基于 Harris 兴趣点和空域均值信息的图像复制粘贴窜改检测算法*

赵 洁[1,2], 武 斌[1], 张 艳[1,2]
(1. 天津城市建设学院 计算机与信息工程学院, 天津 300384; 2. 天津大学 电子信息工程学院, 天津 300072)

摘 要: 提出了一种基于兴趣点检测和特征匹配的图像复制粘贴窜改检测方法。首先采用 Harris 算子检测图像中的角点作为兴趣点,然后提取以兴趣点为中心的邻域内空域的五个均值特征形成特征向量,最后记录相等位移矢量的发生频率并通过阈值化处理得到匹配的兴趣点,从而标志复制粘贴区域。仿真实验表明,该算法不仅可以有效检测多区域复制粘贴窜改操作,而且能够有效抵抗多种窜改后处理操作,包括加性高斯白噪声,JPEG 压缩,对比度、亮度和曝光度调整以及 JPEG 压缩和加噪的混合操作。

关键词: 图像窜改检测; 复制粘贴; Harris; 兴趣点
中图分类号: TP391.41 **文献标志码**: A **文章编号**: 1001-3695(2013)09-2791-04
doi:10.3969/j.issn.1001-3695.2013.09.058

Detection algorithm of image copy-move forgery based on Harris and spacial average information

ZHAO Jie[1,2], WU Bin[1], ZHANG Yan[1,2]
(1. *School of Computer & Information Engineering, Tianjin Institute of Urban Construction, Tianjin* 300384, *China*; 2. *School of Electronic & Information Engineering, Tianjin University, Tianjin* 300072, *China*)

Abstract: This paper proposed a detection method of image copy-move forgery based on the interest points detection and feature matching. First, it applied Harris operator to detect corners as interest points, then extracted five spacial average features in the neighborhood of which as the center to constitute feature vector, and finally recorded the occurrence frequency of position transfer vector to obtain matching interest points with thresholding processing, thus marked copy-move regions. Experimental results show that the algorithm can not only detect multi-region copy-move manipulation effectively, but also be able to effectively resist various tampering post-processing operations, including additive white Gaussian noise, JPEG compression, contrast, brightness and exposure adjustment and the hybrid operation of JPEG compression and noise addition.

Key words: detection of image forgery; copy-move; Harris; points of interest

0 引言

数字时代造就了功能强大的图像编辑处理软件,使得普通用户可以很容易地修改一幅图像而不留下视觉痕迹,这彻底颠覆了传统眼见为实的观念。2007 年底至今,国内连续爆出了“华南虎”“藏羚羊”和“广场鸽”的造假事件,数字图像的恶意窜改对科学研究、司法取证、保险索赔和媒体公信力等方面造成了严重的负面影响,因此针对图像窜改的取证研究具有十分重要的现实意义。近年来,基于图像本身性质的盲取证技术由于不需要事先在图像中嵌入认证信息的独特优势,已经成为目前数字取证研究的热点方向之一。

复制粘贴是图像窜改最为常用的手段之一,是指复制图像中的一部分区域,将其粘贴到同一幅图像中的另一个不相交的区域上,从而达到遮蔽目标或伪造场景的目的。由于同一幅图像有着一致的噪声、纹理和颜色等信息,同时窜改者往往会在复制粘贴操作后进行边缘模糊、加噪、JPEG 压缩等后续操作,使得窜改图像更难以被人眼辨别。由于同幅图像的复制粘贴操作会在图像中引入两块或多块具有一定面积的相似区域,而自然物体纹理的多样性和光照的复杂变化决定了自然图像中出现相似区域的概率很小。因此,相似区域的存在可以作为图像复制粘贴窜改取证的依据。

近年来,国内外学者针对图像复制粘贴窜改进行了不少的有益探索,并且已经取得了一些成果。现有的复制粘贴窜改检测算法主要分为两类:

a)基于分块特征匹配的方法。文献[1~3]将图像分块后进行 DCT(discrete cosine transform),并采用变换后的 DCT 系数提取特征;文献[4,5]对小波变换后的低频分量分块提取奇异值特征;文献[6]提取图像块空域的七个鲁棒性特征来表征图像块,再采用主转移向量的方法去除错误的相似块来定位窜改区域。

b)基于兴趣点检测和特征匹配的方法。文献[7,8]采用 SIFT(scale invariant feature transform)[9]检测兴趣点,并对兴趣

收稿日期: 2012-12-19; **修回日期**: 2013-01-31 **基金项目**: 天津市高等学校科技发展基金计划资助项目(20120712);天津城市建设学院教育教学改革与研究项目(JG-1220)

作者简介:赵洁(1984-),男,天津人,讲师,博士研究生,主要研究方向为数字取证与图像处理(zhaoj@tju.edu.cn);武斌(1966-),男,教授,主要研究方向为现代显示技术与图像处理;张艳(1982-),女,讲师,博士研究生,主要研究方向为数字图像处理.

点周围邻域用适当的特征向量进行特征描述;文献[10,11]采用 SURF(speed up robust feature)[12] 检测和描述兴趣点,通过特征向量的匹配实现窜改区域的定位。

基于兴趣点检测和特征匹配的方法一般分为三个步骤,首先是兴趣点的识别和选择;然后采用适当的特征向量对每个兴趣点周围的邻域进行特征描述,并且描述子要有较好的区分性和鲁棒性;最后进行描述子的匹配,从而提取图像中对应的匹配点,实现相似区域的标志定位。现有的算法一般是基于 SIFT 和 SURF 检测兴趣点,计算复杂度高,检测的兴趣点多,而且提取的兴趣点在图像上并没有实际的物理特征,即非视觉上的角点。Harris 角点检测算子具有旋转不变性,并且对图像亮度和对比度变化不敏感,广泛应用于各种图像匹配算法中。本文提出了一种基于 Harris 兴趣点检测和特征匹配的图像复制粘贴窜改检测方法。仿真实验表明,该算法不仅能够有效检测并定位多区域复制粘贴窜改操作,而且可以对抗多种窜改后处理操作,包括加性高斯白噪声,JPEG 压缩,对比度、亮度和曝光度调整以及 JPEG 压缩和加噪的混合操作。

1 检测算法

Harris 算子是一种计算简单、应用广泛的角点检测算子,只使用灰度的一阶差分和滤波,可以定量地提取特征角点并且提取的角点特征均匀。由于计算过程用到图像的一阶导数,故对存在灰度变化、图像旋转、视点变换和噪声干扰的图像也能稳定地提取角点。因此本文提出的算法采用 Harris 角点作为兴趣点,并提取每个兴趣点为中心的邻域内空域的五个均值特征形成特征向量,通过位置转移向量的频率统计连接标志匹配点。

1.1 Harris 算子

Harris 算子检测角点的基本思想[13]是:在图像中假想一个局部窗口,当窗口沿各个方向移动时,如果窗口内区域的灰度发生了较大的变化,则认为窗口内遇到了角点。对于图像 $I(x,y)$,在点 (x,y) 处平移 $(\Delta x,\Delta y)$ 后的自相似性可以通过自相关函数表示为

$$c(x,y,\Delta x,\Delta y)=\sum_{(u,v)\in W(x,y)} w(u,v)(I(u,v)-I(u+\Delta x,v+\Delta y))^2 \tag{1}$$

其中:$W(x,y)$ 是以点 (x,y) 为中心的窗口,$w(u,v)$ 为高斯加权函数。通过泰勒公式展开,自相关函数可以近似为二次项函数:

$$c(x,y,\Delta x,\Delta y)\approx[\Delta x\ \Delta y]M(x,y)\begin{bmatrix}\Delta x\\ \Delta y\end{bmatrix} \tag{2}$$

其中:$M(x,y)=\sum_{u,v} w(u,v)\begin{bmatrix}I_x^2 & I_xI_y\\ I_xI_y & I_y^2\end{bmatrix}$,$w(u,v)=\exp(-\frac{u^2+v^2}{2\sigma^2})$ 为高斯窗函数在 (u,v) 处的系数;I_x、I_y 分别为图像在水平方向和垂直方向上的梯度。二次项函数本质上是一个椭圆函数,椭圆的扁率和尺寸由 $M(x,y)$ 的特征值 λ_1、λ_2 决定。Harris 给出的角点判别方法并不需要计算具体的特征值,而是计算一个角点响应函数 R 来检测图像的角点。

$$R=\det(M)-\alpha\,\mathrm{trace}^2(M) \tag{3}$$

式中:$\det(M)$ 和 $\mathrm{trace}(M)$ 分别为矩阵 M 的行列式和迹;α 为经验常数,一般取 0.04 ~ 0.06;R 表示像素点的 Harris 响应值,当某点响应值为邻域最大且大于一个阈值 R_0 时,确认该点为角点。

1.2 兴趣点的选择与特征描述子

本文算法采用 Harris 角点作为图像的兴趣点,设 $p_i(x_i,y_i)$ 为 Harris 算子检测得到的某一兴趣点,其中 (x_i,y_i) 为 p_i 在原始图像上的位置坐标。以 p_i 为中心取一个 $s\times s$ 大小的图像区域作为待描述区域,记录每个兴趣点邻域内(对于彩色图像则计算亮度分量)的五个空域均值特征组成特征向量 $V_i=(v_1,v_2,v_3,v_4,v_5)$。其中,$v_5$ 为 $s\times s$ 邻域内所有像素点的灰度平均值,v_1、v_2、v_3、v_4 分别记录该邻域内四个对角方向的特征,如图 1(图中取 $s=11$)所示。

$$v_i=\mathrm{sum}(\mathrm{part}(i))/\mathrm{sum}(\mathrm{part}(1)+\mathrm{part}(2)+\mathrm{part}(3)+\mathrm{part}(4))\quad i=1,2,3,4 \tag{4}$$

特征向量 $V_i=(v_1,v_2,v_3,v_4,v_5)$ 提取了以兴趣点 p_i 为中心 $s\times s$ 邻域的均值信息,同时描述了四个方向上的低频分量信息。下面对于加性高斯噪声的后处理操作进行理论分析。

设加性高斯白噪声 ε 均值为 0、方差为 σ^2,并且假设该噪声对于图像中的每个像素都是独立同分布的。记以 p_i 为中心的 $s\times s$ 的待描述区域为 B_i,则加噪后可以得到:

$$B_i^{\mathrm{AWGN}}=B_i+\varepsilon_{s\times s}=(I+\varepsilon)_{s\times s} \tag{5}$$

$$v_1^{\mathrm{AWGN}}=\frac{\mathrm{sum}(\mathrm{part}(1))+\varepsilon_1}{\mathrm{sum}(\mathrm{part}(1)+\mathrm{part}(2)+\mathrm{part}(3)+\mathrm{part}(4))+\varepsilon_2} \tag{6}$$

其中:$E(\varepsilon_1)=0$,$D(\varepsilon_1)\approx\frac{s^2}{4}\sigma^2$,$E(\varepsilon_2)=0$,$D(\varepsilon_2)\approx s^2\sigma^2$。在 AWGN 不太强的情况下,有下面不等式成立:

$$\mathrm{sum}(\mathrm{part}(1))>>\varepsilon_1$$
$$\mathrm{sum}(\mathrm{part}(1)+\mathrm{part}(2)+\mathrm{part}(3)+\mathrm{part}(4))>>\varepsilon_2 \tag{7}$$

因此,可以得到

$$v_1^{\mathrm{AWGN}}=\frac{\mathrm{sum}(\mathrm{part}(1))+\varepsilon_1}{\mathrm{sum}(\mathrm{part}(1)+\mathrm{part}(2)+\mathrm{part}(3)+\mathrm{part}(4))+\varepsilon_2}\approx\frac{\mathrm{sum}(\mathrm{part}(1))}{\mathrm{sum}(\mathrm{part}(1)+\mathrm{part}(2)+\mathrm{part}(3)+\mathrm{part}(4))}=v_1 \tag{8}$$

同理可以得到

$$v_2^{\mathrm{AWGN}}(v_3^{\mathrm{AWGN}},v_4^{\mathrm{AWGN}})\approx v_2(v_3,v_4) \tag{9}$$

$$v_5^{\mathrm{AWGN}}=\mathrm{mean}(B_i^{\mathrm{AWGN}})=\frac{\sum_{s\times s}(I+\varepsilon)}{s^2}=v_5+\varepsilon^* \tag{10}$$

其中:$\varepsilon^*\approx\frac{\sum\varepsilon}{s^2}$,可以得到 $E(\varepsilon^*)=0$,$D(\varepsilon^*)\approx\frac{\sigma^2}{s^2}$。因而 AWGN 加噪后与未处理前的特征相近,即 $v_5^{\mathrm{AWGN}}\approx v_5$。

特征向量 $V_i=(v_1,v_2,v_3,v_4,v_5)$ 对于加性高斯白噪声的后处理操作具有较好的鲁棒性。同样,由于 JPEG 压缩操作本质上相当于一个低通滤波器,虽然会丢弃图像的部分高频信息,但是基本不会影响低频信息和直流分量,因此所选特征对 JPEG 压缩的后处理操作也同样具有比较好的鲁棒性。

为了消除光照变换的影响,对特征向量进行归一化运算,即 $\frac{V_i}{\|V_i\|}\rightarrow V_i$。假设图像检测到的 Harris 兴趣点数目为 N_p,可以得到图像 $I(x,y)$ 的维数为 $N_p\times 5$ 的特征矩阵 V,其中 V_i 代表特征矩阵 V 的一行,(x_i,y_i) 为 V_i 对应 Harris 兴趣点的坐标值。

1.3 相似性匹配

将特征矩阵 V 进行字典排序,然后计算 V 中相邻两行对应的 Harris 兴趣点坐标值的位移矢量。假设 V 中相邻的两行对应的兴趣点位置为 (x_i,y_i),(x_{i+1},y_{i+1}),则对应的规范化位移矢量为

$$s=(s_1,s_2)=(|x_i-x_{i+1}|,|y_i-y_{i+1}|) \tag{11}$$

遍历字典排序后的特征矩阵 V 的每一行,计算相邻两行的规范化位移矢量,记录满足大于位移距离阈值 T_d 且相等的

位移矢量的发生频率,存储在频率计数器矩阵 C 中,即将对应的计数器元素自增 1:

$$C(s_1,s_2)=C(s_1,s_2)+1 \tag{12}$$

本文算法中进行相似性匹配时需要定义以下两个阈值:位移频率阈值 T_f 和位移距离阈值 T_d。T_f 限定相等位移矢量的匹配点的发生频率,T_f 越小,检测到的误匹配点数目会增加;T_d 限定特征矩阵 V 相邻两行的规范化位移矢量的大小,T_d 决定了算法检测到匹配点的最小距离。由于自然图像中相邻像素点的灰度值具有较强的相关性,因而 T_d 越小,检测到的误匹配点数目也会增加。若 $C(s_1,s_2)>T_f$,则认为检测到相应的匹配兴趣点,它们对应于图像中的复制粘贴区域,并对这些匹配点用不同颜色的线段进行连接标志。

1.4　算法的执行流程

算法首先采用 Harris 算子检测图像的角点作为兴趣点,然后分别提取每个兴趣点 $s\times s$ 邻域内五个空域均值特征形成特征向量,最后通过统计兴趣点之间相等位移矢量的发生频率确定匹配的兴趣点,从而实现复制粘贴区域的定位。具体算法的执行流程如下:

a)假设待检测的原始图像是一幅 $M\times N$ 的灰度图像(彩色图像则应用标准公式 $I=0.228R+0.587G+0.114B$ 转换为灰度图像),应用 Harris 算子检测图像的角点作为兴趣点。

b)设 $p_i(x_i,y_i)$ 为 Harris 算子检测得到的某一兴趣点,以 p_i 为中心取一个 $s\times s$ 大小的图像区域,如 1.2 节所述记录每个兴趣点邻域内的五个空域均值特征组成特征向量 $V_i=(v_1,v_2,v_3,v_4,v_5)$。

c)遍历字典排序后的特征矩阵 F 的每一行,计算相邻两行的规范化位移矢量 s,统计满足 $s>T_d$ 且 s 相等的位移矢量的发生频率,存储在频率计数器矩阵 C 中。

d)对于满足 $C(s_1,s_2)>T_f$ 的兴趣点则认为是一对匹配点,用线段连接所有的匹配点标志复制粘贴检测区域。

2　仿真实验与结果分析

2.1　实验环境与检测效果

实验中选取大小为 512×512 的灰度图像 Truck 作为测试图像,如图 2 所示。仿真环境为 Intel Pentium CPU P6200 2.13 GHz,MATLAB R2010b。窜改图像利用 Photoshop CS4 进行多目标复制粘贴处理得到,如图 3 所示。测试参数为 $\alpha=0.05$,$T_d=16$,$T_f=2$,$s=11$。

在没有进行任何后处理的情况下,利用本文算法得到的 Harris 兴趣点图像如图 4 所示,检测结果如图 5(a)所示,图中用不同颜色的线段连接检测到的匹配点说明相对应的两个图像区域为算法检测出的复制粘贴区域(见电子稿)。为了验证算法的鲁棒性,分别对窜改图像进行各种常见的后处理操作,如添加不同程度的高斯噪声,用不同的质量因子对其进行 JPEG 压缩,对比度、亮度和曝光度调整以及 JPEG 压缩和加噪的混合操作。应用本文算法的检测结果分别如图 5(b)~(i)所示。由于篇幅限制,这里只选取部分实验数据罗列。

从检测结果来看,正如前述理论分析一样,算法对于加性高斯白噪声的后处理操作即使 SNR 值下降到 20 dB 时,仍然可以有效检测出复制粘贴区域的匹配点;对于 JPEG 压缩的后处理操作即使质量因子 Q 下降到 50 时,仍然可以有效检测,并且对于两者混合操作具有一定程度的鲁棒性。这基本可以满足实际窜改取证的需要。试想如果是信噪比过低或者质量因子过小的窜改图像,由于肉眼就可以很直观地感受到噪声的存在,从而使人们直接质疑图像的来源和真实性,显然图像窜改者不会这么做。同时,实验表明,本文算法对于对比度、亮度和曝光度调整的操作同样具有比较好的鲁棒性,这主要是由于选取的特征向量提取了兴趣点邻域内的低频和直流分量数据,它们受上述后处理操作的影响很小。

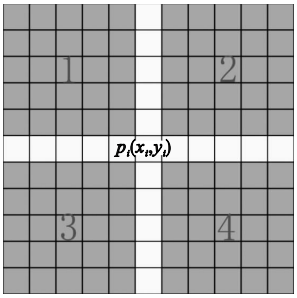
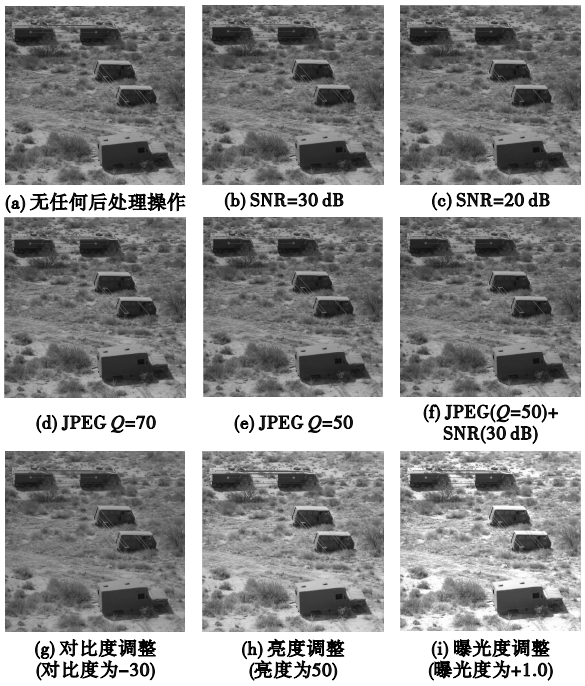


图1　Harris兴趣点$s\times s$邻域的特征描述模式(s=11)

图2　原始图像

图3　窜改图像

图4　Harris兴趣点图像



(a) 无任何后处理操作　(b) SNR=30 dB　(c) SNR=20 dB

(d) JPEG Q=70　(e) JPEG Q=50　(f) JPEG(Q=50)+SNR(30 dB)

(g) 对比度调整(对比度为-30)　(h) 亮度调整(亮度为50)　(i) 曝光度调整(曝光度为+1.0)

图5　本文算法的检测结果

2.2　算法对比分析

为了详细分析算法的优缺点,对窜改图像(图 3)分别应用本文算法与文献[7]算法进行对比实验,实验结果如表 1 所示。本文算法和文献[7]算法都属于基于兴趣点检测和特征匹配的图像复制粘贴窜改检测方法,但是文献[7]算法采用 SIFT 算法[9]提取兴趣点,通过尺度空间极值点检测和特征点位置精确确定的步骤,计算量较大,提取的兴趣点较多。从表 1 可知,本文算法的检测时间远远小于文献[7]算法,这里主要有两个原因:a)本文算法采用 Harris 算子提取图像的兴趣点,计算复杂度低,并且 Harris 算法提取的兴趣点数量远少于 SIFT 算法,因此减少了待匹配的兴趣点的数目,缩短了特征匹配的时间;b)本文算法对于每个兴趣点,只计算其邻域内空域的五个具有均值意义的特征,特征向量的维数较低,并且计算复杂度也较低,从而缩短了特征向量的匹配时间。相比文献[7]算法,本文算法对于大多数后处理操作具有较好的鲁棒性,仅仅对于旋转操作无效,而文献[7]算法也只对旋转 90° 的整倍数

有效。因此本文算法综合性能仍然较好,具有实用价值。

表 1 本文算法与文献[7]算法比较

算法	兴趣点数	匹配点	误匹配点数	检测时间/s
文献[7]算法($\omega=0.5$)	1 328	21	0	95.87
本文算法($T_d=16, T_f=2$)	993	24	0	9.46

3 结束语

针对图像窜改操作中最常见的复制粘贴窜改方式,本文提出了一种基于 Harris 兴趣点和空域均值信息的窜改检测方法。算法通过检测具有视觉意义的 Harris 角点作为兴趣点,并且提取其邻域内空域的五个具有均值意义的特征对兴趣点进行特征描述,大大降低了算法的时间复杂度。实验结果表明,算法不仅能够有效检测多区域复制粘贴窜改操作,并且能够有效抵抗高斯白噪声,JPEG 压缩,对比度、亮度和曝光度调整以及 JPEG 压缩和加噪的混合操作。然而,本文算法也有需要进一步研究和改进的地方,通过仿真实验观察,Harris 算子对于高斯模糊的后处理操作比较敏感,即高斯模糊会使 Harris 算子检测到的兴趣点数量大大减少,从而影响算法的检测结果。因此,在保持算法检测性能的同时,如何使算法对于更多的窜改后处理操作具有更强的鲁棒性是今后研究工作的方向。

参考文献:

[1] FRIDRICH J, SOUKAL D, LUKAS J. Detection of copy-move forgery in digital images[C]//Proc of Digital Forensic Research Workshop. Washington DC: IEEE Computer Society, 2003: 55-61.

[2] CAO Yan-jun, GAO Tie-gang, FAN Li, *et al*. A robust detection algorithm for region duplication in digital images [J]. International Journal of Digital Content Technology and its Applications, 2011, 5(6): 95-103.

[3] HUANG Yan-ping, LU Wei, SUN Wei, *et al*. Improved DCT-based detection of copy-move forgery in images[J]. Forensic Science International, 2011, 206(1-3): 178-184.

[4] LI Guo-hui, WU Qiong, TU Dan, *et al*. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD[C]//Proc of IEEE International Conference on Multimedia and Expo. 2007: 1750-1753.

[5] KANG Xiao-bing, WEI Sheng-min. Identifying tampered regions using singular value decomposition in digital image forensics[C]// Proc of International Conference on Computer Science and Software Engineering. Washington DC: IEEE Computer Society, 2008: 926-930.

[6] LUO Wei-qi, HUANG Ji-wu, QIU Guo-ping. Robust detection of region-duplication forgery in digital images[C]//Proc of the 18th International Conference on Pattern Recognition. 2006: 746-749.

[7] HUANG Hai-ling, GUO Wei-qiang, ZHANG Yu. Detection of copy-move forgery in digital images using sift algorithm[C]//Proc of Pacific-Asia Workshop on Computational Intelligence and Industrial Application. Washington DC: IEEE Computer Society, 2008: 272-276.

[8] AMERINI I, BALLAN L, CALDELLI R, *et al*. A SIFT-based forensic method for copy-move attack detection and transformation recovery [J]. IEEE Trans on Information Forensics and Security, 2011, 6(3): 1099-1110.

[9] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91-110.

[10] XU Bo, WANG Jun-wen, LIU Guang-jie, *et al*. Image copy-move forgery detection based on SURF[C]//Proc of International Conference on Multimedia Information Networking and Security. Washington DC: IEEE Computer Society, 2010: 889-892.

[11] SHIVAKUMAR B, SANTHOSH B. Detection of region duplication forgery in digital images using SURF[J]. International Journal of Computer Science Issues, 2011, 8(4): 199-205.

[12] BAY H, ESS A, TUYTELAARS T, *et al*. SURF: speeded up robust features[J]. Computer Vision and Image Understanding, 2008, 110(3): 346-359.

[13] HARRIS C, STEPHENS M. A combined corner and edge detector [C]//Proc of the 4th Alvey Vision Conference. 1988: 147-151.

(上接第 2790 页)

4 结束语

本文从安全性考虑,基于现实的需要提出了一个基于格的认证加密方案。该方案具有加解密速度快、密文扩展率低、安全性高等优势;提出的方案还存在许多需要改进之处,如提出一个格上可公开验证的认证加密方案,构造一个格上 CCA 安全性的认证加密方案,设计一个格上基于身份的认证加密方案,将其改进为一个效率更高的基于格的签密方案等。

参考文献:

[1] 李树栋. 一个新的可公开验证的认证加密方案[J]. 烟台职业学院学报, 2007, 13(2): 55 - 57.

[2] 林飞. 一种基于 RSA 的认证加密方案[D]. 广州: 暨南大学, 2000.

[3] 章磊, 卢建朱, 凌捷, 等. 一种新的基于多素数 RSA 认证加密方案[J]. 计算机应用研究, 2005, 22(5): 105-107.

[4] 黄益栓, 卢建朱. 一种基于身份的认证加密新方案[J]. 计算机工程, 2007, 33(7): 149-150.

[5] 蔡艳桃. 一种基于身份的认证加密方案的改进[J]. 计算机工程与应用, 2011, 47(15): 119-122.

[6] AJTAI M. Generating hard instances of lattice problems[C]//Proc of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 99-108.

[7] REGEV O. The learning with errors problem[EB/OL]. http:// www.cs. tau. ac. il/ ~ odedr/papers/lwesurvey. pdf.

[8] BLUM A, KALAI A, WASSERMAN H. Noise-tolerant learning, the parity problem, and the statistical query model [J]. Journal of the ACM, 2003, 50(4): 506-519.

[9] ARORA S, GE Rong. New algorithms for learning in presence of errors[C]//Proc of the 38th International Colloquim Conference on Automata, Languages and Programming, Volume Part I. 2011: 403-415.

[10] REGEV O. On lattices, learning with errors, random linear codes and cryptography [J]. Journal of the ACM, 2009, 56(6): 34.

[11] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]//Proc of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 1-23.

[12] MICCIANCIO D. Generalized compact knapsacks, cyclic lattices, and efficient one way functions [J]. Computational Complexity, 2007, 16(4): 411.

[13] LYUBASHEVSKY V, MICCIANCIO D. Generalized compact knapsacks are collision resistant[C]//Lecture Notes in Computer Science, vol 4052. Berlin: Springer-Verlag, 2006: 144-155.