\ y''_{1i}=\left\lfloor abs\left(y'_{1i}\right)-\left\lfloor y'_{1i}\right\rfloor\times 10^{14}\right\rfloor \bmod 2^{10} \end{cases} \tag{13}$$

通过式(13)的x''_{1i}, y''_{1i}来构建新的序列x_{1i}, y_{1i}：

$$\begin{cases} x_{1i}=\left(x''_{1i}+y''_{1i}\right) \bmod 2^{8} \\ y_{1i}=\left\lfloor y''_{1i}\oplus LBS\left(x''_{1i},\,2\right)\right\rfloor \bmod 2^{8} \end{cases} \tag{14}$$

式中：$LBS\left(x''_{1i},\,2\right)$为从$x''_{1i}$向右移2位的操作；$\lfloor\ \rfloor$为向上取整运算。

再从$\left\{x_{1i}\right\}$中挑选出前$(S+36)/2$个元素；从$\left\{y_{1i}\right\}$中挑选出后$(S+36)/2$个元素。并将其组合为序列$\boldsymbol{Z}=\left\{z_1,z_2,\cdots,z_{(S+36)}\right\}$，从而设计加密方法：

$$a_i=i+\bmod\left(floor\left(z(i+1\,000)\times 10^{10}\right),(S+36)-1\right),\ i\in\left[1,(S+36)\right] \tag{15}$$

$$\left[z(i),z\left(a_i\right)\right]=swap\left\{z(i),z\left(a_i\right)\right\} \tag{16}$$

式中：a_i为加密后的位置；$z(i)$为第z个哈希序列值；$swap$为位置交叉运算。

通过式(15)和式(16)的加密后，形成最终的哈希序列$\boldsymbol{H}=\left\{h_1,h_2,\cdots,h_{(S+36)}\right\}$。

最后，采用l_2范数距离d[17]，完成待认证图像的真实性判别。若初始图像、待认证目标分别为$f_1(x,y)$、$f_2(x,y)$；则二者经上述哈希生成过程处理后，形成对应的哈希序列为$\boldsymbol{H}_0=\left\{h_1^0,h_2^0,h_3^0,\cdots,H_{S+36}^0\right\}$、$\boldsymbol{H}_1=\left\{h_1^1,h_2^1,h_3^1,\cdots,H_{S+36}^1\right\}$。根据文献[15]可得二者之间的$d$值计算函数为：

$$d\left(\boldsymbol{H}_0,\boldsymbol{H}_1\right)=\sqrt{\sum_{i=1}^{n}\left[h_i^0-h_i^1\right]^2} \tag{17}$$

将式(17)计算的d值与阈值W对比，若$d\leqslant W$，则将二者当作相似图像；否则，二者是差异图像。

2 实验结果与分析

为了验证本文哈希方案的有效性，在非压缩彩色图像数据库[18](Uncompressed Colour Image Database，UCID)中，随意选择图像作为实验样本。与此同时，为了反映出本文算法的优势，将文献[4−6]和文献[19]4种哈希算法作为对比组。其中，文献[19]利用线性插值与高斯滤波来对图像实施预处理，使其对尺度、噪声等内容修改具备较好的稳健性，并计算滤波图像的四元极性复指数变换矩，以此生成鲁棒哈希，其采用四元极性复指数变换对旋转、平移、噪声等内容修改具有出色的鲁棒性，对此类内容修改具有较高的识别准确率。

在哈希生成阶段，阈值W对图像的判别准确度影响较大，所以，在进行认证实验时，要对W实施优化，利用一个最优值来实现哈希认证。其他实验参数设置如下：初始图像尺寸$M\times N$=512×1 024，$Z\times Z$=360×360，λ=2.5，最大阶数n=5，最大重复次数m=5，初始条件u=0.486，x_0=0.64，y_0=0.79。

2.1 阈值W的优化

在UCID数据库[18]中任意选择60幅图像为样本，把表1中的所有修改类型施加于这些样本，通过PS工具，得到960对相似图像；随后，再选择150幅图像，基于PS软件，通过复制−粘贴、裁剪以及组合恶意攻击，形成1 500对差异图像。通过式(17)来计算这些图像之间的l_2范数距离，以此来确定一个较优的W值。

图6显示了初始图像与内容修改图像之间的频数分布。由图6(a)发现，当$d<27.5$时，相应的频数分布波动剧烈。依据图6(b)发现，当$d>25.5$时，差异图像对应的频率波动较为剧烈。因此，本文取$W=27.5$，用该值完成图像认证。

表1 不同内容修改类型及其参数

Table1 Different attack types and their parameters

operation type	parameter
salt and pepper noise	0.03,0.04,0.05,0.06
brightness adjustment	1.1,1.3,1.7,2.0
rotation	60°,80°,100°,120°
scaling	0.3,0.5,0.7,0.9

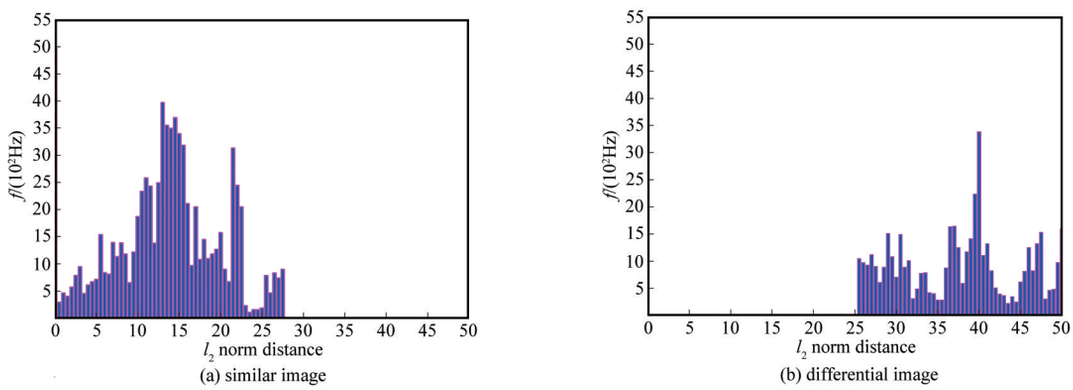


Fig.6 Optimization of threshold W

图6 阈值W的优化

2.2 所提算法的鲁棒性测试

感知鲁棒性是客观量化哈希算法优劣的经典指标[2]，故在此次试验中，从UCID库中选择6幅彩色图像作为样本，如图7(a)~7(f)所示；并把表1中的4种内容修改类型来攻击6个样本。再借助式(17)来获取初始样本与修改图像之间的l_2范数距离，输出数据见图7(g)~7(j)。通过观察图中数据发现，当图像遭遇内容修改后，通过所提算法生成的哈希之间对应地利用本文哈希l_2范数距离都要小于27.5。尤其是旋转变换，所提算法仍然呈现出理想的鲁棒性，在100°范围内，对应的d值小于11，即使是超过100°，对于6个测试样本，其对应的d值仍然远小于阈值27.5。主要是由于所提算法采用了线性插值与非线性滤波来改善哈希对噪声、缩放的鲁棒性；并联合颜色矢量角度与DWT机制，充分提取图像的结构特征，增强哈希对亮度修改的识别能力。另外，所提算法还计算了预处理图像的径向Tchebichef矩，使其对任意角度旋转均有理想的鲁棒性。

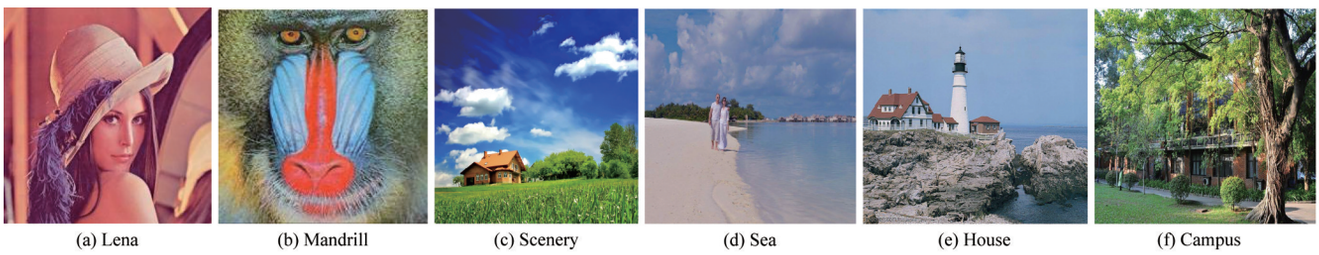
图像在互联网中发送时，经常会受到恶意攻击，此时，产生的哈希序列存在较大的差异，所以，良好的哈希算法应能有效区分常规内容修改操作与恶意攻击，对其做出准确的判别[2]。故在此次试验中，将图8(a)、图9(a)视为样本，把常规内容修改和恶意攻击作用于它，利用l_2范数距离来识别这些待认证图像，数据见表2和表3。通过观察数据发现，对于诸如噪声、亮度等常规的内容修改，见图8(b)~8(c)，二者的l_2范数距离分别为18.21,17.53，远低于27.5，将其判别为相似图像；然而，对于另外3种恶意修改，见图8(d)~ 8(f)，三者的l_2范数距离都高于27.5。说明这3幅图像与初始目标是差异图像，判别为可疑目标。同样，对于图9而言，也有类似的结果，如表3所示，对于旋转、亮度与噪声等变换，其对应的d值远低于27.5，分别为2.86,13.09和11.44。而对于颜色、复制−粘贴等变换，其对应的d值高于判断阈值。

2.3 不同算法的鲁棒性测试

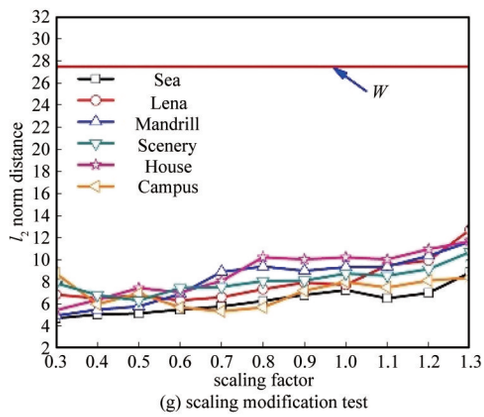
为了突出本文算法的优势，将其与文献[4−6]和文献[19]技术进行测试，首先，在UCID库[18]中任意选择200幅图像作为样本，通过5种哈希算法对其认证，获取对应的接收机工作特性曲线(Receiver Operating Characteristic，ROC)[3]。ROC曲线[3]由P_{TPR}与P_{FPR}组成：

$$P_{\mathrm{TPR}}=\frac{n_1}{M_1},\ P_{\mathrm{FPR}}=\frac{n_2}{M_2} \tag{18}$$

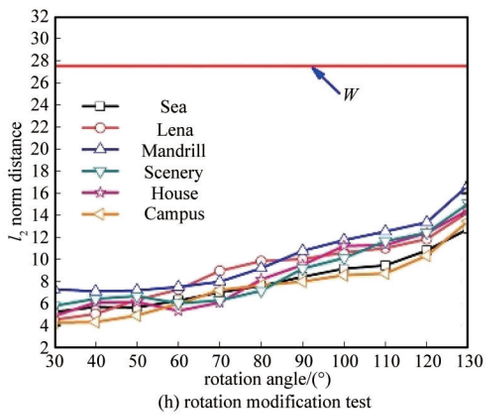
式中：P_{TPR}是正确识别率；P_{FPR}是虚警率；n_1为正确识别的样本数量；n_2为误判的样本数量；M_1,M_2分别是真实图像与待认证图像的总量[3]。



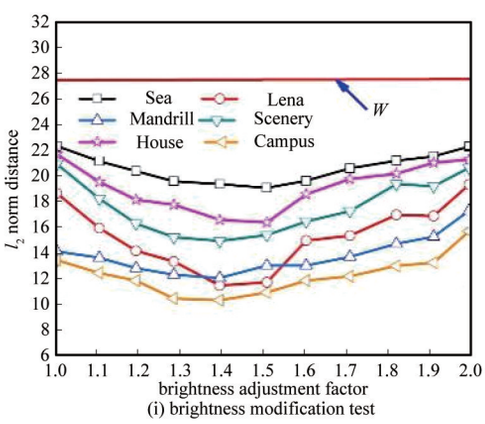
(a) Lena (b) Mandrill (c) Scenery (d) Sea (e) House (f) Campus



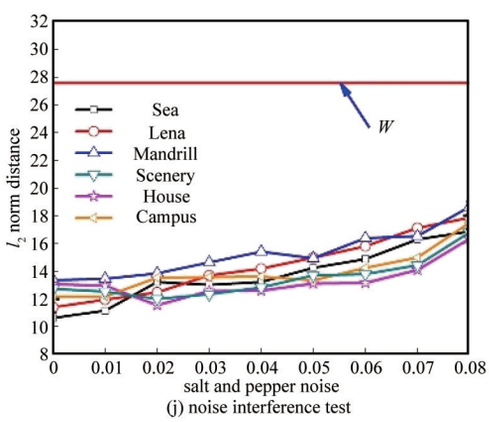
(g) scaling modification test



(h) rotation modification test



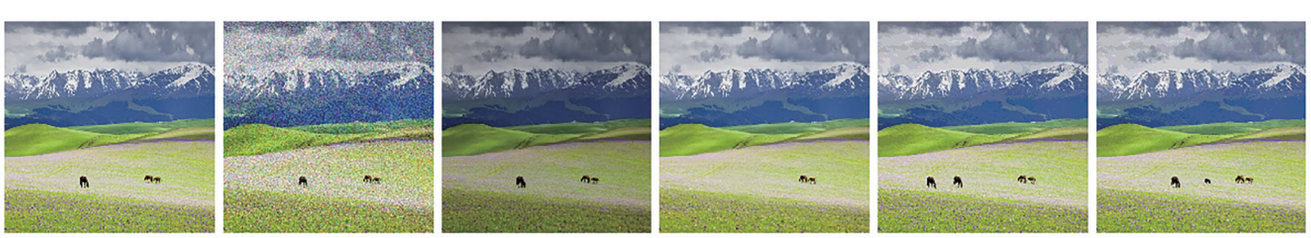
(i) brightness modification test



(j) noise interference test

Fig.7 Perceptual robustness testing

图 7 感知鲁棒性测试



(a) initial image (b) salt and pepper modification (c) brightness modification (d) crop (e) copy paste (f) copy–paste + scaling

Fig.8 Regular content modification and malicious attacks

图 8 常规内容修改与恶意攻击

5 种哈希算法对应的 ROC 曲线如图 10 所示。根据曲线发现，本文算法、文献[4]、文献[5]、文献[6]和文献[19]对缩放、噪声修改都有很好的感知鲁棒性，表现出较佳的 ROC 特性，P_{TPR} 维持在 0.96 以上，见图 10(a)、10(b)。然而，对于亮度与颜色等 3 种几何变换，5 种技术的鲁棒性表现不一致。面对这 3 类修改，所提算法与文献[6]、文献[19]对旋转攻击具有最好的鲁棒性，正确识别率最高。文献[4]、文献[19]与本文算法对颜色修改具有较好的稳健性，拥有较高的正确识别率，而且所提算法对颜色修改的鲁棒性最高，文献[6]的鲁棒性最低，见图 10(e)。相反，文献[5]对旋转与亮度修改表现出较低的鲁棒性，见图 10(c)、图 10(d)。文献[19]对旋转攻击的鲁棒性最好，要优于所提算法，见图 10(c)。另外，从图 10(d)中可知，所提算法对亮度变换也呈现出最高的稳健性。

例如，图像经过亮度修改后，对于$P_{FPR}=0$，文献[4−5]、文献[19]、文献[6]和本文算法的P_{TPR}分别为0.922,0.810,0.902,0.873,0.941；$P_{FPR}=0.3$时，它们的P_{FPR}分别是0.996,0.974,0.992,0.987,0.998。原因是所提算法、文献[4−6]和文献[19]都采用预处理方式来规范目标尺寸和消除噪声干扰，可提高其对缩放与噪声修改的鲁棒性。但是，所提算法采用了颜色矢量角度与DWT方法来提取图像的感知结构特征，使其对亮度、颜色具备出色的稳健性。而且该算法采用图像的径向Tchebichef矩来描述图像中的抗旋转特征，从而增强了哈希序列对旋转的鲁棒性。文献[19]算法采用了线性插值和高斯滤波来处理图像，使其对尺度和噪声具备很好的鲁棒性，并采用四元极性复指数变换来生成哈希，四元极性复指数变换考虑了彩色图像不同分量直接的关系，使其提取的特征对旋转攻击的鲁棒性更加出色，要优于本文算法。但是，文献[19]提取的特征对亮度修改缺乏足够敏感性，使其对亮度修改的鲁棒性有待提高。文献[6]采用预处理来固定哈希长度与消除噪声影响，对这两类攻击具有理想的鲁棒性，而且采用了径向Tchebichef矩来提取亮度分量的形状特征，以此来生成哈希序列，这种Tchebichef矩对旋转具有理想的稳健性，但其只提取图像的L分量中的特征点，忽略了其他分量的信息，导致其对鲁棒特征点提取不够充分，因此，其对抗旋转攻击的鲁棒性要略低于本文算法与文献[19]，另外，该技术忽略了图像的颜色特征，使其对颜色篡改不敏感。而文献[4]也采用了颜色矢量角度来描述图像中最大内切圆里面的抗亮度修改的特征，使其对亮度、颜色攻击具备理想的鲁棒性，但是最大内切圆中的可用信息量整体要少，导致其提取的鲁棒特征点不够充分，使其对亮度、颜色修改的鲁棒性要低于本文算法，而且该算法不能有效描述图像抗旋转修改的特征，使其对旋转修改的鲁棒性不理想。文献[5]采用颜色特征和模糊直方图来生成哈希，对颜色变换具有较好的稳健性，但是颜色特性对亮度L成分的变化不是很稳定，另外，图像的直方图对旋转攻击缺乏鲁棒性，从而导致该方法对亮度、旋转的鲁棒性不佳。

(a) initial image　(b) rotation modification　(c) brightness modification　(d) salt and pepper noise　(e) copy−paste + scaling　(f) color modification

Fig.9 General content modification and malicious attack of "gun library" image

图9 "枪库"图像的常规内容修改与恶意攻击

表2 不同攻击类型图像的认证决策结果

Table2 Authentication decision results of different attack types of images

name	Fig.8(b)	Fig.8(c)	Fig.8(d)	Fig.8(e)	Fig.8(f)
d value	18.21	17.53	33.69	35.87	40.18

表3 各类几何变换图像的认证决策结果

Table3 Authentication decision results of different attack types of images

name	Fig.9(b)	Fig.9(c)	Fig.9(d)	Fig.9(e)	Fig.9(f)
d value	2.86	13.09	11.44	41.37	35.89

3　结 论

为了改善哈希算法对亮度与任意角度的修改，本文设计了径向Tchebichef矩耦合颜色矢量角度的鲁棒图像哈希算法。通过对输入图像实施插值与滤波等预处理方法，改善哈希序列对尺度修改、噪声干扰的鲁棒性；通过计算规范图像的颜色矢量角度，提高哈希对亮度修改的稳定性，并引入DWT机制来压缩哈希序列的长度，提高生成效率；为了改善哈希算法对任意角度旋转的鲁棒性，本文引入径向Tchebichef矩，通过计算与处理图像的Tchebichef矩，联合DWT的低频系数，生成中间哈希序列。设计加密方法，对其完成加密，得到最终的鲁棒哈希序列。在旋转、缩放、噪声以及亮度等攻击实验下，本文哈希算法能够准确识别出常规修改与恶意篡改，具有较高的鲁棒性，而且当虚警率为0.2时，其准确率均维持在0.99以上，具有理想的识别准确率。

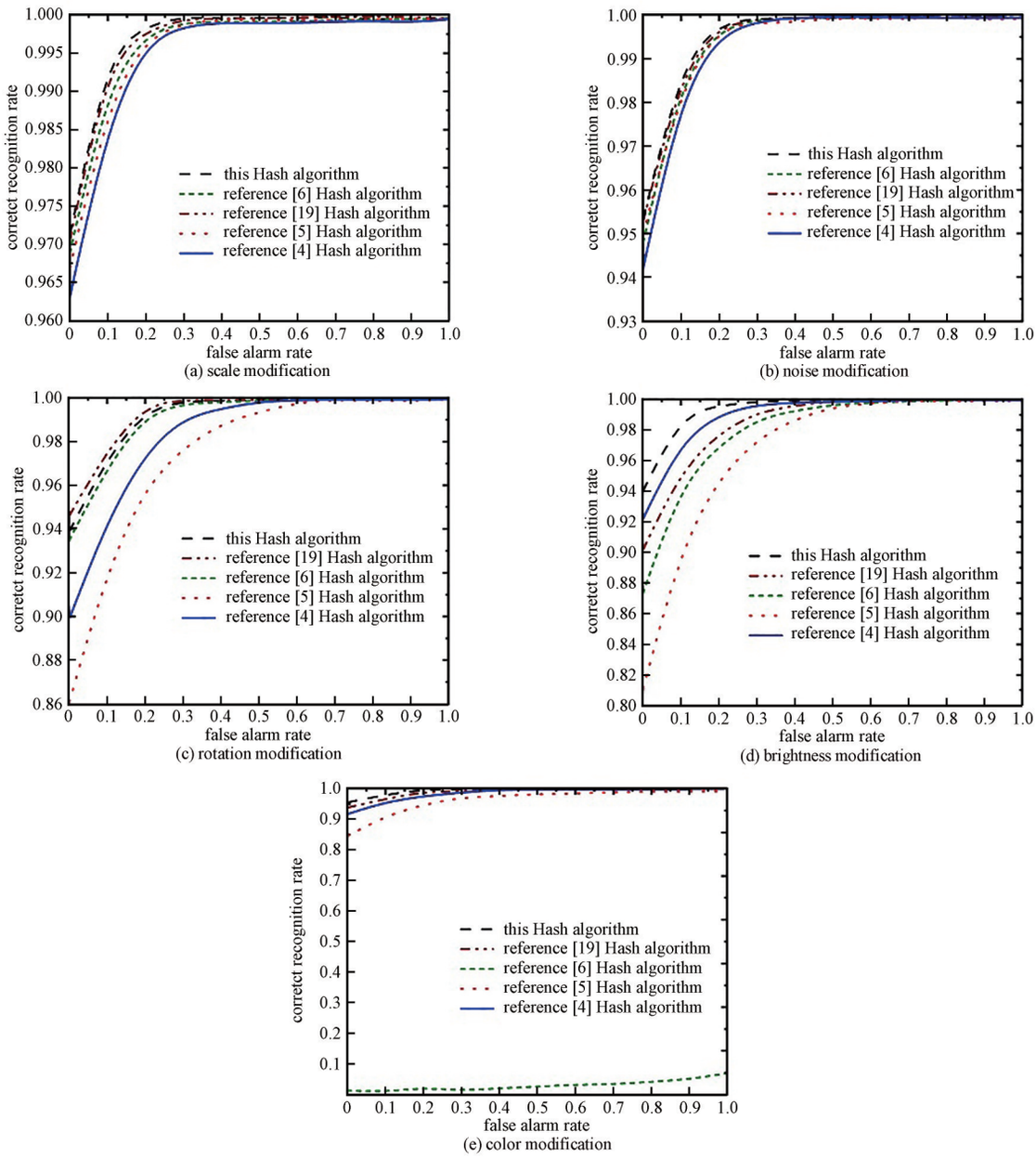


Fig.10 Robustness testing of different algorithms
图 10 不同算法的鲁棒性测试

参考文献：

[1] 史进,蔡竞,徐锋. 基于QR码与级联Fourier变换的图像光学加密算法[J]. 太赫兹科学与电子信息学报, 2020,18(3):462-469. (SHI Jin,CAI Jing,XU Feng. Multi-image optical encryption algorithm based on QR code and concatenated fractional Fourier transform[J]. Journal of Terahertz Science and Electronic Information Technology, 2020, 18(3): 462-469.) doi: 10.11805/tkyda2019217.

[2] 王彦超. 基于联合特征与中心方向信息的图像哈希算法[J]. 西南大学学报(自然科学版), 2018,40(2):113-124. (WANG Yanchao. Image Hashing algorithm based on joint feature and central direction information[J]. Journal of Southwest University (Natural Science Edition), 2018,40(2):113-124.) doi:10.13718/j.cnki.xdzk.2018.02.017.

[3] 王彦超. 基于邻域LBP算子与块截断编码的图像哈希算法[J]. 计算机工程与设计, 2018,39(7):2027-2035. (WANG Yanchao. Image Hashing algorithm based on neighborhood LBP operator and block truncation coding[J]. Computer Engineering and Design, 2018,39(7):2027-2035.) doi:CNKI:SUN:SJSJ.0.2018-07-038.

[4] TANG Zhenjun,LI Xuelong,ZHANG Xianquan. Image Hashing with color vector angle[J]. Neurocomputing, 2018,308(12):147-158. doi:10.1016/j.neucom.2018.04.057.

[5] NILESH D G, DALTON M T. Robust perceptual image Hashing using fuzzy color histogram[J]. Multimedia Tools and Applications, 2019,77(23):30815–30840. doi:10.1007/s11042–018–6115–1.

[6] 陈勇昌. 基于不变特征的数字水印与感知哈希图像认证技术研究[D]. 广州:华南理工大学, 2014. (CHEN Yongchang. Research on digital watermarking and perceptual Hash image authentication technology based on invariant features[D]. Guangzhou,China:South China University of Technology, 2014.)

[7] CHEN Y, YU W, FENG J. Robust image Hashing using invariants of Tchebichef moments[J]. Optik-International Journal for Light and Electron Optics, 2014,125(19):5582–5587. doi:10.1016/j.ijleo.2014.07.006.

[8] ZHANG Benxin, ZHU Zhibin, WANG Shuo. A simple primal-dual method for total variation image restoration[J]. Journal of Visual Communication and Image Representation, 2016,38(2):814–823. doi:10.1016/j.jvcir.2016.04.025.

[9] 孙俊岭, 杨杰. 一种基于微小区域的TV双调和型偏微分方程图像修复方法[J]. 河南理工大学学报(自然科学版), 2018, 37(3):150–157. (SUN Junling, YANG Jie. An image restoration method for TV biharmonic partial differential equation based on micro-region[J]. Journal of Henan University of Technology(Natural Science Edition), 2018,37(3):150–157.) doi:10.16186/j.cnki.1673–9787.2018.03.22.

[10] TANG Zhenjun, DAI Yumin, ZHANG Xianqi. Perceptual image Hashing with histogram of color vector angles[J]. International Conference on Active Media Technology, 2012,33(1):108–126. doi:10.1007/978–3–642–35236–2_24.

[11] QIN Chuan, SUN Meihui, CHANG Chinchen. Perceptual Hashing for color images based on hybrid extraction of structural features[J]. Signal Processing, 2018,142(10):194–205. doi:10.1016/j.sigpro.2017.07.019.

[12] 李秀琴. 基于DWT特征点和方向直方图的图像哈希算法[D]. 广西:广西大学, 2016. (LI Xiuqin. Image Hashing algorithm based on DWT feature points and directional histogram[D]. Guangxi,China:Guangxi University, 2016.)

[13] XIAO Bin, MA Jianfeng, CUI Jiangtao. Radial Tchebichef moment invariants for image recognition[J]. Journal of Visual Communication and Image Representation, 2012,23(2):381–386. doi:10.1016/j.jvcir.2011.11.008.

[14] WU Haiyong, YAN Senlin. Computing invariants of Tchebichef moments for shape based image retrieval[J]. Neurocomputing, 2017,215(19):110–117. doi:10.1016/j.neucom.2015.05.147.

[15] HUA Zhongyun, ZHOU Yicong. Image encryption using 2D logistic-adjusted-sine map[J]. Information Sciences, 2016, 339(C): 237–253. doi:10.1016/j.ins.2016.01.017.

[16] 余萍, 闻恺. 基于混沌交换控制表与关联动态引擎的图像加密算法[J]. 新疆大学学报(自然科学版), 2017,34(4):459–466. (YU Ping, WEN Kai. Image encryption algorithm based on chaotic switching control table and associated dynamic engine[J]. Journal of Xinjiang University(Natural Science Edition), 2017,34(4):459–466.) doi:10.13568/j.cnki.651094.2017.04.015.

[17] YE Qiaolin, FU Liyong, ZHANG Zhao. Lp-and Ls-norm distance based robust linear discriminant analysis[J]. Neural Networks, 2018(105):393–404. doi:10.1016/j.neunet.2018.05.020.

[18] SCHAEFER G, STICH M. UCID—an uncompressed color image database[C]// Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multi-media. San Jose,CA,USA:[s.n.], 2004:472–480. doi:10.1117/12.525375.

[19] KHALID M H, YASMEEN M K, WALID I K. Robust color image Hashing using quaternion polar complex exponential transform for image authentication[J]. Circuits Systems,and Signal Processing, 2018,37(12):5441–5462. doi:10.1007/s00034–018–0822–8.

作者简介：

王　瑶(1979–)，女，硕士，副教授，主要研究方向为计算机图像、信息安全、多媒体技术. email: WangyAo1979ccity@126.com.

陈文宇(1968–)，男，博士，博士生导师，教授，主要研究方向为图像处理、信息安全、计算机应用.