文章编号:1001 - 9081(2008)07 - 1816 - 03

基于指纹的可撤销 Fuzzy vault 方案

冯 全[1,3],肖媛媛[2],苏 菲[3],蔡安妮[3]
(1. 甘肃农业大学 工学院,兰州 730070; 2. 北京工商大学 计算机学院,北京 100037; 3. 北京邮电大学 电信工程学院,北京 100876)
(fquan@sina.com)

摘 要:Fuzzy vault 是一种用生物特征保护密钥的加密框架,其主要缺点在于攻击者可以通过交叉比较同一用户的不同 vault 来获得生物模板的准确信息,从而可以破解 vault。提出了一种使用基于指纹细节点的可撤销的变换模板作为生成 vault 的模板,保护不同密钥时采用不同变换模板,从而解决了这个问题。采用以巴特沃斯低通滤波器为核的函数组作为生成可撤销模板的变换函数。此外还使用了用户口令加密 vault,从而进一步增强了被保护密钥的安全性。

关键词:Fuzzy vault; 可撤销模板; 指纹细节点; 生物加密
中图分类号: TP918 **文献标志码**:A

Cancelable fingerprint fuzzy vault scheme

FENG Quan[1,3], XIAO Yuan-yuan[2], SU Fei[3], CAI An-ni[3]
(1. *School of Engineering, Gansu Agricultural University, Lanzhou Gansu* 730070, *China*;
2. *School of Computer Science and Technology, Beijing Technology and Business University, Beijing* 100037, *China*;
3. *School of Telecommunication Engineering, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: Fuzzy vault is a cryptographic framework that binds the biometric template with a cryptographic key. However, attackers can easily compromise them if they steel more than two vaults of a legal user by cross matching. A new scheme named cancelable fuzzy vault was proposed to overcome this shortcoming, which generated different vaults from different cancelable templates instead of the origin template. In our scheme, a mixture of butterworth low filter was taken as the transform function which generated a cancelable template. In addition, users' passwords were adopted to encrypt the vaults to improve their security.

Key words: fuzzy vault; cancelable template; fingerprint minutiae; biometric cryptosystem

0 引言

近年来出现的生物密码技术(Biometric cryptosystem/Biometric Encryption)是通过使用生物特征来保护密码系统的密钥的一种技术[1]。当用户需要得到一个被保护密钥,只需向系统提供自己的生物特征样本,如果验证样本和注册模板匹配,密钥立即被释放,从而去加/解密数据,或者用于数字签名。这种方法真正实现密钥和用户身份的挂钩,用户无需记住口令;而攻击者很难猜出生物特征,故安全性更高。但这种安全性是建立在原始模板的安全性基础上的,即原始模板不能泄露给攻击者。生物密码技术为密钥安全提供了一种新的保障措施。

文献[2]提出的 Fuzzy vault 方法是其中一种典型的方案。这种方法将待保护的密钥用生物模板编码后,把生物模板数据隐藏在一群随机干扰数据中,从这些混合数据中很难分离出真实数据,真实数据被认为是“上锁”的。真实用户出示的现场样本则用来“解锁”真实数据。它比较适合于认证结果与特征点顺序无关的生物特征数据的保护,甚至可以容忍特征点数目的变化。但它也存在一些安全缺陷[3]:

1)同一个用户的生物模板可以用来绑定多个密钥,生成多个 vault。但如果攻击者设法获得同一用户的两个 vault,通过简单地比较就可以获得用户模板,进而获得密钥。

2)由于 vault 中干扰点的数量远大于真实点数量,攻击者有可能在 vault 中插入自己的生物数据,这使得攻击者和合法用户都能通过认证。

产生第 1 种缺陷的根本原因在于生物模板的唯一性。模板的唯一性和非保密性给生物认证的安全带来了许多挑战,为了应对这些困难,Ratha 等[4]提出了可撤销生物认证的概念(Cancelable Biometrics)。可撤销生物认证的基本思想是利用用户或系统设置的某些可以改变的变换函数或参数,将原始模板转变成变换模板;这种变换是单向的,攻击者即使得到变换模板和变换函数或参数,仍然无法恢复出原始模板。如果现有的变换模板被怀疑出了问题,只要重新设置新的变换函数或参数,就可以生成与以前不同的新模板。因此在变换域中,模板是“可撤销”的。

造成第 2 种缺陷的原因是 vault 数据是“裸露的”,可以对 vault 使用签名来验证其中数据的真实性,但我们认为直接加密 vault 更方便,除了克服第 2 种缺陷,还可以增强 vault 安全性。

1 基于指纹的可撤销 Fuzzy vault

基于以上分析,我们将 Fuzzy vault 与 Cancelable biometrics 结合,提出了可撤销的 Fuzzy vault 方案。本方案有注册和认证两个主要步骤。注册阶段,系统选择合适的变换函数,并随机产生变换函数的参数,将用户原始指纹模板转换为变换模板;再采用 Fuzzy vault 方案实现变换模板对待保护

收稿日期:2008 - 01 - 08;**修回日期**:2008 - 03 - 28。 **基金项目**:国家自然基金资助项目(60472069)。

作者简介:冯全(1969 -),男,四川隆昌人,副教授,硕士,主要研究方向:图像处理、生物认证与加密; 肖媛媛(1972 -),女,内蒙古包头人,讲师,硕士,主要研究方向:软件工程; 苏菲(1972 -),女,陕西西安人,副教授,博士,主要研究方向:图像处理、生物认证与加密; 蔡安妮(1943 -),女,北京人,教授,博士生导师,主要研究方向:多媒体通信、图像处理、生物认证。

密钥 S 的编码和保护;最后使用根据用户口令生成的密钥加密 vault。认证阶段,系统使用由用户口令生成的密钥解密 vault,得到变换的 vault;并使用与注册阶段相同的变换函数和参数将现场指纹样本的特征数据转换到变换空间;在该空间中用变换样本对 vault 进行匹配和筛选,过滤掉大部分的干扰点,然后重构出被保护的密钥 S。

如果用户有不同的密钥需要保护,系统可以生成不同的变换模板,以此构造不同的 vault,从而避免攻击者通过交叉对比破解模板。

本方案中使用的指纹特征是细节点,它可以用一个三元组 (x,y,θ) 来表示,其中 x,y 是细节点所在位置的平面坐标,θ 是细节点的方向。我们假定原始模板和现场样本已经预先对齐。

1.1　可撤销的指纹模板的实现方案

可以使用某种不可逆的函数变换原始生物特征,以生成变换模板。但如何选择合适的变换函数目前还没有定论[4],不过还是有一些基本要求:

1)不可逆性。如果不知道变换函数和变换参数,攻击者无法从变换模板中恢复出原始模板;即使知道这些信息也是如此。通常可以使用多对一的变换,即原始空间中的多个区域变换后在变换空间得到一个有重叠和扭曲的区域,来保证原始模板模式无法从变换模板中唯一地被恢复。

2)变换函数应是局部平滑的(或线性的),全局非线性的。局部平滑性保证了生物数据中局部的小变化在变换后也保持小的变化,这是为了容忍要匹配的两个生物特征数据中的噪声。全局的非线性性则减小了变换前后特征的相关性。

3)通常的匹配器为了克服样本和模板间的类内误差,都具有一定的误差容忍度。某些情况下,特别是点匹配的情况(如指纹认证),这可能导致攻击者使用已经撤销的变换模板直接与新变换模板匹配时仍然能通过认证。为了避免这种情况,变换函数应该尽量将特征点推出匹配器的误差容限范围。

此外,对指纹认证来说,细节点匹配法已经被证明是最可靠的认证方法;因此变换后的特征最好仍然以细节点的形式描述,这样可以直接使用细节点匹配法。考虑以上要求,我们将变换后的细节点特征写作:

$$x' = x + K\cos(\varphi(x,y)) + T(x,y) \tag{1}$$

$$y' = y + K\sin(\varphi(x,y)) + T(x,y) \tag{2}$$

$$\theta' = \theta + \Omega + \Theta(x,y) \bmod (2\pi) \tag{3}$$

其中:x,y,θ 分别代表原始细节点的 x 坐标,y 坐标和方向。式(1)~(3)的意义是:为了满足上述可撤销模板基本要求(3),我们将原始细节点的平面坐标沿 $\varphi(x,y)$ 方向移动一固定长度 K,同时附加一段随细节点位置变化的位移 $T(x,y)$。对原始细节点的方向旋转一固定随机角度 Ω,同时附加一个随位置变换的角度 $\Theta(x,y)$。$\varphi(x,y)$、$T(x,y)$ 和 $\Theta(x,y)$ 都是参数可调的变换函数。

为了构造出符合基本要求(1)和(2)的函数 $\varphi(x,y)$,$\varphi(x,y)$、$T(x,y)$ 和 $\Theta(x,y)$。文献[4]中采用的了 2 组以 2 维高斯函数为核的函数组,且需要对高斯函数求微分。出于编程的方便性,我们则引入了具有同样低通性质、三组独立的、以巴特沃斯低通滤波器为核的函数组:

$$T(x,y) = \sum_{i=1}^{N_T} \frac{T_i}{1 + [D_{(x_i,y_i)}(x,y)/D_{T0}]^{2n_1}} \tag{4}$$

$$\varphi(x,y) = \sum_{j=1}^{N_\Phi} \frac{(-1)^{rand01(j)}\Phi_j}{1 + [D_{(x_j,y_j)}(x,y)/D_{\Phi 0}]^{2n_2}} \tag{5}$$

$$\Theta(x,y) = \sum_{k=1}^{N_\Theta} \frac{(-1)^{rand01(k)}\Theta_k}{1 + [D_{(x_k,y_k)}(x,y)/D_{\Theta 0}]^{2n_3}} \tag{6}$$

其中:n 是巴特沃斯低通滤波函数的阶。(x_i,y_i)、(x_j,y_j) 和 (x_k,y_k) 是细节点平面内的随机点。$D_{(x_i,y_i)}(x,y)$ 是点 (x,y) 距 (x_i,y_i) 的距离。$D_{T0},D_{\Phi 0},D_{\Theta 0}$ 为常数,调节它们可以改变对应巴特沃斯低通滤波函数的过渡带的陡度。T_i,Φ_j,Θ_k 分别决定细节点附加位移、位移方向以及细节点方向旋转角度的幅度。$rand01(\cdot)$ 表示随机取 0 或 1。

对原始模板的每个细节点,我们用式(1)~(6)进行计算,就得到了变换模板。后面进行认证时,现场指纹样本的每个细节点也采用同样的计算,就可以得到变换样本,该样本和变换模板通过普通的细节点匹配器就可以进行比对。

在实际应用中,系统生成变换模板后可以将式(1)~(6)中的参数以及各相关随机数保存起来,如存放在智能卡或服务器上。如果旧模板被撤销后,需要重新发放新模板,系统一般只需要改变以上各随机数,重新生成变换模板即可。

为了在后面 Fuzzy vault 中实现对密钥的编码和解码,我们将变换模板和变换样本中细节点的平面坐标和方向均线性映射到[0,255],分别用 8 个比特表示。

1.2　指纹 Fuzzy vault 的实现

目前已经有几种指纹 Fuzzy vault 的实现方案[5-6],我们在实现时采用了文献[6]的部分思想。但我们的特点是:1)生成 vault 的模板不是原始模板,而是变换模板。2)由于细节点的方向和平面位置有很强的相关性,攻击者可以使用这种相关性破解 vault。因此文献[6]并没有使用方向信息。而变换模板中细节点的位置和方向具有随机性,且不再相关,因此我们的 vault 实现中使用了方向信息作为匹配条件之一。3)文献[6]中,为了克服非线性形变,对细节点位置 (x,y) 的平面做了分块,从而进行粗量化。但由于对齐的问题,本来匹配的点,可能在模板和现场样本中可能会被划分到不同的块中,从而减少了匹配点的数量。我们的方案中不采用粗量化,而是使用了匹配盒。4)虽然使用细节点的平面坐标和方向(共 24 位),但它们只在解密 vault 时用来筛选真实点。在对被保护的密钥进行多项式编码或解码时,仍然只采用平面坐标构成的 16 位二进制数,即计算域是 $GF(2^{16})$。这样做的目的是为了减小运算量。

我们以待保护密钥 S 长度为 128 比特为例来说明我们的 Fuzzy vault 实现方案,其主要过程如下(下述计算是在 $GF(2^{16})$ 上进行):

1)注册时,使用变换模板中细节点来对 S 进行编码,并构造 Fuzzy vault。

首先,我们构造出编码多项式 $f(u)$。由于 S 的长度是 128 比特,而运算域 $GF(2^{16})$,$f(u)$ 的阶 n 应该取 8(128/16)。将 S 顺序分割成 8 个 16 比特的段,即 $S = s_8 s_7 \cdots s_1$。我们计算出 S 的 CRC-16 值,记为 s_0。令 $s_8,s_7,\cdots,s_1,s_0$ 分别作为 $f(u)$ 的系数,即:

$$f(u) = s_8 u^8 + s_7 u^7 + \cdots + s_1 u + s_0 \tag{7}$$

假定变换模板 $M^T = \{(x'_{Ti},y'_{Ti},\theta'_{Ti})\}_{i=1}^{N_T}$,其中 N_T 是模板细节点数目。把变换模板中每个细节点的平面坐标 x'_{Ti},y'_{Ti} 简单串联起来构成一个 16 比特的数 $u_i = [x'_{Ti} \mid y'_{Ti}]$,然后计算出的 $f(u_i)$ 的值。点对 $(u_i,\theta_i',f(u_i))$ 构成真实点集合 G,其中 $i = 1,\cdots,N_T$。

随机产生 N_{chaff} 个干扰点对 (c_j,d_j,e_j),其中 $j = 1,\cdots,N_{chaff}$,$N_{chaff} \gg N_T$。这些点对中 c_j 和 e_j 均是 16 比特的随机数,

必须满足$f(c_j) \neq e_j$;d_j是8比特的随机数,而且(c_j,d_j)不能等于任何一个(u_i,θ_i),这些点对就构成干扰点集合C。将集合G和C充分混合,就得到vault $V = \{(v_i,w_i,p_i)\}_{i=1}^{N_T+N_{chaff}}$,然后将用户口令加密$V$,得到加密vault EV。

2)认证时,系统用用户现场样本和V进行解码,重构出编码多项式,从而恢复多项式系数中隐藏的密钥。

系统获取用户的现场指纹样本,使用与变换模板相同的变换参数,将其细节点按式(4)~(9)进行变换,得到变换样本$M^Q = \{(x'_{Qk},y'_{Qk},\theta'_{Qk})\}_{k=1}^{N_Q}$。并使用用户口令解密$EV$,得到$V$。

对V中的每个点(v_i,w_i,p_i),把16比特v_i拆分成两个8比特的数,分别记为x''_i和y''_i,记$\theta''_i = w_i$。这样就构造出一个细节点集合$VC = \{(x''_i,y''_i,\theta''_i)\}_{i=1}^{N_T+N_{chaff}}$,显然其中只有$N_T$个真实的细节点,其他都是干扰点。为了选出其中的真实点,我们用M^Q去做过滤,即用每个$(x'_{Qk},y'_{Qk},\theta'_{Qk})$与它们进行匹配。匹配时,我们以每个$(x'_{Qk},y'_{Qk},\theta'_{Qk})$为中心,规定一个匹配盒,盒子的三个半径代表了对细节点的x,y和θ三个量的非线性形变的容忍程度。凡是落入该盒子内的VC的点,我们就认为是一个候选细节点。所有的候选细节点对应的(v_i,w_i,p_i)就构成了候选点集合$T = \{(v_i,w_i,p_i)\}_{j=1}^{N_{cand}}$,通常$N_{cand} \ll N_{chaff} + N_T$。

如果是真实用户,经过过滤,T大部分点属于变换模板的集合G中的真点,但也会混杂部分假点。我们需要对T进行解码,以重构出编码多项式,从而恢复出秘密S。我们只有选出T中的$n+1=9$个(n是编码多项式的阶)真实点,则可以恢复出秘密S。当然我们事先并不知道哪些点是真实点,显然这是一个密码技术中的带噪声点的秘密共享的$(n+1,N_{cand})$—门限方案。我们采用遍历的方法,任取T中的9个点对,为简单起见,我们记为$\{(v_i,p_i)\}_{i=1}^{9}$,采用拉各朗日插值法重构多项式$f^*(u)$:

$$f^*(u) = \frac{(u-v_2)(u-v_3)\cdots(u-v_9)}{(v_1-v_2)(v_1-v_3)\cdots(v_1-v_9)}p_1 + \frac{(u-v_1)(u-v_3)\cdots(u-v_9)}{(v_2-v_1)(v_2-v_3)\cdots(v_2-v_9)}p_2 + \cdots + \frac{(u-v_1)(u-v_2)\cdots(u-v_8)}{(v_9-v_1)(v_9-v_2)\cdots(v_9-v_8)}p_9 \quad (8)$$

展开上式后,得到$f^*(u) = c_8u^8 + c_7u^7 + \cdots + c_1u + c_0$。我们取出其中各单项式系数,串联起来作为候选密钥$S^* = c_8c_7\cdots c_1$,并取出常数$c_0$项作为验证码。然后计算$S^*$的CRC-16值,若恰好等于$c_0$,就有很大的概率认为$S^*$就是$S$。如果不等,选取$T$中其他$n+1$个点重复上述计算,直到找到满足CRC-16校验的密钥。如果遍历完T没有找到满足上述检验条件的S^*,则说明T真点少于9个,则解码失败。

2 实验结果与分析

我们对上述方案在FVC2002-DB1和DB2上进行了测试。两个库中各有100人指纹,每人8幅指纹图像。DB1中,每幅图像大小是388像素×374像素;DB2中,每幅图像大小是290像素×560像素。按照FVC2002竞赛规则,对每枚指纹的8副图像需要进行交叉比对,这样没枚指纹共有28对对应关系。我们选择细节点多的指纹为模板,少的作为样本。按照前面介绍方法进行密钥恢复实验。由于生成变换模板和vault时,都存在随机性,为了检验算法的可靠性,我们用每个模板生成了100个vault,每个vault中干扰点的数目为200。实验中计算$T(x,y)$、$\varphi(x,y)$以及$h_\theta(x,y)$时,取$N_T = N_\Phi = 20$,$N_\theta = 5$;$D_{T0} = D_{\Phi 0} = D_{\theta 0} = 18$;$n_1 = n_2 = n_3 = 2$;$K = 24$。细节点匹配器的平面容限半径为8,方向的容限半径是7。我们对密钥长度是128位,多项式的阶为8情形,测试了密钥恢复的错误接受率和错误拒绝率。实验中,如果从fuzzy vault中恢复出的真实细节点多于8个,即为成功,否则失败。我们的实验结果是对于DB1,错误拒绝率为4.3%。对于DB2,错误拒绝率是9.1%。对不同用户进行了交叉密钥恢复测试,两种情况下,测得错误接受率均为0。

我们看到以上结果与文献[5]报道的错误拒绝率=21%(同样是128位密钥)相比,有了明显改善,除数据库不同之外,这主要得益于使用了细节点方向信息。文献[5]由于只采用细节点的平面坐标,其平面坐标量化粒度是7个像素。而本方案采用3维匹配器后,平面坐标的等效半径相当于11个像素,方向半径相当于10°;因此允许较大的指纹形变,这增加了筛选出真实点的可能,而又不会导致假点明显的增加。使得本方案的错误拒绝率有了较大的减少。实验中发现DB1上的结果明显好于DB2,分析原因是:1)DB1的指纹图像形变小于DB2,DB2上相当一部分指纹中模板和样本的匹配点的距离超出了容限盒的范围。2)DB2中指纹图像的细节点数目明显少于DB1,匹配点的数目也少于DB1。

3 结语

可撤销的Fuzzy vault方案采用可撤销模板作为构造vault的依据,可以避免攻击者使用交叉对比来获取用户真实模板;使用用户口令对vault进行加密使得vault更加巩固;加上Fuzzy vault自身的安全机制,使得被保护的密钥有了很高的安全性。我们现在工作是在模板和样本预对齐的条件下完成的,然而在实际中,模板和样本需要盲对齐,这是很困难的,目前还没很好的解决方案。文献[4]的方法是使用指纹中心点及其方向来实现对齐,文献[7]则使用一组纹线的最大曲率点实现对齐。下一步,我们将研究自动对齐算法,使本方案能实用化。

参考文献:

[1] ULUDAG U, PANKANTI S, PRABHAKAR S, *et al*. Biometric cryptosystems: Issues and challenges [J]. IEEE, 2004, 92(6): 948-960.

[2] JUELS A, SUDAN M. A fuzzy vault scheme [C]// International Symposium on Information Theory(ISIT). Lausanne, Switzerland: IEEE Press, 2002: 408.

[3] SCHEIRER W J, BOULT T E. Cracking fuzzy vaults and biometric encryption[EB/OL]. [2007-05-06]. http://www.vast.uccs.edu/~tboult/PAPERS/Scheirer-Boult-BCC07-Crack-Fuzzy-Vault.pdf.

[4] RATHA N K, CHIKKERUR S, CONNELL J H, *et al*. Generating cancelable fingerprint templates[J]. IEEE Transaction on Pattern analysis and machine intelligence, 2007, 29(4): 561-572.

[5] CLANCY T, LIN D, KIYAVASH N. Secure smartcard-based fingerprint authentication[C]// Proceeding of ACM SIGMM Workshop on Biometric Methods and Applications. Berkley, CA: ACM Press, 2003: 45-52.

[6] ULUDAG U, JAIN A. Fuzzy vault for fingerprints[C]// 5th International Conference, AVBPA 2005. New York: Springer, 2005: 310-319.

[7] ULUDAG U, JAIN A. Securing fingerprint template: Fuzzy vault with helper data[C]// Proceeding of Computer Vision and Pattern Recognition Workshop. New York: IEEE Press, 2006: 163-166.