一种基于CS-SIFT抗几何攻击的图像双水印算法

李 浩[1] 李宏昌[2]
(武警工程大学信息工程系 西安 710086)[1] (武警工程大学理学院 西安 710086)[2]

摘 要 利用压缩感知(CS)技术及图像尺度不变特征变换(SIFT),研究了一种既能抗几何攻击又能实现盲水印的方法。第一重版权水印经过扩频,嵌入在非抽样轮廓变换(NSCT)低频子带的DWT域中;第二重认证水印通过对含第一重水印的图像压缩感知生成,并作为零水印提交IPR数据库保存。提取水印时,先通过获取的零水印信息得到SIFT特征模板,并对含水印图像完整性进行验证及篡改定位和恢复,再根据SIFT特征点的尺度特征和坐标关系,对图像进行几何校正,使水印信息的提取位置同步。实验表明,该算法透明性良好、水印容量较大,而且对于常规攻击和多种几何攻击都具有良好的鲁棒性。

关键词 数字水印,压缩感知,零水印,尺度不变特征变换,几何校正
中图法分类号 TP751.1 **文献标识码** A

Geometric Attack Resisting Double-watermarking Algorithm Based on CS-SIFT

LI Hao[1] LI Hong-chang[2]
(Department of Information Engineering, University of CAPF, Xi'an 710086, China)[1]
(Institute of Science, University of CAPF, Xi'an 710086, China)[2]

Abstract A geometric attack resisting and watermarking blind extraction implemented algorithm is proposed based on compressive sampling(CS) techniques and the SIFT feature. The first copyright watermarking is spectrum spread and embedded in DWT domain of NCST's lower frequency band. The second watermarking is authentication watermarking. It is generated by compressive sampling of the first watermarking, and stored in IPR database as zero-watermarking. In the process of watermarking extraction, firstly, SIFT feature template is acquired through zero-watermarking, and it verifies the integrity of watermarked image, locates and restores alterations. Then the image is calibrated with scale features and coordinate relationship of SIFT feature points so as to update watermarking extracting locations. The simulation shows that, the proposed algorithm has huge watermarking capacity and favorable transparency. It is robust to ordinary attacks as well as several geometric attacks.

Keywords Digital watermarking, Compressive sampling(CS), Zero-watermarking, Scale invariant, Geometric calibration

1 引言

目前,大多数水印算法都可有效抵抗加噪、滤波、JPEG压缩等攻击造成的像素值的轻微改变,对于水印检测提取的影响相对较小;而平移、缩放、旋转等几何攻击,破坏了水印与图像空间坐标的同步性,使检测器无法确定水印的正确位置、无法正确提取水印,导致算法的鲁棒性较差。因此,抗几何攻击既是数字水印技术的难点,也是常见的攻击。某种水印算法抗几何攻击的能力如何,是衡量该算法优劣的重要指标。

现有的抗几何攻击水印算法大致可分为4类:1)将水印嵌入到对几何攻击具有不变性的变换域中[1-3],如奇异值分解、Tucker分解、基于矩的图像归一化区域、Fourier-Mellin变换域等;2)嵌入水印同时嵌入一个用于估计图像几何变换的参数模板[4];3)将水印嵌入到图像的稳定特征区域来实现水印的同步[5,6];4)依靠图像的稳定特征对图像进行同步校正后提取水印[7]。以上4类算法在水印容量、稳定性、抗几何攻击以及实用性方面均有不同程度的缺陷。

本文研究了一种抗几何攻击的双水印算法。第一重水印为有意义的鲁棒水印,置乱加密后经扩频嵌入到NSCT低频子带的DWT域;第二重水印为认证水印,采用CS技术对载体图像进行分块压缩感知,生成的观测值矩阵作为零水印提交IPR数据库,同时兼有提取图像SIFT特征点模板和篡改定位恢复的功能。可分别从受攻击图像和零水印恢复的图像中提取SIFT特征点进行匹配校正来恢复同步。压缩感知、提取SIFT特征点和零水印等技术的融合使该水印算法不仅能够抵抗几何攻击,而且可进行完整性验证、水印的盲提取。

2 压缩感知理论简介

压缩感知理论最早由Candes等人[8]提出,证明了只要信号在某个正交空间具有稀疏性,就能以较低的频率($M<<N$)采样信号,且可以对原信号高概率重构,打破了Nyquist-Shannon采样定理的束缚,使压缩采样同步完成。其理论的核心是将具有稀疏性或在一些基下能稀疏化表示的高维信号降维处理,得到低维信号,该低维信号可以高概率恢复原高维信号。因此,对非稀疏信号而言,要先对信号进行稀疏化表示。具体过程如下:

李 浩(1990—),男,硕士,主要研究领域为数字水印、图像处理;李宏昌(1956—),男,教授,硕士生导师,主要研究领域为数字图像处理、激光武器。

(1)将初始多维信号 S 稀疏分解及降维处理后得到一维信号 x，$x\in R^N$，满足 $sup(x)=\{i:x_i\neq 0\}$ 且 $sup(x)\leqslant K$，x 称为 K-稀疏信号：

$$x=T(S) \tag{1}$$

(2)取一平稳 $M\times N(M<<N)$ 维高斯随机矩阵 Φ 作为观测矩阵，Φ 满足受限等距约束性[9]（restricted isometry property，简称 RIP），并且测量数目满足：

$$M\geqslant O(K\log N) \tag{2}$$

(3)对 x 进行观测压缩，得到压缩信号 $y\in R^M$，完成投影观测压缩：

$$y=\Phi x \tag{3}$$

(4)恢复过程首先还原稀疏信号 x，可由求解最小化范数优化方程来精确逼近[10]：

$$x=\min\|x'\|_1,\Phi x'=y \tag{4}$$

(5)再由 x 通过(1)的逆过程恢复初始信号 S：

$$S=T^{-1}(x) \tag{5}$$

3 SIFT 特征点匹配校正原理

SIFT(Scale Invariant Feature Transform)算法最初由 Lowe 在 1999 年提出，并在 2004 年得以完善[11,12]。SIFT 特征点对图像缩放、旋转和平移具有不变性，其算法的核心思想是通过寻找、过滤尺度空间内的极值点，找出稳定的特征点，并在每个稳定的特征点周围提取图像的局部特性，最终形成每个特征点的坐标、尺度因子、方向因子以及 128 维的局部描述子。利用 SIFT 特征点的信息可以对两幅特征相同或相似的图像进行特征点的匹配，并通过一定的算法进一步实现几何校正。

3.1 缩放矫正

图像缩放会导致尺度因子随之等比例变换，利用尺度因子的变换量可以进行缩放校正。缩放倍数 δ 可由下式计算：

$$\delta=\frac{1}{n}\sum_{i=1}^{n}\frac{s_1(i)}{s_2(i)} \tag{6}$$

其中，s_1 和 s_2 分别代表匹配点在原始图像和攻击后图像中的尺度因子，n 是参与校正点的组数。

3.2 循环平移矫正

原始图像和攻击后图像某组匹配点的坐标分别为 (x,y) 和 (x',y')，图像大小为 $M\times N$，则该点的循环平移参数 Δx 和 Δy 由下式得到。

$$\Delta x=\begin{cases}x'-x+M, & x'<x\\ x'-x, & \text{其它}\end{cases}$$
$$\Delta y=\begin{cases}y'-y+N, & y'<y\\ y'-y, & \text{其它}\end{cases} \tag{7}$$

通过计算所有匹配点平移参数的平均值即可得到整幅图像的平移校正参数：

$$\begin{cases}\Delta x_c=\frac{1}{n}\sum_{i=1}^{n}\Delta x_i\\ \Delta y_c=\frac{1}{n}\sum_{i=1}^{n}\Delta y_i\end{cases} \tag{8}$$

3.3 旋转矫正

任取原始图像中的两个特征点 p 和 q，则受攻击图像中对应的特征点为 p' 和 q'，将特征点所对应的向量平移到同一坐标系中，将 p 与 p' 重合，则通过两点长度计算公式 $\sqrt{(x-x')^2+(y-y')^2}$ 可求得 $\overline{pq}$、$\overline{p'q'}$、$\overline{qq'}$，则旋转角度为 θ 为：

$$\theta=\arccos\left(\frac{\overline{pq}^2+\overline{p'q'}^2-\overline{qq'}^2}{2\,\overline{pq}\cdot\overline{p'q'}}\right) \tag{9}$$

通过计算多组特征点旋转角度的平均值即可得到整幅图像的旋转校正参数 θ_c：

$$\theta_c=\frac{\sum_{i=1}^{n}\theta_i}{n} \tag{10}$$

4 水印算法

4.1 版权水印预处理

采用 Arnold 变换对水印图像进行置乱，变换次数可作为密钥 key1。为提高水印的安全性，再对置乱后的水印进行混沌加密，混沌发生器的初值条件作为加密密钥 key2。

4.2 版权水印嵌入

版权水印嵌入过程如图 1 所示，具体步骤如下：

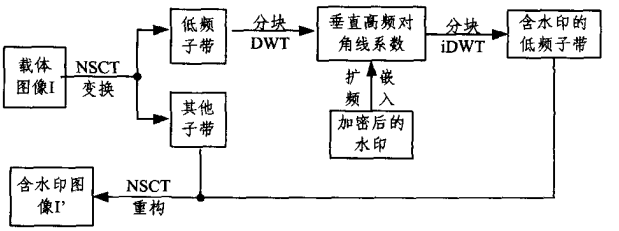


图 1 版权水印嵌入过程

(1)对大小为 $N\times N$ 的灰度载体图像 I 做 L 级 NSCT 分解，取低频子带系数 A。

(2)对低频子带系数 A 进行大小为 8×8 的不重叠分块，加密后的水信息 W 的大小为 $M\times M$，其中 $M\leqslant N/8$。

(3)对各分块做 DWT 变换，对于某一分块来说，取其垂直高频分量的对角线上的系数 $B_{ij}(k)(k=1,2,3,4)$ 作为嵌入系数。

(4)取长度与 B_{ij} 长度相等的两组正交序列 S_0、S_1 对水印 W 扩频，嵌入强度为 α：

当 $W_{ij}=0$ 时，$B_{ij}(k)=B_{ij}(k)+\alpha\times S_0(k)$；

当 $W_{ij}=1$ 时，$B_{ij}(k)=B_{ij}(k)+\alpha\times S_1(k)$。

(5)对各块进行 iDWT，得到嵌入水印信息后的低频子带 A'。

(6)将低频子带系数 A' 与其他各子带系数一起进行 NSCT 重构，得到含水印图像 I'。

4.3 零水印生成

零水印生成过程如图 2 所示，过程如下：

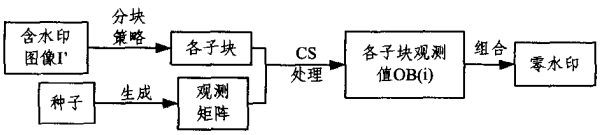


图 2 零水印生成过程

(1)将 3.2 节中得到的含水印图像 I' 按 $B\times B$ 大小分块。B 的大小由期望生成的水印尺寸和对篡改的定位精度决定。

(2)通过抽取某矩阵某些行列的一部分生成观测矩阵，该抽取方法作为生成观测矩阵的种子。

(3)将各分块通过观测矩阵进行 CS 处理得到各个分块的观测值 $OB(i)$。

(4)将观测值组合在一起生成水印，将生成观测矩阵的种子和分块尺寸作为水印密钥 key3 保存。

(5)将水印和密钥注册到内容认证的 IPR 数据库中。

4.4 水印检测提取

水印提取过程如图 3 所示。

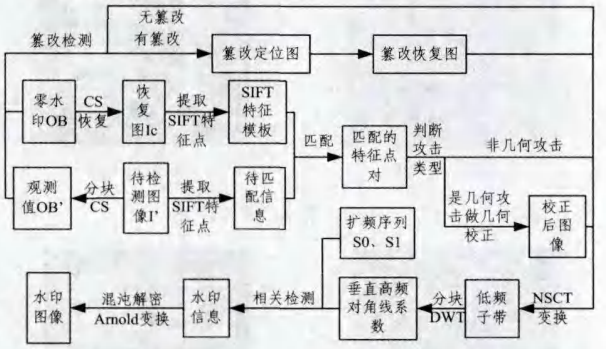


图 3 水印提取过程

(1)通过密钥 key3 向 IPR 数据库获取零水印信息即 CS 观测值 OB,并进行 CS 恢复,得到恢复图像 Ic。

(2)攻击检测:

路径一:分别提取 Ic 和待检测图像 I' 的 SIFT 特征点,判断是否遭受几何攻击,若是,则进行 SIFT 特征点匹配矫正。

路径二:采用与生成零水印相同的方法对待检测图像 I' 做分块 CS 处理,将观测值 $OB'(i)$ 与 IPR 数据库的观测值 $OB(i)$ 作比较,当两者之间的差异 $D(i)$ 超过某一阈值 Th 时,则认为该分块遭受篡改。综合所有被篡改的分块即得到篡改定位图,必要时可通过这些分块的观测值进行 CS 恢复。

若没有检测到上述攻击,则直接进入(3)中处理。

(3)对(2)中得到的图像进行 NSCT 变换(与嵌入算法相同),提取低频子带系数 A'。

(4)对 A' 进行大小为 8×8 的不重叠分块。

(5)对各分块做 DWT 变换,取其垂直高频分量的对角线上的系数 B'_{ij}。

(6)S_0、S_1 分别与每块对角线上的系数做相关检测:如果 $corr(S_0, B'_{ij}) > corr(S_1, B'_{ij})$,则 $W'_{ij}=0$;否则,$W'_{ij}=1$。W' 即为提取出的水印信息。

(7)通过对 W' 进行解密操作,即可得到恢复出的版权水印图像。

5 仿真实验及分析

选用大小为 512×512 的 Lena 图像作为载体图像,如图 4 所示;以大小为 32×32 的"工程大学"字样的二值图像作为水印图像,如图 5 所示。选择 32×32 大小的 CS 分块策略,实验平台为 Matlab7.0。

图 4 载体图像

图 5 水印图像

5.1 攻击校正

表 1 分别列出了缩放校正、循环平移校正和旋转校正测试得到的数据。

显然,通过实验数据与理论值的对比得知,只有在图像缩小时准确率比图像放大时低,这是由于缩小时图像的部分信息丢失导致,而在图像放大、循环平移、旋转方面,利用 SIFT 特征点进行校正具有较高的准确率。

表 1 缩放、循环平移、旋转校正测试

攻击方法	变化量	理论校正量	实际校正量
缩放	1/2	2.000	2.067
	2	0.500	0.499
循环平移	(0,100)	(0,−100.0000)	(0,−100.0002)
	(100,0)	(−100.0000,0)	(−100.0000,0.0009)
旋转	10°	−10°	−10.007°
	30°	−30°	−30.072°

5.2 抗攻击能力

图 6 为含水印图像。图 7 为提取出的水印图像。在没有受到任何攻击的情况下,视觉上无法区别含水印图像和载体图像,提取出的水印图像也清晰可辨。此外,从 $PSNR=43.4318$ 和 $NC=1$ 这两个客观指标来看,本文算法能够较好地满足水印的透明性和有效性。

图 6 含水印图像

图 7 提取出的水印图像

(1)常规攻击

常规攻击如表 2 所列,显然,不同的常规攻击导致了图像质量不同程度的下降,该算法对于 JPEG 压缩、噪声、滤波等常规攻击具有较好的鲁棒性,这主要源于水印的嵌入位置在 NSCT 低频子带的 DWT 域的次高频上,而常规攻击对于低频子带的影响较小。图 8—图 12 分别给出了常规攻击下的含水印图像及提取出的水印。

表 2 常规攻击

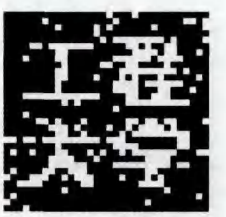
攻击方式	PSNR	NC
JPEG 压缩(Q=70)	41.6050	0.9208
JPEG 压缩(Q=35)	36.9717	0.8630
椒盐噪声(0.01)	26.4013	0.9056
乘积噪声(0.01)	26.1196	0.9313
中值滤波	30.7466	0.9011

(a)攻击后的图像

(b)提取的水印

图 8 $Q=70$ 的 JPEG 压缩攻击

(a)攻击后的图像



(b)提取的水印

图 9 $Q=35$ 的 JPEG 压缩攻击

(a)攻击后的图像　　(b)提取的水印

图 10　0.01 的椒盐噪声攻击

(a)攻击后的图像　　(b)提取的水印

图 11　0.01 的乘积噪声攻击

(a)攻击后的图像　　(b)提取的水印

图 12　中值滤波攻击

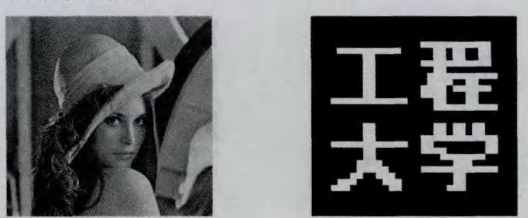
(2)几何攻击

表 3 是几何攻击的数据。图像缩小导致部分信息丢失，使提取出的水印信息不完整，故提取出水印的 *NC* 值不能达到 1。而图像放大不存在信息丢失，因此水印可完全提取出来；同理，循环平移则未导致图像信息损失，因此在水印提取前进行校正，可使水印信息同步，提取出水印的 *NC* 值为 1；旋转攻击不仅使水印信息失去同步性，而且旋转超出原始图像大小的边缘部分也被切去，导致了部分信息的损失。在提取水印之前，同步性虽然可以通过逆向旋转来恢复，但信息的缺失却导致提取出水印的 *NC* 值不能够达到 1。

表 3　几何攻击

攻击方式	变化量	PSNR	NC
缩放	0.5	—	0.9011
	2	—	1.0000
循环平移	100 行	12.2850	1.0000
旋转	10°	12.4901°	0.9234°
	30°	10.5774°	0.9066°

从图 13—图 16 可直观地看出几何攻击下的含水印图像及提取出的水印。



(a)攻击后的图像　　(b)提取的水印

图 13　缩放 2 倍的攻击

(a)攻击后的图像　　(b)提取的水印

图 14　循环平移 100 行攻击

(a)攻击后的图像　　(b)提取的水印

图 15　旋转 10°的攻击

(a)攻击后的图像　　(b)提取的水印

图 16　旋转 30°的攻击

5.3　篡改定位

对含水印的图像进行局部涂抹篡改，如图 17(a)所示。依照 3.4 节中篡改检测的方法，可得到篡改定位图，如图 17(b)所示。显然，定位的精度取决于 CS 分块的大小，本实验中，在分块大小为 32×32 的情况下，当篡改区域宽度或长度小于 32 时，最高只能达到以 32×32 为单元的定位精度。

(a)篡改后图像　　(b)篡改定位图

图 17　篡改涂抹攻击

结束语　本文针对盲水印的实现、水印容量以及抗几何攻击能力三者不能同时兼顾的矛盾，研究了一种基于 CS-SIFT 抗几何攻击的双水印算法。该算法中的版权水印信息经过扩频处理可以遍布整幅图像，提高了水印的容量；认证水印(在本文中即零水印)既可用于图像的完整性验证，又可为 SIFT 特征点匹配校正提供特征点的提取模板。仿真实验表明，本文算法不仅能够抵抗常规攻击，对几何攻击也有较好的鲁棒性，同时该算法还具备完整性验证、篡改定位及恢复的功能。

参 考 文 献

[1]　夏建平，周激流，何坤，等. 基于小波变换和 Tucker 分解的彩色

图像数字水印[J]. 计算机应用研究,2010,27(2):798-800
[2] 何冰,朱志平. 基于奇异值分解的抗几何攻击鲁棒性盲水印算法[J]. 技术研究,2012,11(3):71-73
[3] 张翼,唐向宏. 基于图像归一化的抗几何攻击水印技术[J]. 电路与系统学报,2009,14(6):53-58
[4] Pereira A,Pun T. Robust template matching for affine resistant image watermarks [J]. IEEE Transactions on Image Processing,2000,9(6):1123-1129
[5] 楼偶俊. 基于 Contourlet 域特征点的抗几何攻击水印方法[J]. 计算机研究与发展,2010,47(1):113-120
[6] 陈利利,王向阳. 基于 SIFT 的椭圆区域鲁棒数字水印方案[J]. 计算机工程与应用,2012,48(1):98-101,107
[7] 赵文娴,王玲,杨镭饴. 基于 SIFT 的 NSCT-SVD 域水印算法[J]. 计算机工程与应用,2012,48(10):106-110
[8] Candes E J,Wakin M B. An introduction to compressive sampling[J]. IEEE Signal Processing Magazine,2008,25(2):21-30
[9] Baraniuk R,Davenport M,Devore R,et al. A simple proof of the restricted isometry property for random matrices[J]. Constructive Approximation,2008,28(3):253-263
[10] Dossal C, Reyre G, Fadili J. A numerical exploration of compressed sampling recovery[J]. Linear algebra and Its Applications,2010,432(7):1663-1679
[11] Low D G. Object recognition from local scale-invariant features [C] // International Conference on Computer Vision. Corfu, Greece,1999(9):1150-1157
[12] Lowe D G. Distinctive image features from scal-invariant key points[J]. Internatonal Journal on computer Vision, 2004, 60 (2):91-110

(上接第 251 页)

模型[9],这种情况下框架的安全性降低到决策 MBDH 假设的程度。

假设部分攻击者有能力获得用户的生物特征采样、临时密钥 D^j 和临时关键字 x_{j-1},他就可以利用用户的生物特征顺利访问数据拥有者的文件。然而,一旦攻击者提出访问请求,CS 就会使用密钥隔离机制更新文件头并将更新后的文件头和文件体一起发送给攻击者,基于这种更新机制的特性,攻击者仅有微乎其微的概率解密出文件头。相反,合法用户可以根据公式 $x_j = H((x_0^*)^j) \bmod p$ 将其私钥从 x_{j-1} 更新为 x_j。此外,合法用户可通过 $D_i^{j+1} = (D_i^j)^{x_j}$ 计算更新密钥 $D_{i\in(\omega\cap\omega')}^{j+1}$。

因此,该框架是受到严格的保护的,此外,基于密钥隔离机制还可实现安全密钥的更新。

3.2 性能分析

该部分通过数值分析评估本文提出的访问控制框架的性能,包括由于 CS 和用户的更新操作引起的性能开销。

引理 1 在一个素数顺序为 p 的组中,任意元素 g 的 y 次方(y 是在 Z_p 中随机选取的)可以通过最多 $O(\ln p)$ 次乘法运算计算得到。

证明:首先用二进制表示 y,$y = y_0 \cdot 2^0 + y_1 \cdot 2^1 + \cdots + y_n \cdot 2^n$,其中 $2^n < y \leqslant 2^{n+1}$,$y_i = 0$ 或 1。从而有 $g^y = \prod_{i=0}^{i=n} (((g^{y_i})^2)^{\cdots})^2$。这样计算 g^y 最多需要 n 次平方运算和 n 次乘法运算,相当于总共需要 $O(\ln p)$ 次乘法运算,$n \approx O(\ln y)$ 与 $O(\ln p)$ 是同一个数量级。

引理 2 对于任意元素 $\beta \in Z_p^*$,其中 p 是素数,给定一个数 $x \in Z_p^*$,$\beta^{\frac{1}{x}}$ 的计算开销为 $O(\ln p)$ 次乘法运算。

证明:由于 p 是素数,x 对于是 p 相对素数。根据 Euclid 算法,存在整数 a,b 满足 $ax + bp = 1$,容易得到:

$$\beta = \beta^{ax+bp} = \beta^{ax},\ \beta^{\frac{1}{x}} = \beta^{a} \tag{4}$$

从上面的等式中可知,计算 $\beta^{\frac{1}{x}}$ 大概需要 $O(\ln p)$ 次乘法运算。

CSP 更新开销:从式(3)中可知,每次 CS 更新文件头仅需要执行 $|\omega'| \cdot O(\ln p)$ 次乘法运算(见表 1),同时 CS 删除原来的文件头并通过加 1 更新 CR_{cloud},这个更新操作的开销可忽略不计。

用户更新开销:用户想访问其感兴趣的文件,首先请求 CS 提供 CR_{cloud},将得到的 CR_{cloud} 与 CR_{user} 比较。接下来用户根据两者的不同更新其私钥。根据引理 1,用户需要{$|\omega'| \cdot O(\ln p)$}次乘法运算(见表 1)。

表 1 计算复杂度

操作	复杂度
文件访问——CSP 更新	$\|\omega'\| \cdot O(\ln p)$
文件访问——用户更新	$\|\omega'\| \cdot O(\ln p)$

结束语 本文中研究了云计算中基于生物特征的访问控制问题和密钥暴露问题。为了保护敏感数据和私钥的机密性,以免受到恶意云服务器和外部攻击者的攻击,并克服生物特征噪声大的缺点,本文提出了一种更新 FIBE 框架,即持续地在 CS 和用户之间执行更新操作。在文件创建过程中利用 FIBE 的特性提供基于生物特征的访问控制。此外,通过使用密钥隔离框架,本文的访问控制架构可以更新安全密钥,类似于一次一密机制。通过安全分析和性能分析,证明该架构是安全和轻量级的。

参 考 文 献

[1] Shamir A. Identity-Based cryptosystems and signature schemes [C] // Procedings of the Crypto 1984. volume 196 of LNCS, 1984:47-53
[2] Itkis G, Reyzin L. SiBIR: Signer-base intrusion-resilient signatures [C] // Procedings of the Crypto 2002. volume 2442 of LNCS,2002:499-514
[3] Dodis Y,Katz J,Xu S,et al. Key-Insulated Public-Key Cryptosystems[C] // Procedings of EUROCRYPT 2002. volume 2332 of LNCS,2002:65-82
[4] Bellare M, Palacio. Protecting against key exposure: Strongly key-insulated encryption with optimal threshold [EB/OL]. [2002]http://eprint. iacr. org/2002/064
[5] Hanaoka, Imai. Parallel key-insulated public key encryption [C]// Procedings of the PKC 2006. volume 3958 of LNCS,2006:105-122
[6] Katz D, Xu Yung. Strong key-insulated signature schemes [C] // Procedings of the PKC 2003. volume 2567 of LNCS,2003:130-144
[7] Le Z,Ouyang Y,Ford J,et al. hierarchical key-insulated signature scheme in the CA trust model [M]// Information Security and Cryptology. Springer,2006
[8] Zhou Y,Cao Z,Chai Z. Identity based key insulated signature [C]// Procedings of the ISPEC 2006. volume 3903 of LNCS, 2006:226-234
[9] Sahai A,Waters B. Fuzzy Identity Based Encryption [C]// Proceedings of EUROCRYPT 2005. volume 3494 of LNCS, 2005: 457-473