一种基于 BioHashing 和洗牌算法的可撤销密钥绑定方案

郭 静，徐江峰
（郑州大学 信息工程学院，郑州 450001）

摘 要：针对传统加密方案中密钥管理困难的问题，提出了一个新的通过指纹管理密钥的密钥绑定方案。该方案通过 BioHashing 方法得到用户指纹特征的二进制序列，对得到的序列执行一个改进的洗牌算法进行置乱，最后通过 Fuzzy Vault 方案将特征值与密钥进行绑定。仿真分析表明，利用 Fuzzy Vault 方案的容错机制和 BCH 码的纠错机制，该方案可以在保证指纹信息安全的情况下正确恢复密钥。同时，改进的洗牌算法实现了特征模板的可撤销性和不可逆性。

关键词：密钥绑定；BioHashing；洗牌算法；Fuzzy Vault；容错；纠错
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2014)05-1511-05
doi:10.3969/j.issn.1001-3695.2014.05.055

Cancellable key binding scheme based on BioHashing and shuffling algorithm

GUO Jing, XU Jiang-feng
(*School of Information Engineering, Zhengzhou University, Zhengzhou* 450001, *China*)

Abstract: For the difficulty of key management in the traditional encryption system, this paper put forward a novel key binding scheme using the fingerprint to manage the key. It firstly converted the fingerprint feature into a string of binary sequence by the BioHashing method, and then performed an improved shuffling algorithm to scramble the binary sequence, after that it binded the key to the scrambled sequence by a Fuzzy Vault scheme. The simulation result shows that by the error tolerance ability of the Fuzzy Vault along with the error correction ability of the BCH error-correcting code, the scheme can restore the key correctly under the condition that fingerprints are safe. Meanwhile, the improved shuffling algorithm implements the irreversibility and the cancellability of the fingerprint template.

Key words: key binding; BioHashing; shuffling algorithm; Fuzzy Vault; error tolerance; error-correcting

0 引言

当今社会，信息安全越来越受到人们的重视，密码系统的应用无处不在。但在传统的密钥体制中，为了安全，密钥都是足够长且随机的，人们要记忆它几乎是不可能的，密钥管理问题成了决定整个密码系统安全性的关键。近年来出现的生物特征加密技术（biometric encryption，BE）是通过使用生物特征来保护密钥的一种技术[1]。它使用生物特征来代替密钥，或者将生物特征和密钥以某种方式结合起来，不但解决了存储和管理密钥的麻烦，而且密钥本身可以对生物特征加密保护，使得攻击者既获取不到密钥也不容易获得加密后的生物特征模板，真正实现密钥和用户身份的紧密结合。按照密钥与生物特征结合方式的不同，生物特征加密可以分为密钥释放（key release）、密钥绑定（key binding）和密钥生成（key generation）三种[2]。其中密钥绑定指的是在数据库模板中把生物特征数据和密钥以某种方式有机结合到一起，只有生物特征匹配成功时密钥才被相应的算法提取出来[3]。典型的密钥绑定方案包括 Fuzzy Vault[4] 和 Fuzzy Commitment 方案[5] 等。

指纹以其可区分性高、特征固定、易采集和存储量小等优点，成为目前应用最广泛的生物特征[6]。指纹匹配技术在广义上可以分为基于指纹细节点特征匹配和基于指纹图像特征匹配两大类[7]。基于指纹细节点特征匹配的技术是当前最流行匹配最准确的一种，但是这种方法匹配的高准确性依赖于对指纹图像大量的预处理和对细节点提取后的处理，如图像增强、脊线检测、脊线细化、细节点提取、伪细节点去除等；而基于指纹图像特征的技术则不需要进行太多预处理，直接从原始灰度图像就可以提取出指纹的全局信息，这种方法尤其在遇到指纹图像质量非常差时更为有效，因为质量太差的图像往往提取不到足够的细节点特征完成匹配。

指纹的图像特征主要有 Jain 等人[8] 提出的基于 Gabor 滤波函数库得到的 FingerCode 和 Jin 等人[9] 提出的基于 BioHashing 方法得到的 BioCode。FingerCode 无法克服指纹旋转、形变等问题，验证阶段得采用每次将指纹图像旋转一定角度，再重新尝试验证的方法，而且 FingerCode 的区分性不高[10]。BioHashing 方法采用的是小波傅里叶梅林变换得到的特征向量，特征向量本身具有较高的区分性能[10]，而且小波傅里叶梅林变换对于图像的平移不变，同时能够把图像的旋转和尺度变化

收稿日期：2013-07-17；**修回日期**：2013-08-27

作者简介：郭静（1988-），女，河南博爱人，硕士研究生，主要研究方向为生物特征加密（i_welcome_you@163.com）；徐江峰（1965-），男，河南禹州人，教授，博士，主要研究方向为数据加密、图像加密、混沌加密、信息隐藏、数字水印.

转换为沿坐标轴的平移。

利用指纹进行密钥绑定的经典方案大多采用指纹的细节点特征,如 Fuzzy Vault 方案。但正如前面所述,需要对指纹图像进行大量的预处理等。并且因为 Fuzzy Vault 方案要过滤大量的杂凑点,解码的时间复杂度非常高。针对这些问题,近年来也提出了一些利用指纹的图像特征进行密钥绑定的方案。文献[11]采用 Gabor 滤波得到 FingerCode 后,通过一个修改的 Fuzzy Vault 方案将指纹特征与密钥进行绑定。文献[12]结合 Gabor 滤波和 BioHashing 两种方法,在 BioHashing 的框架下,用 Gabor 滤波得到的 FingerCode 代替原方法中的小波傅里叶梅林特征,并通过 Fuzzy Commitment 方案进行密钥绑定。上述方案都解决了指纹图像需要大量预处理的问题,但因为采用的都是 Gabor 滤波得到的 FingerCode,在恢复密钥时都必须将指纹图像旋转一定角度再重新尝试验证,而这将大大降低系统的效率和使用的方便性。

本文在权衡基于指纹细节点特征和基于图像特征进行密钥绑定的利与弊后,针对现有 Fuzzy Vault 方案恢复密钥时间复杂度高以及采用 FingerCode 系统效率低等问题,探索采用 BioHashing 进行密钥绑定的可行性。方案首先通过改进的 BioHashing 方法最大限度地保留指纹特征,而后通过改进的洗牌算法实现特征的可撤销性和不可逆性,接着通过一个修改的 Fuzzy Vault 方案绑定密钥并解决经典方案恢复密钥时间复杂度高的问题。Fuzzy Vault 方案的容错机制和纠错码的纠错机制保证了密钥的正确恢复。

1 相关知识

1.1 改进的 BioHashing

BioHashing 方法由 Andrew 等人提出,其基本思想是对原始指纹图像进行小波傅里叶梅林变换得到特征向量,而后将特征向量和存储在用户身份令牌中的一组伪随机数进行迭代内积,然后选定一个阈值将结果二值化,产生一组对应特定用户的二值序列,通过比较二值序列达到身份认证的目的。

上述方案随机映射后的特征维数较小,降维丢失了较多的指纹特征,使得攻击者获得令牌后很容易非法访问攻破系统。而且原方案对随机映射后的所有特征位使用了一个全局阈值 0 进行二值化,这显然是不太合适的[13]。

针对上述问题,本文分别从随机映射的方式和阈值的计算两方面对原 BioHashing 方案进行改进。随机映射采用同指纹特征矩阵相同维数的正交随机矩阵分别对特征矩阵进行行和列的映射,阈值则通过计算所有指纹图像随机映射后特征矩阵的平均值得到一个全局阈值矩阵。并且表征每个手指的特征矩阵也是通过计算此手指的多个指纹图像随机映射后特征矩阵的平均值得到。

改进后的方法通过对特征矩阵的行和列用一个同维数的正交随机矩阵进行量化,最大限度地保留了指纹特征,并且表征一个手指的特征矩阵是通过计算此手指多个指纹图像特征矩阵的平均值得到,从而拉大了指纹的类间距。二值特征中的每一位都有一个对应的阈值,充分考虑到特征向量中各位之间的差异性,并且阈值矩阵只需要求一次即可应用于所有的用户。因为随机矩阵的作用仅仅用来量化原始特征矩阵,所以可以将其正交化后存储于系统数据库中,免去了每次使用时用户令牌计算的麻烦。

1.2 改进的洗牌算法

文献[14]为实现虹膜模板的可撤销性提出了洗牌算法。算法的思想是:首先将二进制串特征序列分块,如按八位为一块分成若干块;然后生成一个与特征块数相同长度的密钥,按照密钥位对应位置是 0 还是 1 对特征块进行置乱。如果块对应的密钥位是 1,则将整个块依次往前放;如果是 0 则将对应的块依次往后放。

洗牌算法通过洗牌密钥对特征块进行了置乱,当模板受到威胁时,更换密钥就可以生成另一个特征模板,满足了生物特征模板可撤销性的要求,但它并没有实现生物特征模板变换的不可逆性。为此,本文将上述洗牌算法进行改进:算法对特征分块后,生成一个比特征块数少的密钥,随机选择起始位置按原来的方法对特征块进行置乱,置乱后丢弃未参与洗牌块以实现特征的不可逆性。

改进后的算法可以随机选择洗牌的起始位置以决定丢弃块的位置,也可以随机选择丢弃块数的多少。这样,攻击者并不知道从什么地方开始洗牌,也不知道丢弃了哪部分的特征,充分保证了模板的不可逆性,也增强了算法的灵活性。洗牌后虽然有一部分特征被丢弃,但相对于采用随机映射降维而言还是保留了大量的特征信息。进行洗牌算法后仍然可以保持二进制序列特征的唯一性,并且可以提高真正用户和仿冒者的可区分性[10]。洗牌密钥保存在用户的令牌里,不同用户的洗牌密钥可以不同。

以 4 位洗牌密钥、6 个特征块、洗牌起始位置为 2 为例,改进的洗牌算法简单功能演示如图 1 所示。

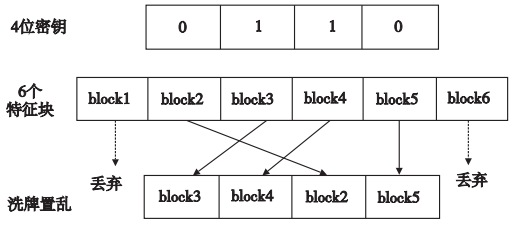

图1 改进的洗牌算法示例

1.3 修改的 Fuzzy Vault 方案

Fuzzy Vault 是 Juels 等人提出的经典密钥绑定方案。Nagar 等人[11]在 2006 年针对原方案加/解锁时间复杂度高的问题,提出了通过表格绑定特征和密钥修改的 Fuzzy Vault 方案。其基本思想是:

1)加锁过程

a)对密钥进行编码分块后,计算得到 n 个十进制密钥值。

b)存储密钥。生成一个 $n \times 3$ 的表格 K,在每行的三个位置随机选择一个放入十进制密钥值,记录下存储密钥的位置。选择一个间距 d,在行的其他两处填上与密钥值相差为 d 的值作为杂凑点,使三个值构成一个等差数列。依次处理每行,记录每行密钥存放的正确位置。

c)将特征值与密钥绑定。构建一个与表格 K 相同的表格 B,将特征值分块,计算每个特征块的十进制值,然后根据密钥存放的位置在表格 B 每行的相应位置填入特征值。仍然选择一个间距,使每行的三个元素构成一个等差数列。

2)解锁过程

a)按加锁时分块的方法得到查询特征值,比较表格 B 中每行的三个元素,选择与特征值最接近的值记录其位置。依次处理每个特征值。

b)根据特征值在表格 B 中的位置从表格 K 中取出对应位置的值。

c)解码恢复密钥。

文献[11]中间距 d 只是为了得到与真值接近的值作为杂凑点以便更好地区分真伪特征而选择的。本方案不仅利用 d 生成杂凑点来保护真正的特征值,而且通过 d 实现系统的容错,从而减少需要纠错的特征位。假如得到二进制特征序列后每八位为一块对特征进行分块,则选取间距 $d=3$,可以实现最低一位的容错,即可以不考虑每八位查询特征和注册特征的最低位是否一致。同样道理,如果选择 $d=7$,可以实现低两位的容错;$d=15$,可以实现低三位的容错;$d=31$,可以实现低四的容错。因为 d 取更大值时,系统几乎已经不能准确辨别出真伪特征,所以其他情况不再考虑。

为了得到更好的容错性能,本方案对存储密钥的表格也作了修改,直接采用密钥的二进制值。这里需要保证的是每行的三个值不能是全 0 或全 1。

修改后的特征值与密钥绑定方案简单功能演示如图 2 所示。

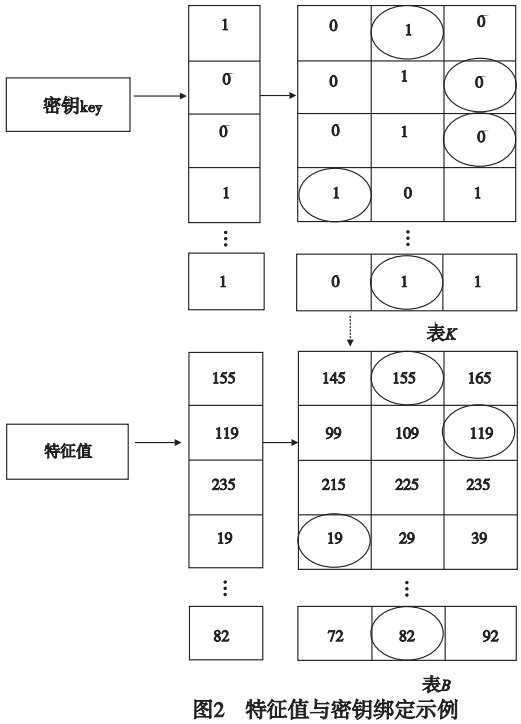

图2　特征值与密钥绑定示例

图 2 中演示的是 $d=10$ 的情况,它可以实现低两位的容错和某些低三位的容错。

经过上述修改后,方案不仅实现了模板与密钥的绑定,而且通过设定特征值的间距和冗余的密钥实现了容错。

1.4　BCH 纠错码

BCH 码是线性分组码中应用最普遍的一种。它可以很容易地根据要求的纠错能力构造,译码器也相对容易实现,因而得到了广泛地应用。使用时通常用 BCH(n,k,t)来表示,其中 n 表示编码后码长,k 是编码前信息长度,t 是纠错能力。更加详细的资料可参考文献[15]。

2　基于指纹 BioHashing 的可撤销密钥绑定方案

整个方案分为注册和验证两个阶段。注册阶段负责生成可撤销的安全指纹模板并与密钥绑定。验证阶段负责与待验证指纹进行匹配恢复密钥。

以下是整个方案详细的注册和验证过程。

1)注册阶段

a)采用改进的 BioHashing 方法获得手指的二进制特征模板。具体做法是:

(a)获得小波傅里叶梅林特征矩阵。给定一个手指的多幅指纹图像,对每幅图像截取指纹中心 128×128 的 ROI 区域。分别提取其小波傅里叶梅林变换特征,得到每幅图像 64×64 的特征矩阵 X。

(b)生成正交随机矩阵量化特征矩阵。随机生成一个 64×64 的行正交矩阵 A,通过计算 $Y=AXA^{\mathrm{T}}$ 分别对手指的每一个特征矩阵进行行和列的量化。

(c)计算表征一个手指的特征矩阵和全局阈值矩阵。将单个手指多个量化后的特征矩阵相加取其平均值作为此手指的特征矩阵。计算所有手指特征矩阵的平均值,得到一个与特征矩阵同维数的全局阈值矩阵。

(d)二值化。将每个手指的特征矩阵与全局阈值矩阵的对应元素比较,小于阈值矩阵对应元素的值设为 0,否则设为 1。这样,就得到了此手指的二进制特征矩阵。按行连接矩阵的所有元素,得到最终表征此手指的 4096 位二进制特征模板。

b)采用改进的洗牌算法实现指纹模板的可撤销性和不可逆性。具体做法是:

(a)将上面得到的 4096 位二进制特征每 8 位为一个分块,共得到 512 块的特征。

(b)随机生成一个比特征块数少的洗牌密钥,比如 500 位的洗牌密钥,随机选择洗牌的起始位置,按照特征块对应的密钥是 0 还是 1 对 500 个特征块进行置乱。置乱后丢弃没有参与洗牌的 12 个特征块,以实现特征的不可逆性。

c)将特征值与密钥通过修改的 Fuzzy Vault 进行绑定并设定容错大小。

(a)构建两个表格 K 和 B,按照修改的 Fuzzy Vault 方法填入特征值和密钥。

(b)确定间距 d,也就确定了每块中低四位有容错能力的位数。

(c)BCH 编码。将每 8 位中没有容错能力的高位进行 BCH 编码。

依次处理每个块,得到整个手指编码后的二进制信息。同时丢弃每块中未参与编码的低位以实现系统的安全性,这样即使攻击者得到用户的令牌,也无法得到用户完整的指纹信息。编码后的信息存储在用户的令牌中。数据库中存储的是表 K、表 B、正交随机矩阵以及全局阈值矩阵。

2)验证阶段

a)采用与注册阶段相同的步骤得到查询指纹的二进制特征。

b)对二进制特征采用与注册时相同的洗牌密钥和起始位置执行改进的洗牌算法。

c)根据系统对该用户设定的间距,得到每块特征值中参

与编码的高位。

d)对每块得到的高位信息进行 BCH 纠错译码,并随机填充低位,重新得到每个 8 位的块。

e)对每一个块计算其十进制特征值并比较表 B 中相应行的三个值,选择与其最接近的值并记录位置。依次处理所有特征值,得到一张记录位置的表。

f)对照表 K,根据上一步记录的位置取出 K 中对应位置上的值,还原出密钥 key。

g)得到密钥后,通过式(1)获得最终密钥:

$$\text{Key} = \text{hash}(\text{key} \| \text{message}) \tag{1}$$

其中:Key 是最终使用的密钥;hash(·)是通用的单向散列函数(如 SHA-1、SHA-256 等);key 是经过特征值和密钥绑定后恢复的密钥;‖代表比特连接操作;message 是一段明文字符,同样存储在用户的令牌中。当密钥 Key 受到威胁时,可以更换 message 来发布一个新的密钥。

如果是真实用户的特征值,则经过容错、纠错并结合表格 K 中冗余的密钥值即可正确恢复密钥。

3 实验结果与分析

本方案在 FVC2002DB2 数据库上进行仿真测试。该数据库有 100 个手指,每个手指 8 次采样,共 800 幅指纹图像。由于进行小波傅里叶梅林变换依赖于指纹的中心点,而数据库中部分指纹没有中心点,所以实验选取了 50 个手指,每个手指取 6 幅图像,共 300 幅图像。首先对这 300 幅图像进行归一化处理,然后寻找指纹中心点,以中心点为中心裁剪 128 × 128 的图像作为 BioHashing 算法的输入图像。按方案中计算手指二进制特征模板的方法,取一个手指的 6 幅指纹图像计算手指的特征,训练 300(50 × 6)幅图像计算全局阈值。小波傅里叶梅林变换特征矩阵的维数为 64 × 64,随机映射矩阵维数为 64 × 64,得到的 BioCode 为 4096 位。

下面对改进的 BioHashing 方法的认证性能进行实验分析。其中,FRR 是错误拒绝率,FAR 是错误接受率,EER 是等错误率。因为当指纹与令牌都安全时系统 $EER = 0$ 的实验结果已经被多次重复而得到公认,所以本文着重考虑的是其他情况下系统的性能,如多幅图像求平均值时仿冒指纹,多幅图像的平均值运算对认证结果的影响等,实验结果如表 1 ~ 3 所示。

验证时采集两幅图像,求它们量化后特征矩阵的平均值作为待查询特征值。BioHashing 性能如表 1 所示。

表 1 采用两幅图像平均值的改进 BioHashing 方法认证性能

阈值	FRR/%	FAR/%		EER/%
		两假	一真一假	
2 800	0.00	0.00	14.33	7.17
3 000	0.00	0.00	0.01	0.01

由表 1 可以看出,采用两幅图像量化后特征矩阵的平均值作为查询指纹的特征时,可以在阈值增大的情况下进一步提高系统的认证性能。

因为所有的指纹图像都参与了平均值运算,因此系统的认证性能将得到提高。下面通过实验进行验证,对每个手指选取 4 幅图像,全局阈值采用 200(50 × 4)幅图像训练得到。系统中参与平均值运算的指纹称为旧指纹,每个手指未参与平均值运算的两幅指纹称为新指纹。仍然分为单幅图像验证和两幅图像取平均值验证两种,结果如表 2 和 3 所示。

表 2 新指纹图像的改进 BioHashing 方法认证性能

阈值	FRR/%		FAR/%	
	旧指纹	新指纹	旧指纹	新指纹
2 400	0.00	5.63	0.10	0.00
2 800	0.00	18.76	0.00	0.00

表 3 采用两幅新指纹图像平均值的改进 BioHashing 方法认证性能

阈值	FRR/%			FAR/%	
	旧指纹	新指纹	一新一旧	两假	一真一假
2 800	0.00	15.43	1.13	0.00	5.88
3 000	0.00	21.83	2.58	0.00	0.01

结合表 2 和 3 可以看出,参与平均值运算的旧指纹的确比不参与平均值运算的新指纹性能更好,即平均值运算确实对系统的认证性能产生了影响。同时还可以看出,对系统性能影响最严重的情况是当验证的两幅指纹图像一幅为真一幅为假时,系统不能很好地作出区分。但这个问题可以通过借用图像配准领域基于互信息的思想得到解决。在采集两幅图像后先计算其互信息,进而在特征进入系统计算前就拒绝这样的访问。

在间距分别采用 3、7、15、31 进行容错,BCH 码进行纠错时,新方案的密钥恢复性能如表 4 所示。

表 4 新方案的密钥恢复性能

BCH 纠错码	间距 d	FRR/%				FAR/%
		旧指纹		新指纹		
		一次验证	三次验证	一次验证	三次验证	
(15,7,5)	3	18.91	15.86	43.25	38.44	0.00
(15,6,3)	7	9.97	4.11	29.63	27.61	0.00
(15,5,3)	15	10.77	4.03	32.78	28.53	0.00
(15,4,4)	31	4.54	1.12	20.74	18.46	0.00

由表 4 可以看出,方案可以在 FAR 为 0 的情况下实现对密钥的正确恢复。同时也可以看出,新指纹是制约系统性能的一个重要因素。

4 安全性分析

方案中存储在数据库中的信息包括 BioHashing 中的正交随机矩阵 A 和全局阈值矩阵,Fuzzy Vault 中的表 K 和 B;存储在用户令牌中的信息包括洗牌算法中的洗牌密钥和起始位置,以及经过 BCH 编码的特征信息和需要输入到哈希函数中的 message。整个系统需要保护的是用户的指纹信息和最终密钥。

如果攻击者攻破数据库获得表 K 和表 B。对于用户的指纹信息而言,如果攻击者想要从表 K 暴力破解获得正确的指纹信息,假设系统总共有 500 个特征块,则需要作 3^{500} 次尝试。对于密钥而言,因为表 B 每行不是全 0 或全 1,所以攻击者想要从表 B 猜出密钥需要作 2^{500} 次尝试。由以上分析可知,即使攻击者获得数据库中的数据,也破解不出原生物特征信息以及密钥,系统仍是安全的。并且系统可以通过发布新的洗牌密钥或新的正交矩阵等相关参数改变数据库中的数据,使得泄露的数据无效。

考虑用户令牌丢失的情况。对于用户的指纹信息而言,因为进行 BCH 编码时舍弃了一部分特征信息,并且在进行洗牌算法时也不可逆地丢弃了一部分的特征,所以当令牌丢失时,攻击者通过令牌中指纹特征的 BCH 编码并不能获取用户完整的指纹信息。对于密钥而言,如果攻击者分析出系统的 BCH

编码方式,就可以得到部分特征序列。若攻击者将假指纹输入系统,并且成功地将假指纹得到的特征序列用令牌中获得的序列来代替输入系统,就可以得到密钥 key,连接令牌中的 message 就可以得到最终密钥 Key。所以一旦用户令牌丢失,则密钥就有可能被窃取。针对这个问题,可以将 message 保存到别的地方,或者采用口令来代替等方法,使得攻击者不能获得最终密钥。

5　结束语

为解决传统加密方案中密钥管理困难的问题,本文提出了一个新的将指纹与密钥通过 Fuzzy Vault 绑定到一起的密钥绑定方案。此方案可以为不同的应用绑定不同的密钥,并且保证在释放密钥的同时不泄露原始指纹特征信息。即使数据库被攻破,攻击者也得不到用户的特征信息,并可以通过更改方案的诸多参数使得泄露数据无效。理论分析和仿真结果表明了方案的有效性,但同时也暴露出其存在的不足,即未参与平均值运算的指纹恢复密钥的性能不理想,以及当用户令牌丢失时系统可能面临安全性的威胁,这也是下一步的研究打算。

参考文献:

[1] ULUDAG U, PANKANTI S, JAIN A K. Fuzzy vault for fingerprints [C]//Proc of Audio and Video-based Biometric Person Authentication. Berlin:Springer, 2005:310-319.

[2] 姚琳, 范庆娜,孔祥维. 基于生物加密的认证机制[J]. 计算机应用研究,2010, 27(1) : 268-270.

[3] 谭台哲,章红燕. 一种改进的指纹 Fuzzy Vault 加密方案[J]. 计算机应用研究,2012, 29(6):2208-2210.

[4] JUELS A, SUDAN M. A Fuzzy Vault scheme[J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257.

[5] JUELS A, WATTENBERG M. A fuzzy commitment scheme[C]// Proc of the 6th ACM Conference on Computer and Communications Security. New York:ACM Press, 1999: 28-36.

[6] 田捷,杨鑫. 生物特征识别理论与应用[M]. 北京:清华大学出版社,2009.

[7] JIN A T B,LING D N C,SONG O T. An efficient fingerprint verification system using integrated wavelet and Fourier-Mellin invariant transform[J]. Image and Vision Computing, 2004,22(6): 503-513.

[8] JAIN A K, PRABHAKAR S,HONG L,*et al*. Filterbank-based fingerprint matching[J]. Image Processing, 2000,9(5):846-859.

[9] JIN A T B,LING D N C,GOH A. BioHashing: two factor authentication featuring fingerprint data and tokenised random number[J]. Pattern Recognition,2004,37(11): 2245-2255.

[10] LUMINI A,NANNI L. An improved BioHashing for human authentication[J]. Pattern Recognition, 2007, 40(3):1057-1065.

[11] NAGAR A,CHAUDHURY S. Biometrics based asymmetric cryptosystem design using modified Fuzzy Vault scheme[C]//Proc of the 18th International Conference on Pattern Recognition. [S. l.]:IEEE Press, 2006: 537-540.

[12] 陈开志,胡爱群,宋宇波,等. 基于 BioHashing 和密钥绑定的双重可删除指纹模板方法[J]. 高技术通讯,2010,20 (11): 1115-1120.

[13] LIU Er-yun, LIANG Ji-min, PANG Liao-jun, *et al*. Minutiae and modified Biocode fusion for fingerprint-based key generation [J]. Journal of Network and Computer Applications, 2010,33(3): 221-235.

[14] KANADE S, CAMARA D, KRICHEN E,*et al*. Three factor scheme for biometric-based cryptographic key regeneration using iris[C]// Proc of Biometrics Symposium. [S. l.]:IEEE Press, 2008: 59- 64.

[15] BOSE R. 信息论、编码与密码学[M]. 武传坤,李徽,译. 北京:机械工业出版社,2010.

(上接第 1490 页)

6　结束语

云存储中共享数据的安全问题一直是研究热点,而采用属性加密的访问控制技术是解决该问题的一个手段。本文提出了一种属性可撤销的密文属性加密方案,基于代理重加密技术和序列标志法实现了系统的属性撤销,并运用安全性证明技术分析得出该算法在 DBDH 假设下 CPA 是安全的,并且由于密文的长度随访问结构中属性的数目变化较小,将大大降低用户使用云存储时的存储开销,适合小数据的存储操作。在本方案的基础上,下一步研究重点将在访问控制结构和代理重加密算法的优化上,以实现更加灵活的访问控制。

参考文献:

[1] SAHAI A,WATERS B. Fuzzy identity-based encryption[C]//Proc of Advances in Cryptology-EUROCRYPT. Berlin: Springer-Verlag, 2005:457-473.

[2] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Proc of the 14th Interntional Comfernce on Practie and Theory in Public Key Cryptography. Berlin:Springer,2011: 53-70.

[3] DAZA V, HERRANZ J, MORILLO P, *et al*. Extended access structures and their cryptographic applications[EB/OL]. (2008-11-28). http://eprint. iacr. ong/2008/502. pdf.

[4] EMURA K, MIYAJI A, NOMURA A,*et al*. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[C]// Proc of the 5th International Conference on Information Security Practice and Experience. Berlin:Springer,2009: 13-23.

[5] DOSHI N, JINWALA D. Constant ciphertext length in CP-ABE[EB/OL]. 2012. http://eprint. iacr. org/2012/500. pdf.

[6] YU Shu-cheng, WANG Cong, REN Kui,*et al*. Attribute based data sharing with attribute revocation[C]// Proc of the 5th ACM Symposium on Information, Computer and Communications Security. New York:ACM Press, 2010: 261-270.

[7] HERRANZ J, LAGUILLAUMIE F, RàFOLS C. Constant size ciphertexts in threshold attribute-based encryption[C]//Proc of the 13th International Conference on Practice and Theory in Public Key Cryptography. Berlin:Springer,2010:19-34.

[8] 王晓锦,张旻,陈勤. 一种高效属性可撤销的属性基加密方案[J]. 计算机应用, 2012, 32(S1):39- 43.

[9] 刘帆,杨明. 一种用于云存储的密文策略属性基加密方案[J]. 计算机应用研究, 2012, 29(4):1452-1456.

[10] 冯登国,张敏,张妍. 云计算安全研究[J]. 软件学报, 2011, 22(1):71-83.

[11] 冯登国. 国内外密码学研究现状及发展趋势[J]. 通信学报, 2002, 23(5):18-26.

[12] 徐鹏,金海,邹德清. 加密数据云存储及其隐私保护[J]. 中国计算机学会通讯, 2012, 8(7):22-28.