基于 Jerk 系统的彩色图像加密算法 *

陈国林[a], 张 卫[a,b†], 刘金梅[a,b]

(暨南大学 a. 信息科学技术学院; b. 暨南大学—喀山联邦大学信息技术及分形信号处理联合实验室, 广州 510632)

摘 要: 提出了一种用三维 Jerk 系统对彩色图像加密的算法。首先对 Jerk 系统输出的混沌序列进行预处理,使其成为更为理想的伪随机序列;其次用得到的混沌序列对图像进行行、列置乱变换;最后再用混沌序列对置乱后的图像进行扩散,完成加密。此外,在解密中利用原图像相邻像素的相关性增强了算法的抗攻击能力。仿真结果表明,Jerk 系统产生的混沌序列有理想的伪随机性,该加密算法可以达到很好的加密效果,并具有较强的抗攻击性能。

关键词: 混沌; Jerk 系统; 混沌加密; 彩色图像加密; 安全性分析

中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2012)01-0312-04

doi:10.3969/j.issn.1001-3695.2012.01.086

Color image encryption algorithm based on Jerk system

CHEN Guo-lin[a], ZHANG Wei[a,b†], LIU Jin-mei[a,b]

(*a. College of Information & Science Technology, b. Joint-Lab of Jinan University—Kazan Federal University, Jinan University, Guangzhou* 510632, *China*)

Abstract: This paper presented an image encryption scheme based on a three dimensional Jerk system. Firstly, the method preprocessed chaotic sequences from the Jerk system for better randomness. Then, used the sequences to shuffle the positions of image pixels. Finally, diffused the shuffled image by virtue of the chaotic sequences. And utilized the correlation of adjacent pixels to enhance anti-attack capability of the algorithm in decryption process. Simulation results indicate that the method has good effect of encryption and strong performance of security.

Key words: chaos; Jerk system; chaotic encryption; color image encryption; security analysis

随着网络技术的快速发展,为了信息传输安全,大量的加密方法得到长足的发展。1989 年英国数学家 Matthews[1] 首次明确提出混沌加密。混沌系统应用于图像加密,是 Fridrich[2] 于 1997 年首先提出的,此后混沌加密成为学者们研究的热点。

混沌加密算法以非线性动力学中的混沌现象为理论基础,因其对初值的高度敏感性、本身的非线性和不可确定性而应用于信息加密中。近年来人们提出了许多关于混沌系统对图像加密的方法[3~9]。在文献[3]中,提出一种 logistic 映射产生的混沌序列控制图像中像素循环置乱的加密方法;在文献[4, 6]中,提出用二维混沌映射产生的序列分别对灰度图像进行置乱和扩散,实现加密;在文献[9]中彩色图像变换到三维立方体,置乱和扩散结合到一起处理,用三维 Lorenz 系统产生的混沌序列进行直接加密。低维混沌存在密钥空间小、安全性不高的缺点,因此本文用三维 Jerk 系统产生的混沌序列对图像加密。该系统结构简单,密钥空间大,可产生多个混沌序列,方便彩色图像加密;与 Lorenz 等三维系统相比,其有更突出的伪随机性。并且目前 Jerk 系统尚未被用于图像加密中,所以研究其在图像加密中的应用很有意义。

1 混沌模型

在图像加密过程中,优秀的系统所产生的混沌序列随机性会更好,这也就决定了所加密图像的保密性更强。本文所用的混沌系统是 Jerk 系统,系统方程为

$$\begin{cases} \dfrac{dx}{dt} = y \\ \dfrac{dy}{dt} = z \\ \dfrac{dz}{dt} = ay - z + bx^2 + c \end{cases} \tag{1}$$

其中:a、b、c 为系统参数,a、b、c 取不同的值时,系统表现为不同的状态,a、b、c 在特定的范围内时,选取合适的初始值后,系统经过过渡阶段后进入混沌状态,其相图如图 1 所示。

2 产生伪随机序列

首先给定 Jerk 系统的初始值 $x_0 = 0$, $y_0 = 0$, $z_0 = 0$,定制参数 $a = -0.62$, $b = 0.165$, $c = 1.98$,迭代 5 万次后,使之运行在混沌状态,截取 n 个值进行分析。按照 Golomb 在 1967 年对伪序

收稿日期: 2011-05-14; **修回日期**: 2011-06-20 **基金项目**: 广东省科技计划省国际合作项目(2010B050900016);暨南大学科研培育与创新基金研究国际合作研究项目(21609606)

作者简介:陈国林(1987-),男,河南信阳人,硕士研究生,主要研究方向为图像加密、图像处理(guolinchen@yeah.net);张卫(1959-),男(通信作者),安徽合肥人,研究员,博导,主要研究方向为信号分析与处理理论与技术;刘金梅(1975-),女,山东昌乐人,博士,主要研究方向为混沌与保密通信、网络信息安全.

列随机性提出的三点公设,理想混沌序列应具备以下统计特性:均匀分布;自相关为 δ 函数,互相关为零。通过对 Jerk 系统所产生混沌序列的分析发现,序列值域为 $-6.6977 < x < 4.6968$, $-3.9088 < y < 5.9766$, $-4.4827 < z < 5.8368$,均值为 $x = -1.6022$, $y = 0.00026320$, $z = 0.0014$,互相关最大值为 0.7520,结果如图 2 所示。伪随机的特征还不够理想,需要用式(2)对产生的混沌序列进行有效的预处理[10],使之成为更理想的伪随机序列。

$$x_i = 10^k x_i - \mathrm{round}(10^k x_i) \tag{2}$$

其中:x 表示混沌序列;round(x)为取最接近整数运算。

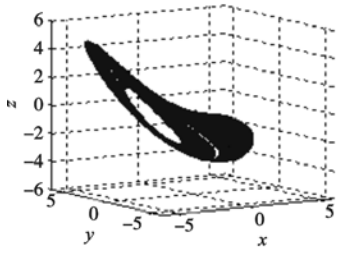


图1　Jerk系统进入混沌状态的相图

通过这样的预处理,所得到的混沌序列值域映射到(−1,1),其均值为 $x = -5.0014e-005$, $y = 7.6904e-005$, $z = 4.5304e-004$,自相关次峰值为 0.0060,互相关最大值为 0.0057,非常接近于 0。自相关和互相关特性如图 2 所示,比文献[11]中的混沌序列的相关特性更小,表现出了极为理想的伪随机性。

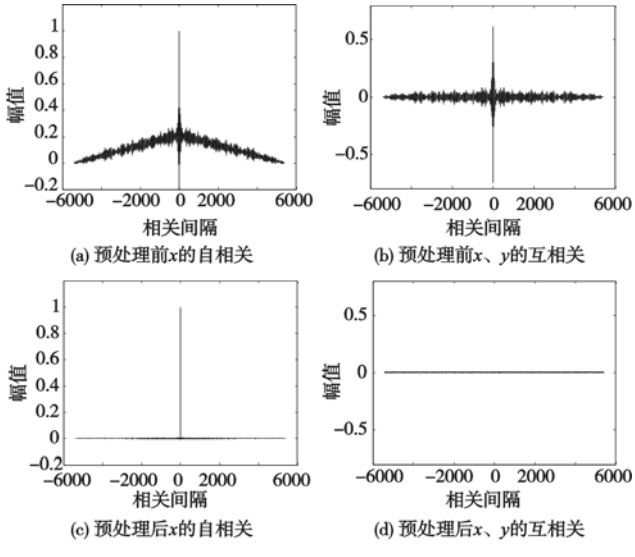


图2　预处理前后x的自相关和x、y的互相关

3　加密算法

彩色图像是由 R、G、B 三部分组成,所以对于一个大小为 $M \times N$ 的彩色图,在 MATLAB 中是一个 $M \times N \times 3$ 的多维数组。一幅图像在空间域可以用位置和像素值这两种信息进行描述,因此,基于空间域的图像加密是在这两种最基本信息上来设计加密算法的。

3.1　图像置乱

图像的相邻像素有很强的相关性,为了打乱这种强相关性,可以用像素置乱的方法处理原图像,以达到加密效果。图像置乱步骤如下:

a)把一幅彩色图像 im(M,N,3)转换为 R、G、B 三个层次的二维矩阵,再把二维矩阵各自按行转换为一维数组 imRs(L)、imGs(L)、imBs(L),其中 $L = M \times N$。

b)选择适当的参数和初始值作为密钥一部分,得到三组预处理的混沌序列 x、y、z,从序列中分别截取长度为 L 的混沌序列 $x(L)$、$y(L)$、$z(L)$,并分别按从大到小或从小到大的顺序排列,从中得到排序值在原序列中的位置索引数组 D。

c)根据步骤 b)得到的 $D(di)$,对原图像转换的数组进行排列,用 D 中的值作为数组的地址,把 $D(di)$ 分成 4 段,4 段都依次对原图序列置位,如第 1 段按照 imRs1($n+3$) = imRs($D(di)$),其中 $n = (1,4,7,\cdots,L-3)$, $di = (1,2,\cdots,L/4)$。同样得 imGs1、imBs1。

d)把新得到的 imRs1、imGs1、imBs1 三个序列排列成二维矩阵 imR(M,N)、imG(M,N)、imB(M,N)。

e)把步骤 d)得到的二维矩阵按列展开为一维序列 imRs2(L)、imGs2(L)、imBs2(L),在混沌序列中分别取另一段长度为 L 的序列 $x2(L)$、$y2(L)$、$z2(L)$,再用上面的步骤 b) ~ d)进行置乱,将所得到的序列再排列为矩阵形式,就得到 imRR(M,N)、imGG(M,N)、imBB(M,N)。

3.2　图像扩散

图像扩散是按一种算法改变像素值来完成图像加密,算法步骤如下:

a)选取合适的参数和初始值,Jerk 系统产生混沌序列 x、y、z,去除过渡序列,从混沌序列中分别截取一段长度为 $2L$ 的混沌序列 $x(2L)$、$y(2L)$、$z(2L)$。

b)取混沌序列 $x(2L)$、$y(2L)$、$z(2L)$的奇数位组成序列 $x(L)$、$y(L)$、$z(L)$,再将序列值按照式(3)映射到[0,255]区间上,转换为 Uint8 格式数据 xu8(L),yu8(L),zu8(L);再排列成 $M \times N$ 的矩阵形式,得到 xu(M,N)、yu(M,N)、zu(M,N)。

$$x = \mathrm{int}(\mathrm{mod}(x,1) \times 255) \tag{3}$$

c)原图像 R 层经过置乱得到 imRR(M,N),按照式(4)得到值 $D \in [0,2]$,D 的三个值将分别对应 xu(M,N)、yu(M,N)、zu(M,N),imRR(M,N)中每一个像素根据其 D 值分别与相应混沌序列中的值进行异或运算(如 imRR(i,j)的 $D = 1$ 时,将与 yu(i,j)进行异或)完成 R 层加密。同样可得到 G、B 层的加密图像,最终组合成加密后的图像 imm(M,N,3)。

$$D = \mathrm{mod}(\mathrm{imRR}(i,j),3) \tag{4}$$

对加密后的完整密文进行常规解密就是其加密过程的逆过程,只要在同一个系统下,选用加密时所用的密钥,即可得到加密前的原图像。

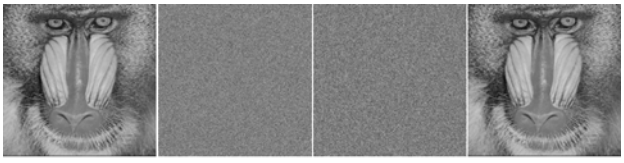
4　抗攻击的解密算法

考虑到密文在传送中可能受到攻击或干扰,本文提出了一种可抗一定范围攻击的解密算法,该算法的可靠性依据是加密算法的像素置乱和扩散的均匀性,以及图像相邻像素之间的高度相关性。由于密文的相邻像素基本不相关,并且在解密过程中被攻击部分将均匀分布到整个图像上,所以可用原图像相邻像素的相关性来修复被攻击图像,从而得到更完好的原图像。

方法是:被攻击密文经过常规解密后得到图像 imm,取 imm(i,j)像素值与其周围 8 个像素值;根据相关性,选其中差值较小的 3 个值,计算其均值 Q,再把 imm(i,j)与 Q 比较,当差值大于 K 时,用 Q 取代 imm(i,j)。其中 K 是根据原图的色彩变化所取的阈值,当色彩变化快时 K 值增大,当色彩变化缓慢时 K 值减小,如此可以得到解密的原图像。

5　实验结果

选用大小为 512 ×512 ×3 的彩色图像 Baboon. bmp 作为实验图片,仿真结果如图 3 所示。图 3(a)是原始彩色图像;(b)是置乱后的图像;(c)是加密后的图像。在同一混沌系统下用相同的密钥对加密后图像(c)进行解密操作,可得到解密后的图像(d)。



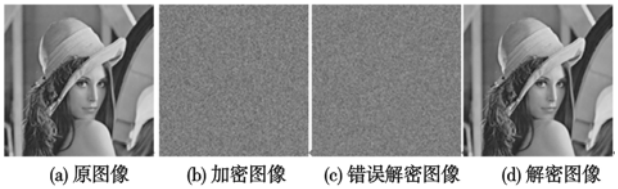
(a) 原始图像　(b) 置乱图像　(c) 加密图像　(d) 解密图像

图3　实验结果图像

6　实验结果分析

6.1　密钥敏感性分析

密钥敏感性测试结果如图 4 所示。其中,(a)为原图像 Lena;(b)是加密密钥为 $x=0.2, y=0.1001, z=0$ 时的加密图像,当解密密钥与加密密钥完全一致时,加密图像可得到完全解密,如(d)所示;当任选一解密密钥 $x=0.2, y=0.1001, z=0.000000000000001$ 时的解密图像如(c)所示,仍为无序图像。密钥敏感性测试的结果表明,经过本文加密算法得到的加密图像,在对其解密时,只有解密密钥与加密密钥完全一致时才能得到完全解密的原图像;而当解密密钥值有 10^{-16} 的微小变化时,完全得不到原图像信息。所以,本算法对密钥有极强的敏感性。



(a) 原图像　(b) 加密图像　(c) 错误解密图像　(d) 解密图像

图4　密钥敏感性分析

6.2　密钥空间分析

为应对穷举攻击,加密方案应该具有尽可能大的密钥空间。混沌系统有 3 个控制参数和 3 个初始值。使用这 6 个值作为密钥,MATLAB 中默认计算精度为 10^{-16},密钥对 10^{-16} 的微小变化敏感,所以加密系统的密钥空间为 10^{96}($\approx 2^{319}$)。再考虑选取序列的位置以及图像大小的条件,或者加大计算精度,密钥空间将远大于 2^{319},这使穷举攻击几乎不可能成功。

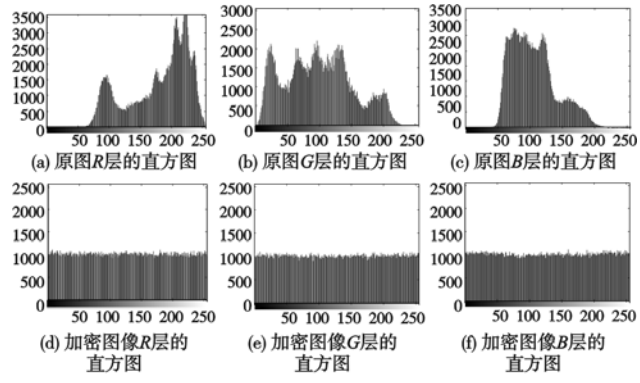
6.3　统计分析

1)灰度直方图　直方图是图像的重要统计特征,它直观地反映了数字图像的每一灰度级与该灰度级出现频率的对应关系。图 5(a)~(c)是原始图像的各层灰度直方图,(d)~(f)则对应密文图像的各层灰度直方图。由图 5 可见,密文与明文的直方图区别很大,密文的直方图分布非常均匀,表明该方案能够有效抵御基于像素值统计的攻击。

2)相邻像素的相关性　由于一幅图像中相邻像素间存在较大的相关性,这使攻击者容易对图像进行加密分析,因而优秀的加密算法应当有效地打乱这种相关性,使相关系数接近零。这里在 Lena 原图像和加密图像中选取 2 000 个相邻像素点,其分布的相关性如图 6 所示。可见,原图像像素间相关性表现出明显的线性分布,而加密图像像素间的相关性呈现随机分布。再用式(5)对两图像在垂直、水平和对角线三个方向的相关系数进行计算,将计算结果和同样使用三维混沌系统的文献[12,13]的结果相比较,结果如表 1 所示。其中第一行的 Lena 相关系数为本文算法所得,另两行来自文献,结果表明本算法所得密文的相邻像素的相关性更小。表 2 所列出的是 Lena、Baboon、Peppers 原图像与其各自加密图像在 R、G、B 层上的相关系数,结果表明原图像和加密图像之间的相关性非常小。

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{5}$$

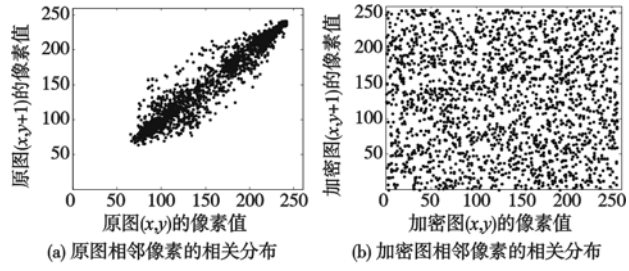
其中,$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{k=1}^{N}(x_k-E(x))(y_k-E(y))$;$x$、$y$ 为图像中相邻像素的灰度值;$E(x)$为期望值;$D(x)$为方差。



(a) 原图R层的直方图　(b) 原图G层的直方图　(c) 原图B层的直方图

(d) 加密图像R层的直方图　(e) 加密图像G层的直方图　(f) 加密图像B层的直方图

图5　加密前后图像的直方图



(a) 原图相邻像素的相关分布　(b) 加密图相邻像素的相关分布

图6　图像相邻像素的相关分布

表 1　加密前后图像相邻像素的相关系数

不同加密的 Lena		垂直方向	水平方向	对角线方向
Lena	加密前	0.9794	0.9891	0.9691
	加密后	0.00068592	-0.0016	-0.00062059
Lena[13]	加密前	0.9606	0.9304	0.9057
	加密后	0.0025	0.0061	0.0074
Lena[12]	加密前	0.9686	0.9324	0.9208
	加密后	-0.0053	0.0213	-0.0270

表 2　原图像与加密图像之间的相关系数

加密图像	Lena	Baboon	Peppers
R 层相关系数	0.00068812	0.0027	-0.0023
G 层相关系数	-0.0070792	-0.00096328	-0.0026
B 层相关系数	0.0018	-0.0018	0.00090683

6.4　抗干扰能力分析

图像在传输或进行其他处理时,可能会受到攻击或干涉,所以密文的抗干扰能力是必须要考虑的。本文分别对密文加噪声密度为 0.1 的椒盐噪声和剪切其右下角 300 ×200 区域的数据,结果如图 7(b)(e)所示;原图像受到上述两种攻击后分别如图 7(a)(d)所示;常规解密后得到图像如图 7(c)(f)所示;用抗攻击解密算法解密出的图像如图 7(g)(h)所示。由实

验结果可见,加密算法本身对椒盐噪声和剪切攻击有一定的抵抗能力,而抗攻击算法对这两种攻击有较强的抵抗能力。

7　结束语

本文提出了一种新的基于 Jerk 系统的混沌图像加密算法,Jerk 系统产生的混沌序列表现出理想的伪随机特性。仿真实验结果表明,该算法可以实现对彩色数字图像的加、解密,并且达到很好的加密效果。从算法安全性的分析中可以看出,该算法密钥空间大,有极强的密钥敏感度和非常好的统计特性,并且抗攻击算法具有较强的抗椒盐噪声和剪切攻击能力。

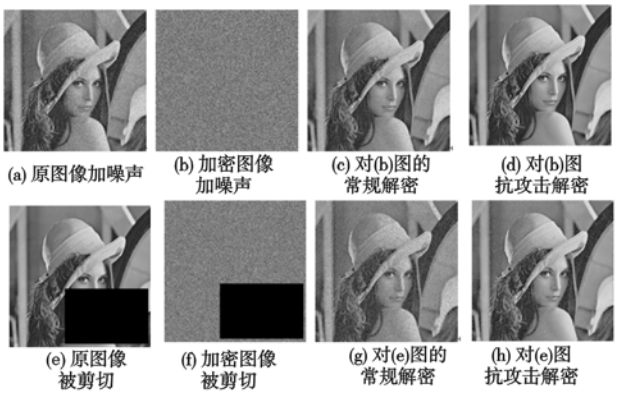


图7　加密图像受干扰的分析

参考文献:

[1] MATTHEWS R A J. On the derivation of chaotic image encryption algorithm[J]. Cryptologia,1989,13(1): 29-42.

[2] FRIDRICH J. Image encryption based on chaotic maps[C]//Proc of IEEE International Conference on Systems, Man and Cybernetics. 1997:1105-1110.

[3] WONG K W, KWOK B S H, YUEN C H. An efficient diffusion approach for chaos-based image encryption[J]. Chaos, Solitons and Fractals,2009,41(5):2652-2663.

[4] FAN Jiu-lun, ZHANG Xue-feng. Image encryption algorithm based on chaotic system[C]//Proc of the 7th International Conference on Computer-Aided Industrial Design and Conceptual Design. 2006: 113-117.

[5] CHEN G, MAO Y, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004,21(3):749-761.

[6] 邱燕,陈斌峰,王艳阳. 基于二维超混沌系统的数字图像加密算法[J]. 陕西国防工业职业技术学院学报,2007, 17(4):17-21.

[7] ZHU Zhi-liang, ZHANG Wei, WONG K W, *et al*. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences,2011,181(6):1171-1186.

[8] TAHA B A, FOURNIER-PRUNARET A K, BOUALLEGUE D R. A fast color image encryption scheme based on multidimensional chaotic maps[C]//Proc of the 2nd International Global Information Infrastructure Symposium. 2009:1-4.

[9] GMBSS K, CHANDRASEKARAN V. A novel image encryption scheme using Lorenz attractor[C]//Proc of the 4th IEEE Conference on Industrial Electronics and Applications. 2009:3653-3657.

[10] CHEN Xi-ming, ZHOU Ping. Tracking control and synchronization for two-dimension discrete chaotic systems[J]. The Journal of China Universities of Posts and Telecommunications,2002,9(3): 7-10.

[11] 郑凡,田小建,范文华,等. 基于 Henon 映射的数字图像加密[J]. 北京邮电大学学报,2008,31(1):66-70.

[12] 胡学刚,王月. 基于复合混沌系统的图像加密新算法[J]. 计算机应用,2010,30(5):1209-1211.

[13] 刘云,郑永爱. 基于混沌系统的彩色图像加密新方案[J]. 计算机工程与应用,2011,47(3):90-93.

(上接第 307 页)

4.3　认证强度的保证

在 CBAC 访问过程中要通过账号和口令认证,其中口令是不保存的,这在一定程度上保证了口令的安全。对于共享的文件只能靠身份认证保证安全,因此账号和密码的安全性要用 PAM 模块进行加强。例如,账户名称和密码的设置要符合一定的安全复杂度,而且不能被其他用户甚至 root 用户读取。主体之间的标志只有 UID 是透明的。

5　结束语

本文分析了当前 Linux 下的主要访问控制机制的特点,根据密钥认证和安全分级策略设计了一种文件访问控制机制。这种机制的主要优点是主客体只需关联几个密钥就可以实现灵活的安全访问,其配置和实现都相对容易,实现了较细粒度的访问控制而且给用户一定的自主选择权。但是,文件属主需要进行大量的访问设置和口令输入,这在一定程度上给实际应用造成了不便。此外,在远程用户数量较多的情况下,如分布式网络密钥应用[13]情况下密钥共享也是一项比较复杂的任务。下一步的研究重点是如何提高可用性,如将密钥导入 USB 设备,避免用户多次重复输入密码,从而实现快速访问,以及采用分类安全思想进一步简化安全设置等。

参考文献:

[1] 毕晓普. 计算机安全学[M]. 王立斌,黄征,等译. 北京:电子工业出版社,2005:84-101.

[2] 倪继利. Linux 安全体系分析与编程[M]. 北京:电子工业出版社,2007.

[3] 石文昌. 安全操作系统的发展[J]. 计算机科学,2002,29(6):1-10.

[4] MALLEY S, VANCE C, SALAMON W. Implementing SELinux as a Linux security module, NAI LabsReport JHJ01-043S[R]. 2002.

[5] 赵亮. Linux 安全模块(LSM)简介[EB/OL]. (2003-07-26)[2011-05-10]. http://www.ibm.com/developerworks/cn/linux/l-lsm/part1/.

[6] HARRINGTON A, JENSEN C. Cryptographic access control in a distributed file system[C]//Proc of the 8th ACM Symposiumon Access Control Models and Technologies. New York: ACM,2003:158-165.

[7] AL-HAMDANI W A. Cryptography based access control in healthcare Web systems[C]//Proc of Information Security Curriculum Development Conference. NewYork: ACM,2010.

[8] KUMAR A, CHOPDEKAR S. Get started with the Linux key retention service[EB/OL]. (2007-04-11)[2011-05-10]. http://www.ibm.com/developerworks/linux library/l-key-retention/index.html.

[9] SANDHU R S, COYNEK E J, FEINSTEIN H L. *et al*. Role-based-access-control models [J]. Computer,1996,29(2):38-47.

[10] HALLYN S E, KEARNS P. Domain and type enforcement for Linux [C]//Proc of the 4th Aunual Linux Showcase & Conference. Berkeley: USENIX Associafion,2005.

[11] 袁春,钟玉琢,张基宏,等. 基于密码学的访问控制和加密安全数据库[J]. 电子学报,2006,34(11):2043-2046.

[12] ANDREW G M, THORSTEN K. The Linux-PAM application developers guide[EB/OL]. (2010-08)[2011-05-10]. http://www.kernel.org/pub/linux/libs/pam/linux-PAM-html/linux-PAM-SAG.html.

[13] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks[C]//Proc of IEEE Symposium on Security and Privacy. 2003:197-213.