结合 Zernike 矩和水印的半脆弱图像认证

吴晓云[1,2] 刘红梅[1,3] 黄继武[1,3]

摘 要 水印安全性、抗 JPEG 的鲁棒性和篡改检测能力的矛盾、计算复杂度是现有基于数字水印的半脆弱图像认证算法需要克服的主要问题. 本文提出一种结合 Zernike 矩和水印的图像认证算法. 利用图像小波变换低频子带的 Zernike 矩幅值的半脆弱特性区分恶意攻击和偶然攻击. 结合基于 HVS (人类视觉系统) 的水印后，可判断图像是否受到伪认证攻击，提高了水印安全性. 通过采用基于提升格式的整数小波变换，有效降低了算法计算复杂性. 实验结果表明，算法对较低质量因子的 JPEG 有损压缩鲁棒，对剪切、替换等恶意修改敏感且可准确定位篡改位置.

关键词 半脆弱图像认证，Zernike 矩，图像水印，人类视觉系统，整数小波变换
中图分类号 TP391

Semi-Fragile Image Authentication Based on Zernike Moments and Watermark

WU Xiao-Yun[1,2] LIU Hong-Mei[1,3] HUANG Ji-Wu[1,3]

Abstract How to ensure watermark security, how to overcome the contradiction between robustness and JPEG lossy compression, how to cancel out the contradiction between fragility and malicious tamper, and how to reduce the computational complexity are the main issues to be solved in the existing semi-fragile image authentication algorithms based on watermark technique. In this paper, a semi-fragile image authentication algorithm using Zernike moments and watermark is proposed. It can distinguish malicious modification from incidental modification according to semi-fragile characteristics of Zernike moments of the low frequency subband in the integer wavelet transform domain of an image. Combining the semi-fragile characteristics of Zernike moments and the watermark based on human visual system, it can discern counterfeit attack, thus, improving watermark security. Computational complexity is reduced by integer wavelet transform using lifting scheme. Experimental results show that the proposed algorithm tolerates JPEG lossy compression to a large extent, and meanwhile it is fragile to malicious tamper and capable of locating the tampered area accurately.

Key words Semi-fragile image authentication, Zernike moments, image watermarking, human visual system, integer wavelet transform

1 引言

数字图像可被图像处理软件轻易地修改，由于更改后的图像可以以假乱真，眼见不再为实已是数字时代一个不争的事实. 因此，必须对数字图像进行认证，以鉴定其内容的完整性和真实性[1].

数字签名是经典的认证方法，但其用于图像认证存在一些不足. 作为数字签名的有效补充，脆弱水印近年来引起了人们广泛的兴趣，它可分为完全脆弱水印和半脆弱水印[2]，两者的区别在于前者对施加于其上的任何操作都十分敏感，后者则对更改图像内容的恶意操作 (剪切或替换) 敏感，而允许不影响内容语义的正常图像处理操作 (JPEG 有损压缩、锐化、模糊等)，故适用于内容认证. 在实际应用中，为了方便传输，需对图像进行压缩 (当前普遍采用 JPEG 有损压缩)，因此，开发对这类压缩不敏感的半脆弱图像认证技术就显得尤为重要.

一般地说，基于水印技术的有效半脆弱图像认证算法应当具备以下特点： 1) 水印图像与原始图像的差异视觉上不可感知； 2) 水印具有较高的安全性，尤其是能够抵抗伪认证攻击[2]； 3) 水印提取无需原始图像； 4) 水印能够承受较低质量因子的 JPEG 有损压缩，而对改变图像内容的恶意操作敏感； 5) 可准确定位恶意篡改区域； 6) 计算复杂度低.

已有不少半脆弱图像认证算法被报道[3~5]. Kundur 等[3]通过量化 Harr 小波变换系数实现水印的嵌入. 利用小波变换的多分辨率特性， 该方案

收稿日期 2005-8-12 收修改稿日期 2006-7-9
Received August 12, 2005; in revised form July 9, 2006
国家自然科学基金 (90604008, 60633030)，国家 973 计划 (2006CB303104)，广东省自然科学基金团队项目 (04205407) 和广州市科技攻关项目 (2005Z3-D0391) 资助
Supported by National Natural Science Foundation of P. R. China (90604008, 60633030), National 973 Program of P. R. China (2006CB303104), Natural Science Foundation of Guangdong (04205407), and Key Project of Science and Technology of Guangzhou (2005Z3-D0391)
1. 中山大学信息科学与技术学院 广州 510275 2. 广东商学院信息学院 广州 510320 3. 广东省信息安全技术重点实验室 广州 510275
1. School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275 2. School of Information Science, Guangdong University of Business Studies, Guangzhou 510320 3. Guangdong Key Laboratory of Information Security Technology, Guangzhou 510275
DOI: 10.1360/aas-007-0145

可以检测到不同分辨率下的水印篡改图，但其用以调制的量化步长违反 HVS (人类视觉系统)，易致水印图在视觉上产生失真. Lin 等[4]利用 JPEG 压缩前后 DCT (离散余弦变换) 系数的两个不变属性，提出一个可以抵抗 JPEG 压缩的认证方案，不过该法承受 JPEG 有损压缩的能力受制于算法. Han 等[5]提出一种基于分块量化的认证算法，它对 JPEG 及 JPEG2000 鲁棒，但是该算法没有考虑水印的安全性. 此外这些算法均是基于传统 DWT (离散小波变换) 或传统 DCT，算法的计算复杂度偏高. 由此可见它们均没能完全满足以上实用认证算法的各项要求.

为了满足上述有效认证算法的各项要求，本文提出一种结合图像 Zernike 矩和水印的半脆弱图像认证算法. 算法遵循 HVS 的特点实现水印的嵌入，以满足水印的不可见性. 利用 Zernike 矩的半脆弱特性，算法可将恶意攻击及偶然攻击区分开，结合水印信息，可识别出伪认证攻击，从而提高水印的安全性. 采用基于提升格式实现的整数小波变换，其计算复杂度较传统 DCT 和传统 DWT 低. 实验结果表明，算法能够容忍较低质量因子的 JPEG 有损压缩，同时对恶意攻击脆弱，并能够准确定位篡改区域.

2 整数小波变换

Sweldens 等[6]提出采用小波提升格式可以实现整数小波变换. 小波提升分为三步：分裂、预测和更新[7]. Daubechies 等[7]给出一种 9-7 双正交小波滤器的提升步骤，对于一维信号 $\{x_l\}_{l\in Z}$，其提升过程为

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases}$$

$$\begin{cases} d_l^{(1)} = d_l^{(0)} + \alpha(s_l^{(0)} + s_{l+1}^{(0)}) \\ s_l^{(1)} = s_l^{(0)} + \beta(d_l^{(1)} + d_{l-1}^{(0)}) \end{cases} \quad (1)$$

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + \gamma(s_l^{(1)} + s_{l+1}^{(1)}) \\ s_l^{(2)} = s_l^{(1)} + \delta(d_l^{(2)} + d_{l-1}^{(2)}) \end{cases}$$

$$\begin{cases} s_l = \zeta s_l^2 \\ d_l = d_l^{(2)}/\zeta \end{cases} \quad (2)$$

这里 s_l 和 d_l 分别为低频和高频分量，$s_l^{(i)}$, $d_l^{(i)}(i = 0, 1, 2)$ 为中间结果，参数 $\alpha = -1.586134342$; $\beta = -0.05298011854$; $\gamma = 0.8829110762$; $\delta = 0.4435068522$; $\zeta = 1.149604398$.

依据整数小波变换理论[8]，上述一维信号 $\{x_l\}_{l\in Z}$ 的整数小波分解构造如下

$$\begin{cases} s_l^{(0)} = x_{2l} \\ d_l^{(0)} = x_{2l+1} \end{cases}$$

$$\begin{cases} d_l^{(1)} = d_l^{(0)} + \mathrm{int}(\alpha(s_l^{(0)} + s_{l+1}^{(0)})) \\ s_l^{(1)} = s_l^{(0)} + \mathrm{int}(\beta(d_l^{(1)} + d_{l-1}^{(0)})) \end{cases} \quad (3)$$

$$\begin{cases} d_l^{(2)} = d_l^{(1)} + \mathrm{int}(\gamma(s_l^{(1)} + s_{l+1}^{(1)})) \\ s_l^{(2)} = s_l^{(1)} + \mathrm{int}(\delta(d_l^{(2)} + d_{l-1}^{(2)})) \end{cases}$$

$$\begin{cases} d_l^{(3)} = d_l^{(2)} + \mathrm{int}((\zeta - \zeta^2)s_l^{(2)}) \\ s_l^{(3)} = s_l^{(2)} + \mathrm{int}((-1/\zeta)d_l^{(3)}) \end{cases}$$

$$\begin{cases} d_l^{(4)} = d_l^{(3)} + \mathrm{int}((\zeta - 1)s_l^{(3)}) \\ s_l^{(4)} = s_l^{(3)} + d_l^{(4)} \end{cases} \quad (4)$$

$$\begin{cases} s_l = s_l^{(4)} \\ d_l = d_l^{(4)} \end{cases}$$

其中 $\mathrm{int}(x)$ 为取整函数. 重构过程只是上述过程的逆过程，不再赘述.

3 Zernike 矩

Zernike 矩广泛应用于模式识别、目标分类、目标识别与方位估计、图像编码和重构等方面. 一幅数字图像的 Zernike 矩集，描述了图像形状的全局特征，其 n 阶 m 重 Zernike 矩的定义见文献 [9].

图像 Zernike 矩的幅值具有认证所需要的半脆弱特性，即图像在正常信号处理前后的矩幅值差异不大，而遭受恶意攻击前后的矩幅值差异十分显著.

下面通过实验证实矩幅值的这种半脆弱特性. 实验对象为图 1 所示的 $512 \times 512 \times 8$ 的六幅测试图像. 由于计算整幅图像的 Zernike 矩的运算量偏大，而图像整数小波变换后的低频子带为原始图像的近似，故使用低频子带计算 Zernike 矩，实验中选择 LL_3 子带并计算其 12 阶共计 49 个矩的幅值，这是因为相对于其它阶的矩值，12 阶矩值在计算复杂度及表征图像特征方面能取得较佳的折衷. 具体的实验步骤如下：

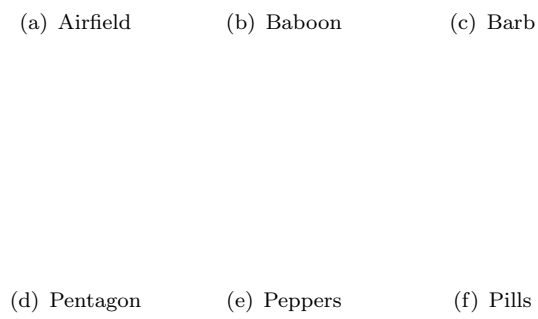
1) 首先对原始图像进行三级整数小波分解，计算 LL_3 子带的 12 阶共计 49 个 Zernike 矩的幅值，记其为 $M_i(1 \le i \le 49)$.

2) 对原始图像分别进行 JPEG 有损压缩、剪切、替换等操作，产生相应的受攻击后的图像，对各攻击图像进行三级整数小波分解，计算 LL_3 子

带的 12 阶共计 49 个 Zernike 矩的幅值，记其为 $M_i^{'}(1 \le i \le 49)$.

3) 依式 (5) 计算攻击前后图像的矩幅值差异.

$$\Delta = \sqrt{\frac{1}{49}\sum_{i=1}^{49}(M_i - M_i')^2} \tag{5}$$



(a) Airfield　(b) Baboon　(c) Barb

(d) Pentagon　(e) Peppers　(f) Pills

图 1　测试图像

Fig. 1　Testing image

实验结果如表 1 所示. 其中 JPEG90 表示图像受到质量因子为 90 的 JPEG 有损压缩，剪切 (Cut) 是指图像的某一区域全部被替换为白色象素. 替换 (Replace) 是指用图像自身某一区域的图像替换另一区域的图像. 由表 1 可见，六幅图像遭受 JPEG40 后 Zernike 矩幅值的最大差异为 156.39, 而受到 16×16 剪切及 16×16 替换攻击后的 Zernike 矩幅值的最小差异分为 1417.60 和 381.95，受到 32×32 剪切及 32×32 替换攻击后的 Zernike 矩幅值的最小差异分为 1271.1 和 748.01. 这说明图像受到 JPEG 有损压缩后的 Zernike 矩幅值差异远远小于其受到剪切、替换等恶意攻击后的 Zernike 矩幅值差异. 可见图像整数小波变换后的低频子带的 Zernike 矩具有半脆弱特性，利用这一特性，根据一个预先设定的阈值，即可将恶意攻击与偶然攻击区分开.

4　图像的半脆弱认证算法

4.1　水印嵌入

本文采用一幅二值图像 W 作水印，记其加密结果为 W^*. 为了保证嵌入水印后的图像与原始图像的差别视觉上不可感知，我们遵循 HVS 嵌入水印.

Watson 等[10]研究了小波域的 HVS，针对 9-7 双正交小波滤波器，提出了一个量化矩阵，水印嵌入时只要小波系数的变化不超过量化矩阵所给定的最大容许值，即可满足水印图像的透明性. 本文使用 Watson 量化矩阵实现小波域内嵌入水印.

对图像进行三级整数小波分解，计算 LL_3 子带 12 阶共 49 个 Zernike 矩的幅值，记为 $M_i(org), 1 \le i \le 49$，然后在 HL_3 子带嵌入水印 W^*，嵌入方法如下：首先计算

$$Q(i,j) = \begin{cases} 0 & \lfloor f(i,j)/JND(i,j) \rfloor \text{为偶数} \\ 1 & \lfloor f(i,j)/JND(i,j) \rfloor \text{为奇数} \end{cases} \tag{6}$$

这里 $JND(\cdot,\cdot)$ 为 Watson 量化矩阵. $\lfloor \cdot \rfloor$ 为地板函数，$f(i,j)$ 为 HL_3 子带内 (i,j) 处的小波系数. 记当前欲嵌入的水印位为 $w^*(i,j)$，则依本页下方式 (7) 修改小波系数.

式 (7) 中小波系数 $f(i,j)$ 为正时选加号，为负时用减号，最后经整数小波逆变换得到含水印图像.

4.2　篡改检测

对待认证图像进行三级整数小波变换，计算其 LL_3 子带 12 阶共 49 个 Zernike 矩的幅值，记为 $M_i(new), 1 \le i \le 49$. 记 $f^{'}(i,j)$ 为 HL_3 子带 (i,j) 处的小波系数，依式 (8) 提取水印

$$w^{*\prime} = \begin{cases} 0 & \lfloor f^{'}(i,j)/JND(i,j) \rfloor \text{为偶数} \\ 1 & \lfloor f^{'}(i,j)/JND(i,j) \rfloor \text{为奇数} \end{cases} \tag{8}$$

可见水印提取时无需原始图像，故为盲提取. 进一步对提取出的水印进行解密，结果记为 $W^{'}$. 分别依式 (9) 和 (10) 计算水印差值图和矩幅值差异.

$$D = |W - W^{'}| \tag{9}$$

$$\Delta^{'} = \sqrt{\frac{1}{49}\sum_{i=1}^{49}(M_i(org) - M_i'(new))^2} \tag{10}$$

$$\tilde{f}(i,j) = \begin{cases} f(i,j) & \text{if} \quad Q(i,j) = w^*(i,j) \\ (\lfloor f(i,j)/JND(i,j) \rfloor \pm 1) \cdot JND(i,j) & \text{if} \quad Q(i,j) \ne w^*(i,j) \end{cases} \tag{7}$$

表 1 攻击前后图像整数小波 LL_3 子带的矩幅值差异

Table 1 Difference of Zernike moments magnitudes of LL_3 subband in integer wavelet domain of an image before and after attack

攻击	Airfield	Baboon	Barb	Pentagon	Peppers	Pills
JPEG90	59.54	33.25	45.07	59.63	40.57	33.14
JPEG70	94.93	73.53	62.87	61.81	52.22	52.62
JPEG50	140.79	104.89	80.82	69.36	81.75	74.45
JPEG40	156.39	105.07	85.15	88.47	83.51	107.76
Cut(16×16)	1417.60	6047.40	4082.40	6268.40	4555.50	1785.20
Replace(16×16)	683.31	828.35	483.79	381.95	653.02	515.07
Cut(32×32)	1271.1	5887.8	4232.2	5625.5	4135.3	2470.8
Replace(32×32)	1633.4	1072.2	1493.3	1191.1	748.01	1038.7

差值图 D 反映出两幅二值图像之间的差异，如果对应象素点的象素值相等，则差值图像上的象素值为 0，表现为黑点，表明该点没被更改；反之为 1，表现为白点，表明该点被篡改. 因此由差值图即可定位图像篡改区域.

在对图像进行认证时，若 D 和 Δ' 均为 0，说明图像真实无误. 若 Δ' 不为 0，令 τ 为一可区分恶意攻击及偶然攻击的阈值，该阈值可由实验得到，此时如果 $\Delta' \leq \tau$，可断定图像受到偶然攻击，否则受到恶意攻击，可进一步由水印差值图定位篡改区域.

5 性能分析

5.1 安全性分析

针对脆弱水印最具威胁力的攻击是伪认证攻击. 攻击者对水印图像实施伪认证攻击后，尽管此时图像的内容已被篡改，但由于嵌入的水印信息未被改动，因此图像依然能够顺利通过认证，可见仅对水印信息加密并不能抵抗伪认证攻击. 本文结合图像 Zernike 矩幅值的半脆弱特性与水印信息，可以识别出这种攻击，分析如下：

水印图像遭受伪认证攻击后，因此时图像内容已被更改，故其矩幅值差异大于 τ，表明图像遭到恶意篡改，不过因伪认证攻击并不影响水印信息，此时水印差值图将会是一幅全黑的图像，表明图像并未被修改. 由这两种自相矛盾的结论即可断定图像受到伪认证攻击，故无法通过认证，从而提高了水印的安全性.

5.2 计算复杂度

我们以图像变换时所需的运算量来评估计算复杂度. 一幅图像进行 DCT 变换时，其运算量为 $O(n \cdot \log(n))$，而传统 DWT 则为 $O(n)$，传统 DWT 的计算量要低于 DCT. 对于 9-7 双正交整数小波变换，由式 (3) 和 (4) 可看出，在一维信号情况下，每计算两个小波系数，只需 7 个浮点乘法和 12 个整数加法，外加 7 个取整运算，而传统 9-7 双正交小波变换每计算两个小波系数需要 16 次浮点乘法和 14 次浮点加法，整数小波变换的运算量比传统 DWT 减少了一半多. 对于二维图像的小波变换，基于提升格式的整数小波变换的运算量则是传统 DWT 的四分之一. 可见采用基于提升格式的整数小波变换的计算复杂度要低于传统 DWT 和传统 DCT.

6 实验结果

(a) (b)

图 2 水印图像 (a) Baboon (PSNR 为 45.11dB)；(b) Pills (PSNR 为 45.54dB)

Fig. 2 Watermarked image (a) Baboon (PSNR=45.11dB); (b) Pills (PSNR=45.54dB)

为了测试本文所提出的算法的性能，实验中采用图 1 所示的 Baboon 及 Pills 两幅图像从水印不可见性、恶意篡改的定位能力及抗 JPEG 有损压缩能力三个方面进行评测，所嵌入的水印是大小为 64×64 的二值图像. 图 2 为 Baboon 和 Pills 的水印图像，与图 1 相应的原始图像相比视觉上无差异，其中 Baboon 水印图像的 PSNR (峰值信噪比) 为 45.11dB，Pills 水印图像的 PSNR 为 45.54dB. 图 3(a)、(e) 为对 Baboon 和 Pills 水印图像进行剪切操作，图 3(c)、(g) 为对 Baboon 和 Pills 水印图像进行替换操作，图 3(b)、(d)、(f)、(h) 为相应的水印差值图，可见本算法可以准确地定位篡改区域. 表 2 给

出了 Baboon 和 Pills 水印图像分别遭受 JPEG 有损压缩及图 3 所示的恶意攻击后的 LL_3 子带的矩幅值差异. 由表 2 可见，只需在一个区间内 (例如 200 ∼ 350) 任选一个值为阈值，即可将 JPEG 有损压缩与恶意攻击区分开，此结果也表明算法能容忍较低质量因子的 JPEG 有损压缩.

(a)　(b)

(c)　(d)

(e)　(f)

(g)　(h)

图 3　篡改检测 ((a)、(c) 、(e)、(g) 为被篡改的水印图像；(b)、(d)、(f)、(h) 为水印差值图)

Fig. 3　Tamper detection ((a)、(c) 、(e)、(g) Tampered image, (b)、(d)、(f)、(h) Difference image)

表 2　图像遭受恶意攻击及偶然攻击前后的 LL_3 子带的矩幅值差异

Table 2　Difference of Zernike moments magnitudes of LL_3 subband of an image before and after malicious and incidental attack

图像	JPEG90	JPEG70	JPEG50	JPEG40	Cut	Replace
Baboon	48.21	73.36	82.77	94.01	3691.50	549.18
Pills	34.18	57.62	88.58	112.37	3050.68	1781.45

7　结论

本文提出一种结合图像 Zernike 矩和水印的半脆弱图像认证算法，主要贡献如下：

1) 基于 HVS 实现水印的嵌入，使得因水印嵌入而导致的图像失真视觉上不可感知，保证了水印的不可见性.

2) 利用图像 Zernike 矩幅值的半脆弱特性将偶然攻击和恶意攻击区分开，结合用于认证的水印信息，可进一步判断出图像是否遭受伪认证攻击，提高了水印的安全性.

3) 采用基于提升格式的整数小波，在计算复杂度方面低于传统 DWT 和 DCT.

实验结果表明本算法能够容忍较低质量因子的 JPEG 有损压缩并且能够准确定位恶意篡改区域.

References

1 Zhu B B, Swanson M D, Tewfik A H. When seeing isn′t believing. *IEEE Transaction on Signal Processing Magazine*, 2004, **21**(2): 40∼49

2 Lin E T, Delp E J. A review of fragile image watermarks. In: Proceedings of the Multimedia and Security Workshop (ACM Multimedia ′99). Orlando: ACM Press, 1999. 25∼29

3 Kundur D, Hatzinakos D. Towards a telltale watermark techniques for tamper-proofing. In: Proceedings of the IEEE Internation Conference on Image Processing. IEEE, 1998. **2**: 409∼413

4 Lin C Y, Chang S F. Semi-fragile watermarking for authentication jpeg visual content. In: Proceedings of SPIE Security and Watermarking of Multimedia Content II. San Jose: SPIE Press, 2000. 140∼151

5 Han S J, Chang I S, Park R H. Semi-fragile watermarking for tamper proofing and authentication of still images. *Lecture Notes in Computer Science*, Springer, 2004, **2939**: 328∼339

6 Sweldens W. The lifting scheme: A custom-design construction of biorthogonal wavelets. *Journal of Applied and Computational Harmonic Analysis*, 1996, **3**(2): 186∼200

7 Daubechies I, Sweldens W. Factoring wavelet transforms into lifting steps. *Journal of Fourier Analysis and Applications*, 1998, **4**(3): 247∼269

8 Calderbank A R, Daubechies I, Sweldens W, Yeo B L. Wavelet transforms that map integers to integers. *Journal of Applied and Computational Harmonic Analysis*, 1998, **5**(3): 332∼369

9 Khotanzad A, Hong Y H. Invariant image recognition by Zernike moments. *IEEE Transaction on Pattern Analysis and Machine Intelligence*, 1990, **12**(5): 489∼497

10 Watson A B, Yang G Y, Solomon J A, Villasenor J. Visibility of wavelet quantization noise. *IEEE Transaction on Image Processing*, 1997, **6**(8): 1164∼1175

吴晓云 博士. 2006 年毕业于中山大学计算机软件与理论专业. 现为广东商学院信息学院讲师，主要研究多媒体信息安全，信息隐藏，数字水印.

(**WU Xiao-Yun** Received his Ph. D. degree in computer software and theory from Sun Yat-Sen University in 2006. He is now a lecturer in School of Information Science, Guangdong University of Business Studies. His research interests include multimedia security, data hiding, and digital watermarking.)

刘红梅 1996 年于清华大学计算机系获硕士学位, 2001 年于中山大学无线电物理专业获博士学位. 2002 年 11 月至 2003 年底在 ENIC, Lille 1, France 从事博士后研究工作. 现为中山大学副教授，研究领域包括信息隐藏，图像/视频水印及视频编码.

(**LIU Hong-Mei** Received her M. S. degree from Department of Computer Science, Tsinghua University, and Ph.D. degree in radiophysics from Department of Electronics, Sum Yat-Sen University in 1996 and 2001 respectively. From November 2002 to December 2003, she was at ENIC, Lille 1, France as a postdoctoral fellow. She is now an associate professor in Department of Electronics at Sun Yat-Sen University. Her research interests include information hiding, image/video watermarking, and video compression.)

黄继武 工学博士, IEEE 高级会员. 先后毕业于西安电子科技大学、清华大学、中国科学院自动化研究所. 现为中山大学电子与通信工程系教授、博士生导师. 主要研究方向为多媒体信息安全, 信息隐藏. 本文通信作者. E-mail: isshjw@mail.sysu.edu.cn

(**HUANG Ji-Wu** Received his B. S. degree from Xidian University in 1982, M. S. degree from Tsinghua University in 1987, and Ph. D. degree from Institute of Automation, Chinese Academy of Science in 1998 respectively. He is currently a professor in the School of Information Science and Technology at Sun Yat-Sen University. His research interests include multimedia security and data hiding. Corresponding author of this paper.)