

面向图像内容认证的半脆弱数字水印算法

吕林涛, 郝亮

(西安理工大学 计算机科学与工程学院, 西安 710048)

(lvtintao@xaut.edu.cn)

摘要:提出一种半脆弱数字水印算法,用于确认图像内容的真实性和完整性。算法首先将缩放图像的边缘作为特征信息,并对特征信息进行混沌调制和私钥加密得到水印信息;然后结合人类视觉系统将水印信息嵌入到载体图像的小波域中;最后用户利用公钥从水印图像中提取特征信息,并与重建的特征信息进行匹配来实现认证。实验结果表明:该算法对常规操作具有免疫性,对恶意处理能够实现准确认证和篡改定位。

关键词:半脆弱水印;特征信息;混沌序列;公钥;人类视觉系统

中图分类号:TP391 **文献标志码:**A

Semi-fragile digital watermarking algorithm for image content authentication

Lü Lin-tao, HAO Liang

(School of Computer Science and Engineering, Xi'an University of Technology, Xi'an Shaanxi 710048, China)

Abstract: A semi-fragile digital watermarking algorithm was proposed to verify the authenticity and integrity of image content. Firstly, the algorithm extracted the edge of the scaled image as the feature information, and the feature information was chaotically modulated and ciphered with the private key to generate watermark information. Secondly, the watermark information was embedded into the wavelet domain of the host image by using Human Visual System (HVS). Finally, a user could extract the feature information from the watermarked image with the public key, and compared it with the reconstructed feature information of the watermarked image to achieve authentication. The experimental results show that the proposed algorithm has the immunity to common image operation, and can also achieve accurate authentication and tampering localization to malicious processing.

Key words: semi-fragile watermarking; feature information; chaotic sequences; public key; Human Visual System (HVS)

0 引言

随着数字水印技术的发展,用于判断图像真实性问题的图像认证水印技术已成为当前研究的热点。近年来在图像认证水印技术研究上不断提出新的算法,如文献[1]利用视觉可觉察门限(Just Noticeable Difference, JND)对小波系数进行量化嵌入水印,通过比较提取的水印信息与原始水印信息的差值是否超过该点的JND数值实现篡改认证,但算法需保留原始水印信息才能进行图像认证。文献[2]将密码学中的公开密钥体制引入到图像认证水印技术中,使得图像认证更加实用化,但算法将水印嵌入在原始图像的最低有效位上,势必产生常规图像操作过于敏感问题。

针对上述及现有图像认证水印算法存在的不足,且考虑到实际应用中数字图像需要压缩存储和传输,用户又仅关心图像所要表达的内容信息等问题,本文提出一种面向图像内容认证的半脆弱数字水印算法。

1 数字水印生成和嵌入算法

1.1 数字水印生成和嵌入模型

本文提出的数字水印生成和嵌入算法构造过程为:1)提取缩放图像的边缘作为特征信息;2)对特征信息进行混沌调制和私钥加密生成水印信息;3)利用视觉感知模型将水印信息嵌入到小波系数中。其数字水印生成和嵌入模型如图1

所示。

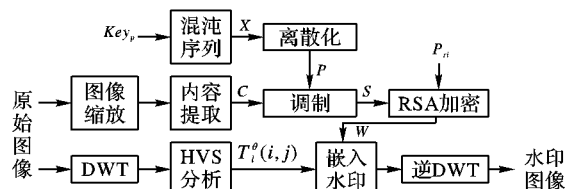


图1 数字水印生成和嵌入模型

1.2 数字水印生成算法

本文提出的基于图像内容的数字水印生成算法由产生缩放图像、提取量化特征信息、调制量化特征信息和非对称加密调制序列四阶段完成。各阶段详细描述如下。

Phase1:产生缩放图像。

设 $O = \{o(i, j) \mid 1 \leq i \leq M, 1 \leq j \leq M\}$ 为原始灰度载体图像,其中 $o(i, j)$ 代表原始载体图像的第 i 行、第 j 列像素的灰度值。产生缩放图像算法描述如下:

1)将 O 分成大小为 4×4 的不重叠的块 $O = \{o_1, o_2, \dots, o_{(M/4) \times (M/4)}\}$;

2)计算每个 4×4 的块 o_i 中像素的灰度均值 m_i , 其中 $i = 1, 2, \dots, (M/4) \times (M/4)$, 随后整合所有的均值 m_i 获得一个大小为 $(M/4) \times (M/4)$ 的缩放图像。

Phase2:提取量化特征信息。

为有效检测缩放图像的边缘特征,通过实验分析比较,本

文选用文献[3]的 Sobel 技术,若设 $m_i (i = 1, 2, \dots, (M/4) \times (M/4))$ 邻近的 8 个像素用 a, b, c, d, e, f, g 和 h 表示,如图 2 所示。

a	b	c
d	m_i	e
f	g	h

图2 像素编配图

则提取量化特征信息算法描述如下。

1) 由式(1)分别计算 m_i 的四个 Sobel 强度变化:水平强度变化 $E(H)$ 、垂直强度变化 $E(V)$ 、左对角强度变化 $E(LD)$ 和右对角强度变化 $E(RD)$ 。

$$\begin{cases} E(H) = (a + 2b + c) - (f + 2g + h) \\ E(V) = (c + 2e + h) - (a + 2d + f) \\ E(LD) = (d + 2f + g) - (b + 2c + e) \\ E(RD) = (b + 2a + d) - (e + 2h + g) \end{cases} \quad (1)$$

2) 由式(2)计算 m_i 的渐变度 $\nabla g(m_i)$ 。

$$\nabla g(m_i) = \sqrt{E(H)^2 + E(V)^2 + E(LD)^2 + E(RD)^2} \quad (2)$$

3) 根据 $\nabla g(m_i)$ 值,将 m_i 分为两类,即 $\nabla g(m_i) \geq T_0, m_i$ 归为边缘点; $\nabla g(m_i) < T_0, m_i$ 归为平滑点。由式(3)生成量化特征信息 $C = \{m_i' \mid i = 1, 2, \dots, (M/4) \times (M/4)\}$ 。

$$m_i' = \begin{cases} 1, & \nabla g(m_i) \geq T_0 \\ 0, & \nabla g(m_i) < T_0 \end{cases} \quad (3)$$

在式(3)中,如果 m_i 是边缘点,则 m_i' 为 1;如果 m_i 是平滑点,则 m_i' 为 0。另外, T_0 值的选取直接影响到特征信息的分布。 T_0 取值大,抗常规处理能力强,但图像特征信息体现不完整; T_0 取值小,图像特征信息丰富,但抗常规处理能力差。实验中 T_0 取值 200 效果较好。

Phase3: 调制量化特征信息。

调制可以改善水印信号的统计特性,减少水印信号嵌入时对原始图像的视觉影响。调制量化特征信息算法描述如下:

1) 利用 Logistic 映射^[24]简单且性能优异的特点生成实值混沌序列 $X = \{x(i) \mid i = 1, 2, \dots\}$, 其中 Logistic 迭代函数的初始值为 Key_p ;

2) 从实值混沌序列 X 中取 $(M/4) \times (M/4)$ 个元素并二值化生成二值混沌序列 $P = \{p(i) \mid p(i) \in \{0, 1\}, 1 \leq i \leq (M/4) \times (M/4)\}$, 且 P 仍具有实值混沌序列的优点。

3) 用二值混沌序列 P 对量化特征信息 C 进行混沌调制,生成调制序列 $S = \{s(i) \mid s(i) = p(i) \oplus m_i', 1 \leq i \leq (M/4) \times (M/4)\}$ 。

Phase4: 非对称加密调制序列。

鉴于水印信息数据量相对较少,选用 RSA 加密算法的私钥 P_n 加密调制序列 S 得到要嵌入的水印信息 W , 将水印信息二维表示为 $W = \{w(i, j) \mid w(i, j) \in \{0, 1\}, 1 \leq i \leq M/4, 1 \leq j \leq M/4\}$, 加密算法表示为 $W = E(S, P_n)$ 。

1.3 数字水印嵌入算法

由于小波变换在变换域信号处理中具有良好的局部空间频率分解特性,符合人类视觉系统 (Human Visual System, HVS)^[5], 同时满足最新的 JPEG2000 静态图像压缩标准^[6]。因此,本文采用小波变换技术实现数字水印嵌入算法。

实验发现,三级小波分解虽能提高鲁棒性,但嵌入水印后的图像会产生明显的失真;一级小波分解虽能满足不可感知性,但又会降低鲁棒性;二级小波分解综合了一级和三级的优

点。因此,本文在图像二级小波分解的低频子带上完成数字水印嵌入。数字水印嵌入算法通过量化、分类、嵌入和逆小波变换四步完成,其算法描述如下。

1) 量化。将子带 Y_2^{LL} 所含小波系数 $Y_2^{LL}(i, j)$ 用量化步长 Δ 量化,如式(4)所示:

$$q(i, j) = \left\lfloor \frac{Y_2^{LL}(i, j)}{\Delta} \right\rfloor \quad (4)$$

考虑到人类视觉系统,则式(4)中量化步长 Δ 值可由 Y_2^{LL} 的两个相邻子带 Y_2^{LH} 和 Y_2^{HL} 内相同位置的视觉感知特性值 $T_i^q(i, j)$ 计算求得,如式(5)所示:

$$\Delta(i, j) = \ln \frac{|T_2^{LH}(i, j)| + |T_2^{HL}(i, j)|}{2} \quad (5)$$

选择子带 Y_2^{LH} 和 Y_2^{HL} 更容易反映原始载体图像的纹理复杂情况,原始载体图像纹理越复杂,量化步长 Δ 值就越大,于是实现了嵌入强度与原始图像特征的自适应。视觉感知特性值 $T_i^q(i, j)$ 可由小波域的人类视觉系统感知模型求得,如式(6)所示:

$$T_i^q(i, j) = a(l, \theta) \times b(l, i, j) \times c(l, i, j)^{0.2} \quad (6)$$

其中 $a(l, \theta)$ 、 $b(l, i, j)$ 、 $c(l, i, j)$ 分别描述频率、亮度、纹理对视觉的影响,具体见文献[7]。

2) 分类。利用计算的 $q(i, j)$ 的值,将小波系数 $Y_2^{LL}(i, j)$ 分为两类:若 $\text{mod}(q(i, j), 2) = 0$, 则为 0 类;若 $\text{mod}(q(i, j), 2) = 1$, 则为 1 类。

3) 嵌入。如果嵌入的 $w(i, j)$ 与 $Y_2^{LL}(i, j)$ 的类别不一致,即 $\text{mod}(q(i, j), 2) \neq w(i, j)$, 则由式(7)求解使得 $Y_2^{LL}(i, j)$ 与 $w(i, j)$ 的类别一致;如果嵌入的 $w(i, j)$ 与 $Y_2^{LL}(i, j)$ 的类别一致,即 $\text{mod}(q(i, j), 2) = w(i, j)$, 则不对 $Y_2^{LL}(i, j)$ 做处理。

$$Y_2^{LL}(i, j) = \begin{cases} Y_2^{LL}(i, j) + \Delta, & Y_2^{LL}(i, j) < 0 \\ Y_2^{LL}(i, j) - \Delta, & Y_2^{LL}(i, j) \geq 0 \end{cases} \quad (7)$$

4) 逆小波变换。用含有水印信息的小波系数 $Y_2^{LL}(i, j)$ 代替 $Y_2^{LL}(i, j)$, 并结合未修改的小波系数进行二级逆小波变换,得到含水印信息的图像。

2 数字水印提取及认证算法

2.1 数字水印提取及认证模型

本文提出的数字水印提取及认证算法的构造过程为:

1) 用户从水印图像中提取水印信息;2) 将水印信息用公钥解密,并用混沌序列解调得到解调后的特征信息;3) 将解调后的特征信息与重建的特征信息进行匹配来实现认证。其数字水印提取及认证模型如图 3 所示。

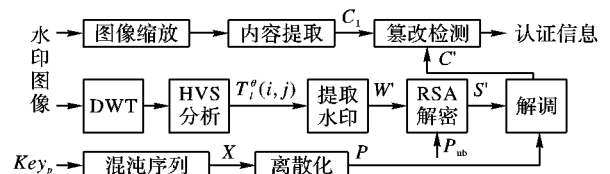


图3 数字水印提取及认证模型

2.2 数字水印提取算法

本文提出的数字水印提取算法通过量化和提取两步完成,其算法描述如下。

1) 量化。对待检测图像 O' 进行二层小波变换。将子带 Y_2^{LL} 的小波系数量化,如式(8)所示:

$$q'(i, j) = \left\lfloor \frac{Y_2^{LL}(i, j)}{\Delta'} \right\rfloor \quad (8)$$

其中量化步长 Δ' 为:

$$\Delta'(i, j) = \ln \frac{|T_2^{LU}(i, j)| + |T_2^{ML}(i, j)|}{2} \quad (9)$$

2) 提取。水印信息 W' 提取方法可表示为:

$$w'(i, j) = \begin{cases} 0, & \text{mod}(q'(i, j), 2) = 0 \\ 1, & \text{mod}(q'(i, j), 2) = 1 \end{cases} \quad (10)$$

其中 $w'(i, j) \in W', i = 1, 2, \dots, M/4, j = 1, 2, \dots, M/4$ 。

2.3 数字水印认证算法

本文提出的数字水印认证算法通过篡改定位和篡改认证两步完成,其算法描述如下。

1) 篡改定位。首先用 RSA 公钥 P_{ub} 对 W' 进行解密得到调制序列 $S' = D(W', P_{ub})$, 并利用 Key_p 生成的二值混沌序列 P 对 S' 进行解调, 得到量化的特征信息 C' ; 接着重建基于图像内容的量化特征信息 C_1 , 求得篡改矩阵 $W^* = C' \oplus C_1$; 最后对篡改矩阵 W^* 进行 2×2 中值滤波来消除常规图像操作引起的篡改区域, 便可通过篡改矩阵 W^* 确定篡改发生的位置。

2) 篡改认证。将已中值滤波的篡改矩阵 W^* 划分成 $n \times n$ 的子块, 计算每个子块的篡改比率 $R^*(u, v)^{[8]}$ 为:

$$R^*(u, v) = \frac{\sum_{x=1}^n \sum_{y=1}^n w^*((u-1)n+x, (v-1)n+y)}{n \times n} \quad (11)$$

其中: $u = 1, 2, \dots, M/(4 \times n); v = 1, 2, \dots, M/(4 \times n); w^*((u-1)n+x, (v-1)n+y) \in W^*$ 。计算最大篡改比率 $\tilde{R}^* = \max_{u,v}(R^*(u, v))$, 并选取检测阈值 T , 以区分常规操作与恶意处理; 如果 $\tilde{R}^* = 0$, 则未遭受任何攻击; $\tilde{R}^* \leq T$, 则为常规操作; $\tilde{R}^* > T$, 则为恶意处理。

3 实验结果比对与分析

本文实验采用原始载体图像为 512×512 的灰度 Lena 图, 混沌序列的初始值 Key_c 选取 0.4123, 小波变换采用 Haar 小波基^[9], $n \times n$ 选取 8×8 。实验测试了算法的透明性、脆弱性、鲁棒性和有效性。

3.1 嵌入水印后的透明性测试与分析

为测试算法嵌入水印后的透明性, 图 4 给出了 Lena 图嵌入水印实验结果, 其水印图像峰值信噪比 (Peak Signal to Noise Ratio, PSNR)^[10] 为 45.1599 dB。实验结果表明, 水印图像满足透明性要求。

3.2 恶意处理下的脆弱性测试与分析

为测试算法在恶意处理下的脆弱性, 本文对水印图像分别进行了替换和剪切测试, 图 5 为替换 Lena 图后的篡改检测结果, 图 6 为剪切 Lena 图后的篡改检测结果。

另外, 本文还选取原始载体图像为 512×512 的灰度 Barbara 图、Peppers 图和 Baboon 图进行测试。表 1 给出了恶意处理下篡改比率 \tilde{R}^* 的测试结果。取 $T = 0.4, \tilde{R}^* > T$ 的认为是恶意处理。实验结果表明, 该算法对恶意处理能够准确认证并篡改定位。

表 1 恶意处理下篡改比率 \tilde{R}^* 的测试结果

篡改方式	Lena 图	Barbara 图	Peppers 图	Baboon 图
替换	0.5469	0.7969	0.6094	0.6875
剪切	0.9063	0.8281	0.7344	0.7813

3.3 常规操作下的鲁棒性测试与分析

为测试算法在常规操作下的鲁棒性, 本文对选取的 4 张水印图像进行了 JPEG 压缩、叠加噪声和滤波等常规操作。图 7 给出了常规操作下篡改比率的测试结果。

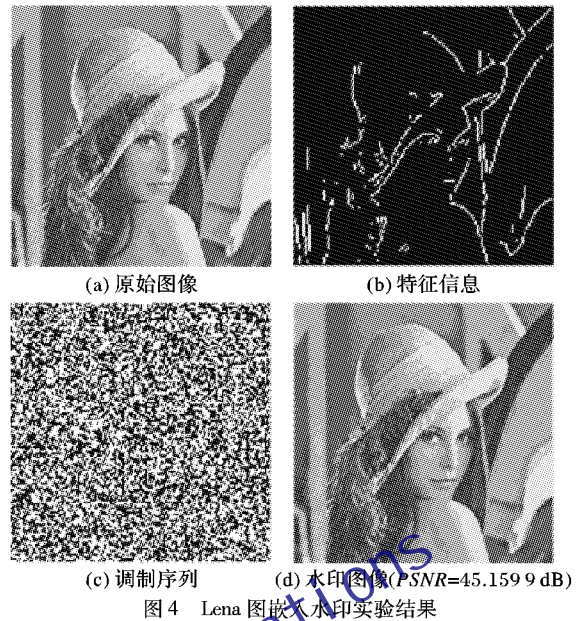


图 4 Lena 图嵌入水印实验结果

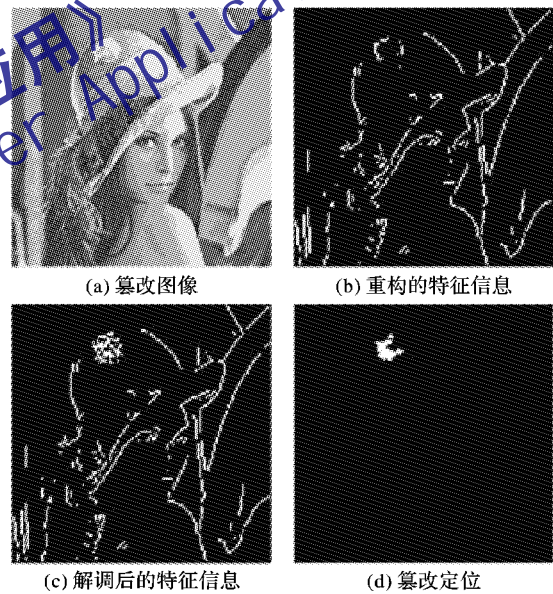


图 5 替换 Lena 图后的篡改检测结果

由图 7 中数据得知, 常规操作下篡改比率 \tilde{R}^* 的值均小于 0.4。为区分常规操作与恶意处理, 本文取检测阈值 $T = 0.4$ 。实验结果表明, 本算法具有准确区分常规操作与恶意处理的能力。

3.4 水印算法的有效性测试与分析

为测试算法的有效性, 将本文算法与文献[11]进行比较, 所用到的载体图像均为灰度 Lena 图。比较结果见表 2。

表 2 与其他算法的性能比较

水印算法	载体图像大小	水印大小	PSNR/dB
文献[11]	512×512	64×64	43.5600
本文算法	512×512	128×128	45.1599

由表 2 可知, 虽然本文算法和文献[11]的 PSNR 值基本接近, 但水印嵌入容量要远大于文献[11]。由此可见, 本文

算法不仅能够提高恶意处理的检测精度,而且可以增强常规操作的免疫性能。

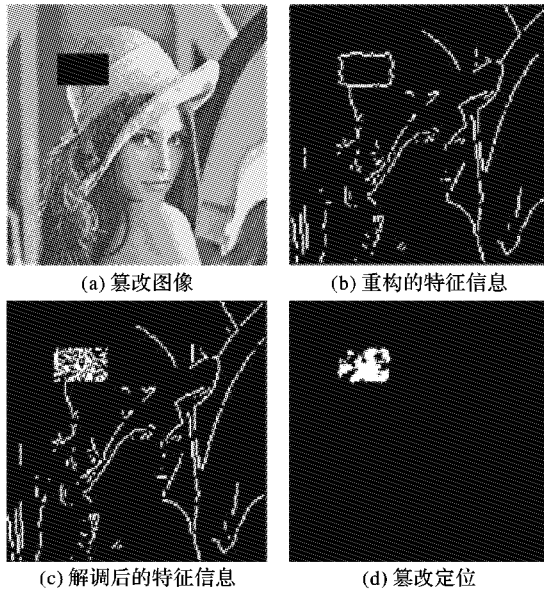
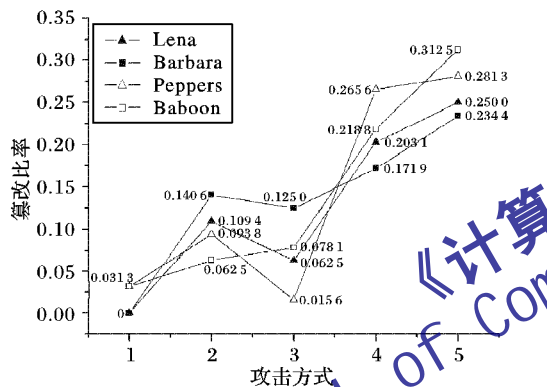


图6 剪切 Lena 图后的篡改检测结果



注: 横坐标中1表示JPEG压缩90%; 2表示JPEG压缩80%; 3表示椒盐噪声1%; 4表示高斯噪声 $\sigma=30$; 5表示中值滤波 4×4 。

图7 常规操作下篡改比率 \tilde{R}^* 的测试结果

4 结语

本文在研究图像认证水印技术的基础上,提出了一种面向图像内容认证的半脆弱数字水印算法。该算法以小波变换为基础,结合混沌理论与非对称加密体制,构造基于图像内容

的数字水印。嵌入和认证时分别采用了私钥和公钥,拥有公钥的用户在对图像进行认证后,因缺少私钥而不能再对图像进行伪造,提高了数字水印的安全性和实用性;采用视觉感知模型来量化嵌入水印,提高了数字水印的透明性。实验结果表明,该算法对常规操作免疫,对恶意处理能够准确判断并篡改定位。

参考文献:

- [1] LU C-S, LIAO H-F M. Multipurpose watermarking for image authentication and protection [J]. IEEE Transactions on Image Processing, 2001, 10(10): 1579-1592.
- [2] WONG P W. A public key watermark for image verification and authentication [C]// ICIP 98: Proceedings of the IEEE International Conference on Image Processing. Washington, DC: IEEE Press, 1998, 1: 455-459.
- [3] CHANG C-C, LIN P-Y. Adaptive watermark mechanism for rightful ownership protection [J]. Journal of Systems and Software, 2008, 81(7): 1118-1129.
- [4] 李剑, 李生红, 孙铁锋. 基于 Logistic 混沌序列和奇异值分解的半脆弱水印算法 [J]. 上海交通大学学报, 2009, 43(7): 1144-1154.
- [5] QI HUIYAN, ZHENG DONG, ZHAO JIXING. Human visual system based adaptive digital image watermarking [J]. Signal Processing, 2008, 88(1): 174-188.
- [6] SUN QIBIN, CHANG S-F, KURATO M, et al. A quantitative semi-fragile JPEG2000 image authentication system [C]// ICIP 02: Proceedings of the IEEE International Conference on Image Processing. Washington, DC: IEEE Press, 2002, 2: 921-924.
- [7] 王振飞, 施保昌, 王能超. 基于小波变换和人类视觉系统的稳健水印算法 [J]. 华中科技大学学报: 自然科学版, 2007, 35(1): 26-28.
- [8] 王向阳, 杨红颖, 侯丽敏. 一种新的半脆弱彩色图像数字水印算法 [J]. 自动化学报, 2007, 33(6): 561-566.
- [9] 刘九芬, 黄达人, 胡军全. 数字水印中的正交小波基 [J]. 电子与信息学报, 2003, 25(4): 453-459.
- [10] 王国栋, 刘粉林, 刘媛, 等. 一种能区分水印或内容篡改的脆弱水印算法 [J]. 电子学报, 2008, 36(7): 1349-1354.
- [11] SUN RUI, SUN HONG, YAO TIANREN. A SVD- and quantization based semi-fragile watermarking technique for image authentication [C]// Proceedings of the 6th International Conference on Signal Processing. Washington, DC: IEEE Press, 2002, 2: 1592-1595.

(上接第1238页)

4.2 权能验证实现

实现权能验证钩子函数 `check_key_capability` 放置在 eCryptfs 文件系统的相应位置,比如 Open 操作,对所有访问内核密钥环的请求进行检测,达到只有合法用户能够访问的目的。

5 结语

存储安全在信息安全中扮演着越来越重要的角色。加密文件系统像其他存储安全机制一样能出色地完成脱机情况下的数据保护,不足在于:在多用户环境下,不能提供联机的数据保护。本文分析了造成 eCryptfs 这种不足的主要原因,指出了采用自主访问控制解决方法的不足,提出了基于密钥权能的访问机制,设计和实现了多用户加密文件系统,满足多用户环境下联机数据保护的目的,即使是系统的超级用户在联

机环境下也无法看到用户的密文数据,要访问密文数据必须提供合法的密钥权能。

参考文献:

- [1] 徐国栋,白英彩. 加密文件系统在 Windows 下的实现 [J]. 微型电脑应用, 2006, 22(5): 56-58.
- [2] 沈士根. EFS 的研究与安全性分析 [J]. 微计算机信息, 2006, 22(24): 96-98.
- [3] ZADOK E, BADULESCU I, SHENDER A. Cryptfs: A stackable vnode level encryption file system, CUCS-021-98 [R]. New York: Columbia University, Computer Science Department, 1998.
- [4] HALCROW M A. eCryptfs: An enterprise-class cryptographic file-system for Linux [EB/OL]. [2009-08-22]. <http://www.dubeyko.com/development/FileSystems/eCryptfs/ecryptfs.pdf>.
- [5] IEEE/ANSI Draft Std. 1003.1e. Draft standard for information technology - POSIX Part 1: System API: Protection, audit and control interface [S]. IEEE, 1997.