ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.6, June 2009, pp.1553−1573
doi: 10.3724/SP.J.1001.2009.03528

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

生物特征模板保护*

李 鹏[1,2], 田 捷[1,2,3+], 杨 鑫[1,2], 时 鹏[1,2], 张阳阳[1,2]

[1](复杂系统与智能科学重点实验室 中国科学院 自动化研究所,北京 100190)

[2](中国科学院 研究生院,北京 100049)

[3](电子工程学院 西安电子科技大学,陕西 西安 710071)

Biometric Template Protection

LI Peng,[1,2] TIAN Jie[1,2,3+], YANG Xin[1,2], SHI Peng[1,2], ZHANG Yang-Yang[1,2]

[1](Key Laboratory of Complex Systems and Intelligence Science, Institute of Automation, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

[3](School of Electronic Engineering, Xidian University, Xi'an 710071, China)

+ Corresponding author: E-mail: tian@ieee.org

Li P, Tian J, Yang X, Shi P, Zhang YY. Biometric template protection. *Journal of Software*, 2009,20(6): 1553−1573. http://www.jos.org.cn/1000-9825/3528.htm

Abstract: This paper reviews the state-of-the-art of biometric template protection technology domestic and abroad, and then systemizes almost all the related research directions. First it is clarified that the underlying disadvantages of traditional biometric systems and the attacks they are vulnerable to. Then the necessity and difficulty of protecting biometric template are drawn naturally. Afterwards this paper classifies the methods and algorithms into various categories based on the operation manner, and elaborates specifically some representative ones, such as Biohashing and Fuzzy Vault and so on. In the experiment, evaluations of Biohashing and Fuzzy Vault are carried on different fingerprint databases, and the results show the advantages and disadvantages of Biohashing method, as well as our improved Fuzzy Fingerprint Vault's better performance and security on FVC2002 DB2.
Key words: biometric; template protection; key; helper data; biohashing; fuzzy vault

摘 要: 对当前国内外生物特征模板保护技术发展的现状进行综述和探索,对该方向的研究内容进行详细的梳理和分类.首先阐述传统生物特征识别系统存在的本质缺陷和易于遭受到的攻击的形式,进而从理论上引出了生物特征模板保护的必要性及其难点所在.然后以模板保护算法的具体操作方式为分类标准,详细阐述了当前在这个领域出现的比较有代表性的算法,诸如 Biohashing 和模糊保险箱(Fuzzy Vault)等.通过实验验证了 Biohashing 算法的优势和缺陷,并且在 FVC2002 DB2 数据库上对提出的改进 Fuzzy Vault 算法进行了验证,结果表明,该算法在识别率和安

* Supported by the National Natural Science Foundation of China under Grant Nos.60621001, 60875018 (国家自然科学基金), the National High-Tech Research and Development Plan of China under Grant No.2008AA01Z411 (国家高技术研究发展计划(863)); the Hundred Talents Program of the Chinese Academy of Sciences (中国科学院百人计划); the Beijing Municipal Natural Science Foundation of China under Grant No.4091004 (北京市自然科学基金)

Received 2008-09-01; Accepted 2008-11-28

全性方面均达到了国际先进水平.

关键词: 生物特征;模板保护;密钥;辅助数据;biohashing;模糊保险箱

中图法分类号: TP301 **文献标识码:** A

1 引 言

随着全球经济和信息技术的不断发展,越来越多的领域需要可靠的身份鉴别.信息化时代的一大特征就是身份的数字化和隐性化,如何准确鉴定一个人的身份,保证信息安全,是信息化时代亟待解决的一个关键问题.在这种需求下,人类所固有的各种各样的生物特征逐渐为人们所认识并开始进行研究,生物特征识别技术也因此获得了长足的发展.随着生物特征识别系统应用的逐渐深入,在为身份认证带来安全和便捷之外,也逐渐暴露出了其本身所固有的一些难以解决的问题,比如假生物特征的攻击,模板一旦丢失则难以重新发布等一系列潜在威胁,这些威胁的存在已成为制约生物特征识别技术进一步发展的瓶颈.

1.1 生物特征和生物特征识别系统

传统的身份认证方法包括基于“你所拥有的”和“你所知道的”两类方式,前者如身份证等,后者如口令、密钥等.身份证容易遗失或者被人伪造,而口令、密钥容易忘记,并且过短的口令容易被猜出,过长的口令(一般称为密钥)不容易被猜出但是存在着记忆不方便的问题,从而又带来了密钥保管方面的问题,一般长密钥都保存在密钥卡上,并且用一个短的口令加以保护,因此,实质上身份认证的安全性还是依赖一个短的口令.

生物特征[1]是“你所固有的”特征,包括人的生理特征和行为特征两大类,其中生理特征如指纹、脸形、虹膜、掌纹、语音等,行为特征主要有步态、签名、击键等,都吸引了大批学者进行了广泛而深入的研究.而生物特征识别技术就是为了进行身份认证而采用自动技术测量人的生理特征或是行为特征,并将这些特征与数据库的模板数据进行比较,从而完成认证的一种解决方案.

在计算机普及应用之前,主要靠人工专家来识别生物特征(如美国的FBI就拥有大量指纹识别专家).而随着生产力的发展和信息技术的普及,使用计算机进行的自动生物特征识别就成为大势所趋,其中自动指纹识别系统(AFIS)是人们首先研究的识别系统.典型的生物特征识别系统包括离线注册和在线识别两部分,如图 1 所示.离线注册部分包括信号采集、特征提取和模板存储等步骤,在线识别包括信号采集、特征提取、配准和模板比对等步骤.生物特征系统对身份的认证有两种模式:认证(1:1)和识别(1:N).认证方式检验“你是否是你所声称的那个人”,而识别方式检验“你的身份信息在这个数据库里吗?你是谁?”,这两种方式在算法处理的时间复杂度方面有较大的差距.

为了评测生物特征识别系统的性能,需要引入真匹配(genuine match)和假匹配(imposter match)的概念.真匹配是来自于同一个个体的不同的样本进行比对,而假匹配是来自不同个体的样本进行比对,从而产生了生物特征识别系统的两类基本的错误:错误匹配(false match)和错误非匹配(false non-match).错误匹配是指假匹配被认定为真匹配,也叫误识;错误非匹配是真匹配被认定为假匹配,也叫拒识.错误匹配率(false match rate,简称 FMR),也叫误识率(FAR),是统计学意义上错误匹配发生的概率;同样,错误非匹配率(false non-match rate,简称 FNMR),也叫拒识率(FRR),是统计学意义上错误非匹配发生的概率.特定的系统可以通过设定不同的阈值来控制参数FMR 和 FNMR,这两个参数是相互影响的,在安全性级别要求不同的场合可以进行相应的参数调整.另外一个衡量系统整体性能的指标是等错误率(equal error rate,简称 EER),FMR 和 FNMR 相等时的值,反映了系统的整体准确率和用户的接受度等重要性能.为了直观地反映不同参数水平下系统的性能,通常将不同参数水平的 FMR 和 FNMR 画到同一张图上,即 ROC 曲线(receiver operating characteristic curve).ROC 曲线和直线 $y=x$ 的交点就是 EER 的位置所在.

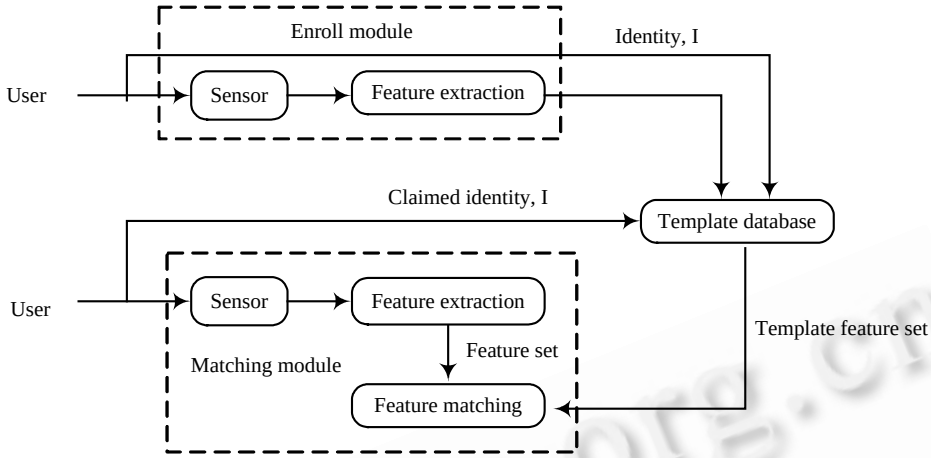


Fig.1 Enroll model and matching module of biometric system

图 1 生物特征系统的注册模块和比对模块

1.2 传统生物特征识别系统的缺陷

传统的生物特征识别系统(以指纹为例)在识别的精度和速度上已经完全可以达到实用的要求,第 4 届国际指纹识别竞赛(FVC2006)[2]中,Open和Light算法的性能均有较大幅度的提高,大部分算法都可以实用化.但是,传统的指纹识别系统大部分采用细节点(minutiae)作为识别特征,并且将细节点的位置、方向等信息以裸数据的形式存储到模板中用于比对.由于传统的系统不采用任何加密措施,系统中存储的是原始的细节点坐标和方向值,因而随着硬件攻击和破解技术的发展,整个生物特征识别系统就有可能完全暴露在黑客的攻击范围内,从而使用户身份的安全性和隐私性受到威胁.生物特征不像口令和密钥,丢失后可以重置,生物特征的丢失是永久性的丢失.已有文献表明,完全可以自动地从指纹细节点模板恢复出原始的指纹图像[3],从而对生物特征识别系统的模板安全提出了更高的要求.除了模板安全方面的威胁以外,生物特征识别系统还面临着其他多种类型的攻击.

Maltoni 等人[4]在指纹识别专著中分析了指纹识别系统易于受到的攻击类型.作者把这些攻击大致分为以下几种类型:

1) 规避:入侵者避开系统的认证功能,非法侵入系统内部,修改合法用户的敏感数据,使得攻击性匹配的成功率增加.
2) 欺骗:高级权限用户(比如管理员)登录系统后,修改普通用户的敏感数据,并且宣称系统遭受到了黑客攻击.比如,银行职员可以登录到金融系统并且修改客户的账户余额,然后谎称入侵者攻击了银行网络并且修改了数据.
3) 共谋:高级权限用户(管理员)和入侵者非法勾结.管理员非法修改用户的生物特征数据或系统参数,使得入侵者成功攻击系统的几率增加.
4) 强迫:攻击者使用暴力强迫用户开放自己的权限,使得攻击者可以随意进入系统.
5) 拒绝服务:攻击者使用某种手段耗尽系统的资源,使系统无法为合法用户提供服务.比如,攻击者组织巨量的非法请求使得服务器的硬件资源被悉数占用,导致无法响应合法用户的正常响应.

以上几种类型只是从宏观的角度给出了系统容易受到的攻击形式,不仅生物特征识别系统容易遭受这些攻击,普通的加密系统也不能幸免,没有具体的针对性.

Ratha 等人[5]特别对生物特征识别系统易于受到的攻击进行了具体分析,并把它们分成了 8 类.如图 2 所示.

图 2 具体给出了生物特征识别系统容易受到的 8 类攻击.类型 1 是给系统提供假的生物特征(指纹、人脸、虹膜等),尤其是假指纹(fake finger),是当前国际研究的热点,目前还没有很好的方法可以解决用假指纹来攻击生物特征系统的问题;类型 2 用预先注入的生物特征来替代现场采集的生物特征;类型 3 篡改特征提取器,使之

生成攻击者希望的特定的特征向量;类型 4 在系统中使用合成的特征向量来代替特征提取器得到的特征向量;类型 5 人为地修改匹配器.使之能够更容易地输出一个较高的匹配分数;类型 6 主要是对生物特征模板数据库进行攻击,比如修改、删除、增加某些模板等;类型 7 攻击数据库和匹配器之间的传输信道,使得匹配获得的输入并不是数据库中存储的模板;类型 8 改写匹配器的 0/1 二值响应,这种类型的攻击是利用了传统生物特征系统简单的二值输出,很容易达到 50%的攻击成功率.

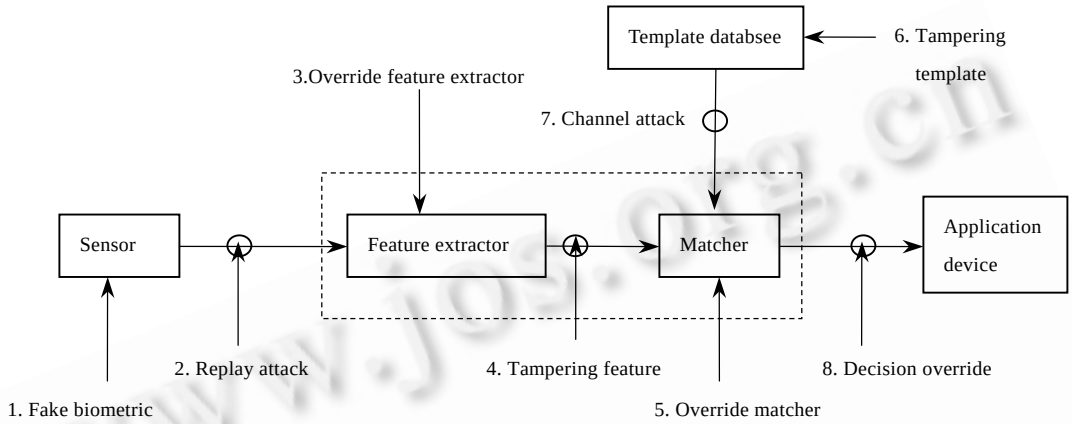


Fig.2 Eight types of attacks sensitive to biometric recognition system (from Ref.[5])

图 2 生物特征识别系统易于遭受的 8 类攻击(来自文献[5])

目前的生物特征加密技术还不能完全防范以上列举的所有类型的攻击,当前的研究热点是保护生物特征模板的安全.其中最为典型且成熟的方法是将密钥与模板有机地融合在一起,使两者都不容易受到攻击,从而达到保证生物特征识别系统安全性的目的.

由于生物特征系统存在上面的隐忧,可以说生物特征在某种程度上已经从“你所固有的特征”逐渐退化为“你所拥有的特征”.而普通的口令和密钥反而可以通过密码学意义上的处理而克服这种危险.UNIX 操作系统中对用户密码的保护就是一个很好的例子.在 UNIX 操作系统中,用户口令 P 不以明文形式存储,而是存储 P 的哈希值 $H(P)$,这样就可以通过比较口令的哈希值来认证用户的身份.而即使是系统的管理员也无法获取用户的口令 P,只能看到 $H(P)$.生物特征由于用户样本类内差较大,不可能直接通过 Hash 函数的加密方式来保护.但是将生物特征科学和密码学相结合,为保护生物特征模板的安全性提供了一条可行的途径.越来越多的研究者意识到了这一点,但是密码学所要求的精确性和生物特征所固有的模糊性之间的矛盾成为了两者结合的最大障碍.如何克服这一矛盾并且能够保证系统的身份认证性能,就是形形色色的生物特征模板保护算法所研究的内容.

1.3 生物特征模板保护技术及其分类

理想的生物特征模板保护技术需要满足以下几点要求[6]:1) 变换后的模板不能通过逆变换来获得原始模板的数据;2) 变换后的模板必须可以应用在不同的数据库中,使得它们之间不能交叉匹配;3) 变换后模板一旦丢失,管理员可以将其作废,并立即用同样的生物特征来发布新的变换模板;4) 变换后模板的身份认证性能不能比原始模板下降得太多.

Uludag 等人[7]比较详细地分析了生物特征加密技术所要解决的问题,即如何在生物特征的模糊性和密码机制的精确性之间寻找一个比较可靠的折衷方案,并且回顾了之前出现的几种算法,比较了它们的优劣性.但是,最近在这个领域又有较大的发展.文献[8]也大致回顾了生物特征加密的发展脉络.Tomko等人[9]是目前所知的第 1 篇致力于此领域的文献.而在国内,王星明等人将加密的概念引入了生物特征识别中,并且进行了开创性的研究[10].

生物特征模板保护技术有许多分支,本文将其大致分为 3 类:

(1) 生物特征哈希(biohashing)[11−28];

(2) 模板形变技术[6,29−39];

(3) 基于辅助数据的理论和方法[40−54],又可以分为密钥绑定和密钥生成两类.

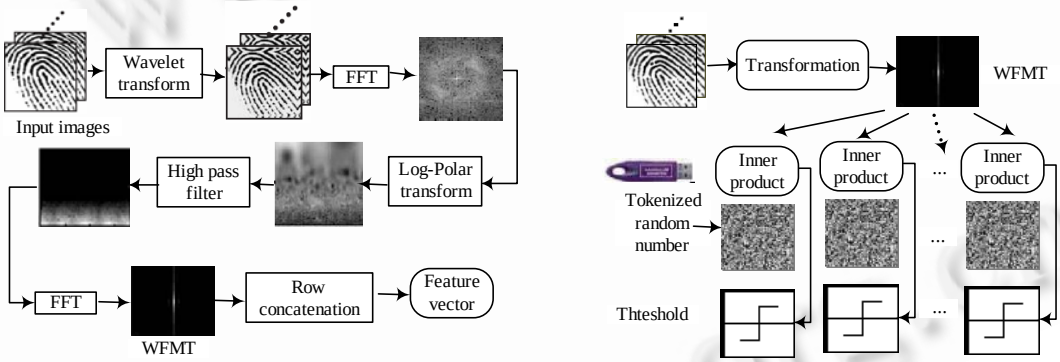
本文对生物特征模板保护技术作了广泛而深入的调研.第 2 节对生物特征模板保护领域具有代表性的理论和算法进行回顾,分别是生物特征哈希、模板形变技术和基于辅助数据的理论方法.第 3 节实现了 Biohashing 和 Fuzzy Vault 算法,并且在公开的数据库上进行了实验测试.最后一节给出结论和未来的研究方向.

2 代表性的理论和算法回顾

本节重点介绍迄今为止国内外学术领域出现的比较经典的生物特征模板保护理论和算法.分 3 小节来叙述,分别是:双因子认证方法——Biohashing、模板形变技术以及基于辅助数据的理论和方法.

2.1 双因子认证方法——Biohashing

Teoh等人[11]提出了使用指纹和随机数结合的双因子身份认证方法.其基本思想是使用指纹图像的小波傅里叶梅林变换特征(wavelet-fmt feature)和存储在用户身份令牌中的一组伪随机数进行迭代内积,产生一组对应特定用户的二值序列,通过比较二值序列来达到身份认证的目的.算法中之所以选择WFMT特征,是因为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转化为沿坐标轴的平移.获取指纹WFMT特征的步骤如图 3(a)[11]所示.



(a) Flowchart of generating fingerprint's WFMT feature

(a) 产生指纹 WFMT 特征的方块图

(b) Flowchart of generating Hashing Key with iterative inner product

(b) 迭代内积产生 Hashing Key 的过程

Fig.3

图 3

首先输入多枚指纹图像,分别经过小波变换、快速傅里叶变换、对数极坐标变换、高通滤波、快速傅里叶变换得到WFMT特征,再进行连接,就可以得到指纹图像经过变换后的特征向量.这个向量因为经过了对数极坐标变换,所以对于指纹的平移、旋转和尺度变化都具有不变性.使用内置在用户令牌内部的随机数种子产生装置生成一组伪随机数,然后用得到的特征向量与随机数向量进行迭代内积,如果内积值大于某个阈值τ,则设为 1,否则设为 0.这样就得到了一组 01 二值向量.这个过程如图 3(b)[11]所示.这种算法完全符合模板可以撤销的要求,一旦用户的身份令牌(即随机数)丢失,可以随即更换另外一个,这样就和更换密码、挂失身份证书一样方便了.

作者通过一系列实验来验证密钥(hashing key)的认证性能,说明使用hashing key来进行比对的性能丝毫不逊于使用原始的指纹细节点特征.但是对这种算法的主要批评在于,如果攻击者获取到用户的身份令牌(与该用户绑定的伪随机数向量组就存储在其中),那么整个算法的性能就会大为降低[12,15,18],这说明在Biohashing算法中起主要作用的是伪随机数向量组,而不是指纹本身,这背离我们使用生物特征进行身份认证的本意.关于这个

问题,我们会在实验部分通过实验结果进行详细讨论.

Lumini 等人[12]也注意到了上面提到的用户的身份令牌丢失的情形,并且通过最坏情况下(假设攻击者B获得了用户A的身份令牌,试图使用A的随机数和B的指纹进行身份验证)的一系列实验,得出了结论:随机数丢失情况下的问题可以通过扩展hashing key的长度来解决.然后提出了 4 项改进措施以扩展key的长度,分别是:1) 对生成的生物特征向量(作者使用DCT变换处理人脸图像)进行正交化处理;2) 把原来方法中的固定阈值τ扩展为一个范围,从 $\tau_{\max}$ 到 $\tau_{\min}$ 设为 p 个值,步长 $\tau_{\text{step}}=(\tau_{\max}-\tau_{\min})/p$;3) 增加投影空间:采用把投影空间数目增加到 k 的方法来使 key 的长度增加到原来的 k 倍;4) 特征置换:对生物特征向量进行 q 次排列,可以得到 q 个特征向量.如果上述所有措施都采用,则可以获得一组长度为 $k\cdot p\cdot q$ 的 hashing key,比对是使用汉明距来训练一组分类器,最后用加和规则来把这些分类器融合在一起.这样就极大地增加了 hashing key 的长度,解决了原有算法所存在的问题.扩展 key 长度的过程可以如图 4 所示.

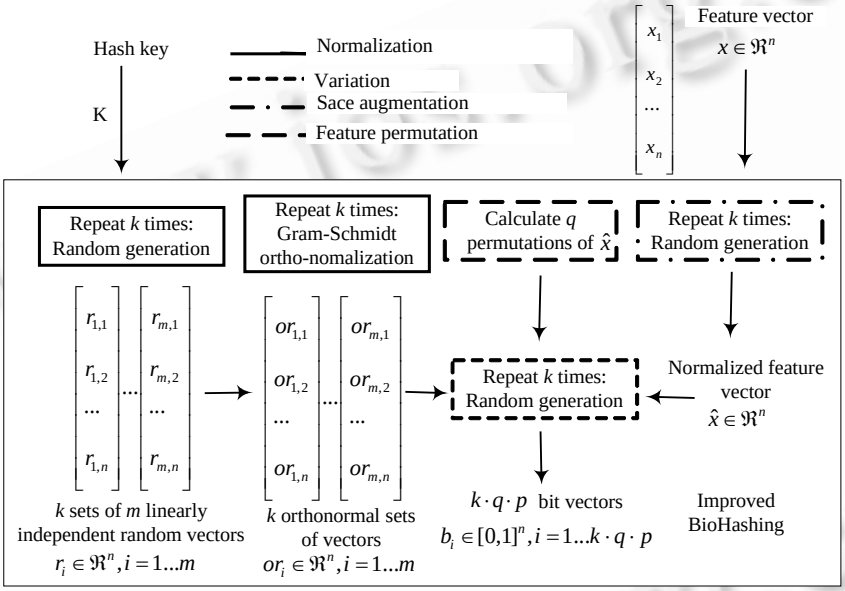


Fig.4 Flowchart of improved Biohashing (from Ref.[12])

图 4 改进后的 Biohashing 算法流程图(来自文献[12])

Biohashing算法最初是针对指纹提出来的,但是算法本身所要求的高区分性的定长特征在指纹中非常难以提取.FingerCode[13]是定长的,但是区分性不高,不能在随机数丢失的情况下保证认证性能[12].其他生物特征,如人脸、掌纹的Biohashing算法相继被提出并进行了相关研究[14−22].一些新技术也被应用于Biohashing算法中,如概率神经网络(PNN)[23]、格雷编码技术[24,25].多模态融合和多特征融合技术也被应用于Biohashing,以解决随机数丢失情况下EER过高的问题[26−28].

2.2 模板形变技术

Ang 等人[29]提出了将指纹细节点模板进行对折的几何变换的方法.该方法将一个密钥k映射为直线的斜率,与指纹图像的奇异点一起确定一条直线,然后将指纹的细节点模板沿着这条直线对折,即将直线一侧的细节点映射到另一侧,得到形变后的模板.在FVC2002 库上的实验表明,该方法的EER大约为 17%左右,比形变之前的4%下降了一些.这种方法的缺点在于它需要检测奇异点,而奇异点本身是难以精确检测的,所以会引入连带误差,而且某些类型的指纹没有奇异点(例如平拱型指纹).另外,使用普通的匹配方式对于处理对折后的模板也存在一些不太妥当的地方,例如会有对折后正好重合的细节点被覆盖.

Ratha等人[6,30]提出了另一种模板形变的方法.其基本思想是把指纹的细节点集合从原始空间中采用单向

函数变换到另外一个空间中去,把变换后的细节点集存储到模板中,在变换空间中进行细节点的比对.所采用的变换可以是一个单向函数族$f(k)$,其中$f(\cdot)$代表从原始空间到变换空间的单向变换函数,而k代表相应的参数集合.一旦系统中使用的变换参数k_1丢失,可立即使用另一组参数k_2进行替换,符合模板保护技术的要求.Ratha等人最终采用叠加的Gaussian核函数的叠加来作为单向变换函数.从概念上讲,如图 5 所示,如果把细节点分布在一张带坐标的白纸上,那么这个变化就可以比作用较小的力把这张白纸揉皱,而细节点落在揉皱的白纸上的坐标,作为模板进行保存.受这个形象的概念的启发,Ratha等人选用Gaussian核函数叠加的方法来进行变换.叠加的Gaussian核函数如式(1)、式(2):

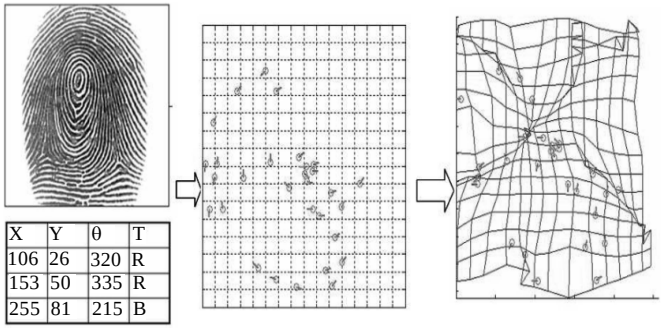
$$\left|\vec{\mathrm{F}}(z)\right| = \sum_{i=1}^{K} \frac{\pi_i}{\left|2\pi\Lambda_i\right|} \exp\left\{-\frac{1}{2}(z-\mu_i)^T \Lambda_i^{-1}(z-\mu_i)\right\} \tag{1}$$

$$\Phi_F(z) = \frac{1}{2}\arg\left\{\nabla\vec{F}\right\} + \Phi_{rand} \tag{2}$$

在实际进行实验的过程中,选用 IBM99 光学数据库,作者随机选用了 24 个 Gaussian 函数,这些函数的标准差都是 50 像素,函数中心被随机放置于 512×512 的图像表面,而峰值分别随机选为+1 或–1.这样,变换函数的每一组参数包含 456 比特(24×(9+9+1)).经过实验研究表明,变换后模板的认证性能 EER 可以达到 10%左右,而不同的变换方式之间的比对的 EER 也在 15%以下.但是,目前典型的 AFIS 在平均质量的光学数据库上的 EER 都可以达到 5%甚至更低.文中并没有给出原始模板的比对性能,而且使用的数据库也不是公开的,所以无法对比这个方法真正的性能参数.但是,这种方法最大的缺点是在配准阶段.众所周知,单纯使用奇异点进行配准是非常不精确的,而且像拱形(arch)指纹根本没有奇异点可以提取.而在加密域内对指纹进行配准是一个非常困难的问题,因为它不可能像传统方法那样使用指纹的所有信息,比如使用全部细节点进行配准,而且还要求达到一定的配准精度,所以寻找一种使用指纹的少量特征信息就可以达到很好的配准精度的方法,对于指纹加密算法的发展会起到很大的推动作用.文献[31,32]也延续了这种思想,对奇异点形变和匿名模板的生成进行了研究.

Ratha等人的方法之所以其性能比原始模板降低了一些,是因为形变后的细节点位置和预期产生了偏差,如果想要达到原始模板的比对性能,则必须对形变函数进行额外的配准,但是这种配准是很难控制的.Lee 等人[33]提出了一种不需要对形变进行额外配准的方法.该方法利用指纹细节点的局部信息的旋转和平移不变性,产生针对于用户的细节点方向和位置的变换函数,应用于细节点模板,产生变换后的模板,然后使用普通的点匹配的方法来比对变换后的模板,如果模板指纹和查询指纹能够保持一致变换,就可以在变换空间内进行模板匹配.如图 6 所示,以细节点为圆心画一组r_k个同心圆环,以细节点的方向为极坐标系的极轴,在每个圆环上等间隔地取s个采样点,记录每个采样点相对于细节点的方向值作为特征向量.这样可以生成对应于第i个细节点的局部方向向量F_i.假设用户拥有一个密钥PIN,可以使用伪随机生成器产生一个向量U_{PIN},其维数与F_i相同.对两个向量进行归一化,即$u_{PIN}=U_{PIN}/|U_{PIN}|$,$f_i=F_i/F_i|$.然后进行操作 $m_i = f_i \circ u_{PIN}$,其中∘代表内积,这样就得到了该用户指纹图像第i个细节点的不变的形变参数 m_i .细节点的形变量由两个与用户相关的(即由用户的PIN决定的)函数——距离形变函数L_{PIN}和角度形变函数 Θ_{PIN} 来决定.为了产生这两个函数,首先把m_i在其取值范围上以T为间隔等分,假设分为n份.然后用PIN伪随机生成两个n+1 维向量 $X=[x_0,x_1,...,x_n]$ 和 $Y=[y_0,y_1,...,y_n]$,其中x_i和y_i范围分别是 $[-\beta,-\alpha]\mathrm{U}[\alpha,\beta]$ 和 $[-\eta,-\gamma]\mathrm{U}[\gamma,\eta]$.对于L_{PIN}和 Θ_{PIN} ,在每一个间隔点上都产生一个控制点,得到控制点向量 $L_{PIN(nT)}$ 和 $\Theta_{PIN(nT)}$,计算方法见式(3).

$$\begin{aligned} L_{PIN(nT)} &= x_0 + x_1 + ... + x_{n-1} + x_n = \sum_{i=0}^{nT} x_i \\ \Theta_{PIN(nT)} &= y_0 + y_1 + ... + y_{n-1} + y_n = \sum_{i=0}^{nT} y_i \end{aligned} \tag{3}$$



X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

Fig.5 Minutiae are placed throughout a plane paper and "crawled" with a local smooth but global non-smooth function (from Ref.[6])

图 5 细节点被放到白纸上然后揉皱,采用局部平滑但全局不平滑的函数(来自文献[6])

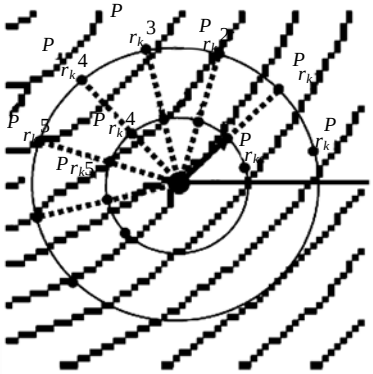


Fig.6 Translation and rotation invariant local orientation vector (from Ref.[33])

图 6 对旋转和平移不敏感的细节点局部方向场向量(来自文献[33])

得到两个控制点向量后,就可以利用线性插值的方法来计算任意 m_i (位于[−1,1]内)的距离变换值和角度变换值.假设$m_i=p$位于$(k-1)T$和kT之间,则距离形变值和角度形变值分别为

$$\begin{aligned} L_{PIN}(p) &= \frac{p-(k-1)T}{T}(L_{PIN}(kT)-L_{PIN}((k-1)T))+L_{PIN}((k-1)T),\ (k-1)T<p<kT \\ \Theta_{PIN}(p) &= \frac{p-(k-1)T}{T}(\Theta_{PIN}(kT)-\Theta_{PIN}((k-1)T))+\Theta_{PIN}((k-1)T),\ (k-1)T<p<kT \end{aligned} \tag{4}$$

该方法的实验部分使用 FVC2002DB1 数据库,挑选前 30 个手指,共 30×8=240 枚指纹.算法的适用性从认证准确度和可变性两个方面来反映,使用 EER 和可分性 Separability 两项指标来衡量.在认证准确度方面,取参数 $\alpha=0,\beta=5,\lambda=0,\eta=5$ 时,系统性能达到最好,EER=5.7%,Separability=2.2.在可变性方面,取参数 α=15,β=20,λ=15,η=20 时系统性能达到最好,EER=3.1%,Separability=2.8.可以通过参数的选取来达到各方面性能的折衷.然而,这种方法仍然不能降低密钥丢失情况下系统被攻击的风险.

Tulyakov等人提出的适用于细节点模板的对称哈希函数[34,35]也属于模板形变技术的一种.作者提出了一种对细节点模板进行对称哈希变换并且在哈希空间内进行匹配的方法,由于模板中细节点的无序性,所以哈希函数的输入也不依赖于顺序(即对称).作者使用了一族对称哈希函数,可以从中随机选取一个或者几个来使用,式(5)即为一族哈希函数:

$$\begin{aligned} &h_1(c_1,c_2,...,c_n)=c_1+c_2+...+c_n \\ &h_2(c_1,c_2,...,c_n)=c_1^2+c_2^2+...+c_n^2 \\ &... \\ &h_m(c_1,c_2,...,c_n)=c_1^m+c_2^m+...+c_n^m \end{aligned} \tag{5}$$

其中, $c_i(i=1,2,...,n)$ 是复数,表示细节点的结构信息.假设经过哈希之后的细节点模板保留了原始模板的配准参数,并且使用投票的方法求得相应的旋转和平移参数,同时确定最相似的哈希值作为对应的模板对,求出其相似度,然后得到全局相似度.作者把这种方法扩展到了密钥绑定方法的范畴中,引入双因子认证的概念,通过特定用户的密钥建立一族哈希函数和细节点结构对之间的随机关系,使得不同的用户之间细节点结构的哈希函数的对应关系不同,从而达到加强安全性的目的.在实验阶段,作者使用FVC2002DB1的100×8=800枚指纹,分别测试了 3 种情况下的细节点哈希函数的性能,分别是:1) 结构中包含 2 个细节点,1 个哈希函数;2) 结构中包含 3 个细节点,1 个哈希函数;3) 结构中包含 3 个细节点,2 个哈希函数.最好的性能是第 3 种情况下获得的,EER=3%,而原始不经过哈希的系统性能为 1.7%,经过融合后的系统性能是 1.9%,基本达到了实际应用的要求.关于这种算法的安全性分析,由于算法实用的方程组中方程个数比变量个数(细节点结构个数)要少,说明不能通过这种

方程组来求解原始的细节点信息.另外,分析了算法对于爬山攻击的鲁棒性,而并没有通过确切的数学分析来给出哈希之后的模板(helper data)泄漏的原始模板的信息熵.但是毫无疑问,这样的方程组泄漏了细节点模板的信息,虽然不能精确解出方程的解,但却可以通过最优化的算法来缩小细节点的搜索范围,然后采用小范围的暴力攻击就有可能使系统被破解.

2.3 基于辅助数据(helper data)理论与方法

根据密钥的使用方式或者产生方式的不同,又可以分为密钥释放(key release)、密钥绑定(key binding)、密钥生成(key generation)3 种具体方法.其中,密钥绑定往往将生物特征信息与外部输入的密钥绑定,进而产生Helper Data,并且往往涉及到密钥恢复的过程;而密钥生成则专注于从模板生物特征信息(template)中提取Helper Data,而密钥并不从外部输入,而是在 Helper Data 的协助下,从查询的生物特征信息(query)中提取出来.

2.3.1 密钥释放(key release method)

密钥释放的方法就是把密钥和生物特征简单地叠加在一起,存储为加密的生物特征模板.而在模板内部,并不对密钥和生物特征做任何复杂的操作,只是简单地叠加.如图 8(a)所示.假如与另外一种加密方式——密钥绑定(key binding,图 8(b))进行对比,这种差别就很明显了[36].

由于密钥释放的方法在理论上十分简单,所以很难抵御对模板的蓄意攻击.假如数据库模板被破解,那么用户的生物特征信息和密钥都将丢失.从理论上严格来说,这种方法并不具备比传统生物特征识别系统更高的安全性.

Moon等人[37]详细讨论了基于指纹的USB身份令牌的硬件需求和软件架构.但是,鉴于目前硬件技术的发展还不能达到破解生物特征模板数据库的层次,所以目前这种方法有一定的应用价值,而且在某种意义上达到了双因子认证(指纹+令牌)的效果,把用户的物理身份和数字身份以较低的安全性结合在一起.国内外有一些科研机构和公司、组织在从事指纹USB Key的研发,少数已经产品化并投放市场,在金融和电子商务、电子政务等领域得到了广泛的应用.

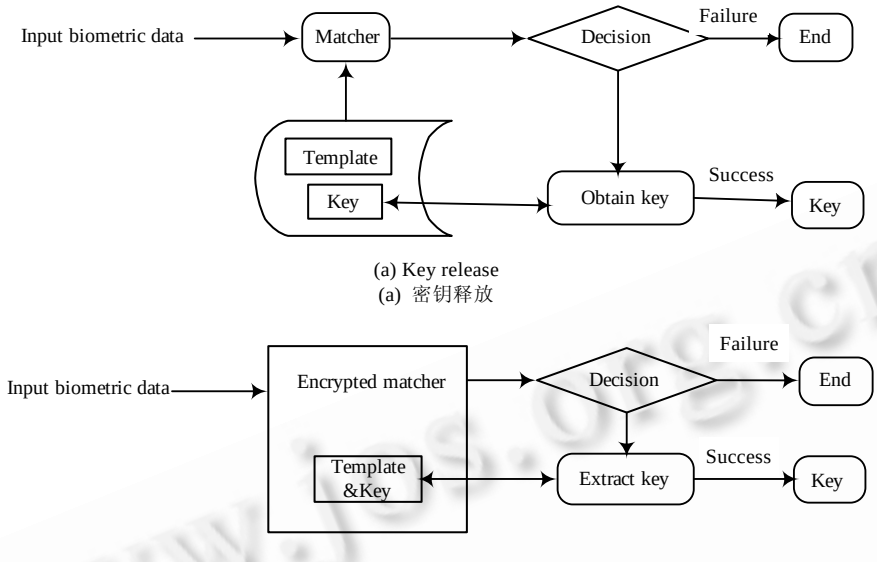
2.3.2 密钥绑定(key binding method)

如图 7(b)所示,密钥绑定的方法在数据库模板中将生物特征数据和密钥数据以某种方式(比如按位异或)有机地结合在一起,只有当生物特征匹配成功时密钥才被以相应的算法提取出来,用于其他场合.当生物特征匹配失败时,系统会输出一个拒绝信号.这里,密钥和生物特征模板经过绑定后形成所谓的辅助数据(helper data),在认证阶段辅助查询生物特征恢复出密钥.

(1) Bioscrypt™算法

Bioscrypt™算法[38]是Soutar等人于 1998 年提出来的,是生物特征加密领域最早的实用化算法之一.算法的基本思想是基于图像处理和傅里叶变换的.算法分为加密和解密两个步骤.加密步骤(如图 8(a)[40]所示).算法在注册步骤把用户的指纹图像与一个密钥绑定在一起,如果认证步骤成功,密钥则被释放出来.算法首先设计了一个相关滤波函数 $H(u)$,这个函数由幅值和相位两部分构成,即 $|H(u)|\mathrm{e}^{-i\varphi(|H(u)|)}$ 和 $\mathrm{e}^{-i\varphi(H(u))}$,这个函数的设计标准是形变误差和区分性,分别是为了使拒识率(FRR)和误识率(FAR)达到最小.然后用一个随机生成的、只包含相位并且与 $\mathrm{e}^{-i\varphi(H(u))}$ 大小相同矩阵 A 与 $\mathrm{e}^{-i\varphi(H(u))}$ 做点乘,得到 $H_{stored}(u)$,同时,将幅值信息 $|H(u)|$ 抛弃,这个过程消除了从$H(u)$反向生成指纹图像的可能.算法同时计算训练指纹图像(来自同一枚手指的 5 幅图像)和$H(u)$的卷积(相关性)得到一个输出$c_0(x)$,为了处理认证阶段的信号变化,使用纠错码技术将$c_0(x)$的元素进行二值化得到c_0,然后把c_0和一个随机生成的N-bit(典型的是 128-bit)密钥k_0绑定在一起生成查找表LT.k_0同时也作为S bits的 $H_{stored}(u)$ 的加密密钥,所得到的结果再进行哈希操作(使用标准加密函数SHA-1 或者Triple-DES)生成一个身份码 id_0 .最后同时把 $H_{stored}(u)$,LT,id_0存储到数据库内作为加密后的生物特征模板,作者称其为Bioscrypt.在解密阶段,如图 8(b)所示,用户输入一枚或多枚(一般是5枚)指纹图像,系统从模板中把 $H_{stored}(u)$ 提取出来,两者结合在一起计算出一个相关性输出$c_1(x)$,然后对照模板中的查找表LT从$c_1(x)$中提取出新的密钥k_1.然后与注册阶段的做法一样,k_1被用来创建一个新的身份码id_1.如果id_0=id_1,则k_1被释放出来;否则,返回“认证失败”的消息,而不向系统中

释放任何错误的密钥.

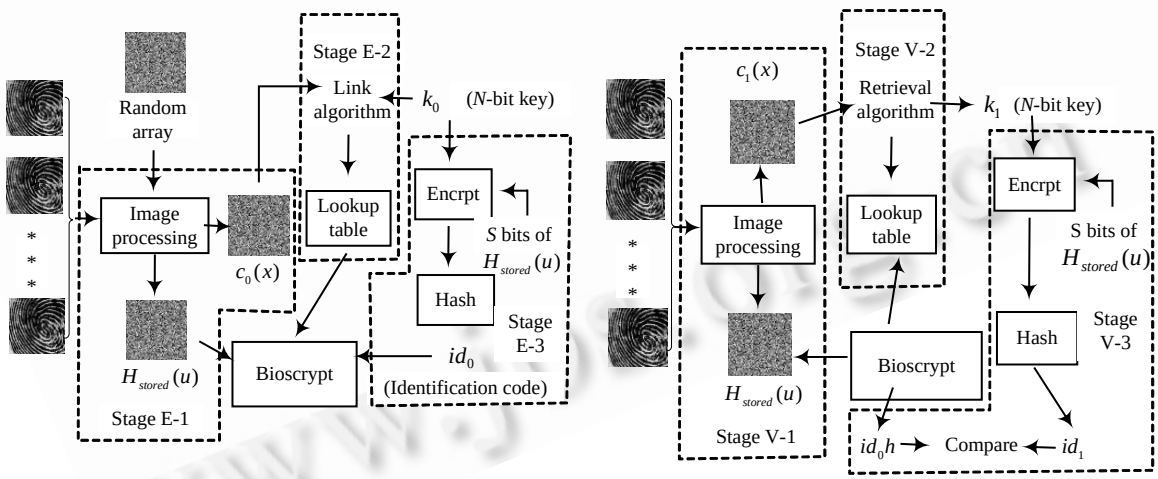


(a) Key release
(a) 密钥释放

(b) Key binding
(b) 密钥绑定

Fig.7 Two key-related encryption methods (from Ref.[37])

图 7 与 key 相关的两种加密方式(来自文献[37])



(a) Encryption phase of Bioscrypt algorithm
(a) Bioscrypt 算法的加密过程

(b) Decryption phase of Bioscrypt algorithm
(b) Bioscrypt 算法的解密过程

Fig.8

图 8

对这种算法的批评主要集中在文献[39,42]中,批评者认为这种算法并不能严格地保证系统的安全性,作者并没有解释算法在加密阶段的熵损失(entropy loss),而且算法的拒识率和误识率都没有明确给出.另外,作者在实验过程中假设对应的指纹图像是预先配准好的,事实上,这一点在当前的图像采集条件下仍然很难做到.

(2) 模糊承诺(fuzzy commitment)方案

Juels和Wattenberg提出了一种模糊承诺方案[40].这是一项较早的(1999 年)理论研究成果,将纠错码技术与

生物特征结合在一起形成一种典型的密钥绑定方案.这个方案是由密码学的比特承诺方案(bit commitment scheme)延伸而来的,并借用了其中的承诺、证据等概念,将其用于生物特征这种本质上模糊(fuzzy)的数据中.模糊承诺方案包含两个步骤:承诺和解承诺.在承诺步骤中,首先从某种纠错码体系中选择一个码字c,长度和生物特征向量ω相同,定义偏差$\delta=\omega-c$,则承诺:$\{hash(c),\delta\}$,其中$hash(\cdot)$是哈希函数.在解承诺步骤中,用户输入一个生物特征向量ω',从承诺中解出一个码字c',计算公式是:$c'=\omega'-\delta=\omega'-\omega+c$,如果$\omega$和$\omega'$在某种距离测度(比如汉明距)下足够接近,即$dist(\omega-\omega')<thr$,其中$thr$是一定的距离阈值,经过某种纠错码的处理,则可认为$c'$与$c$一致,并可以通过校验哈希值$hash(c')$与$hash(c)$是否相等来判断认证是否成功.

基于模糊承诺方案,Hao等人[41]设计并实现了一套虹膜加密方案.相对于指纹来说,虹膜更适合于进行加密研究,因为虹膜有更为规范的编码结构IrisCode,这个结构有2048-bit的固定长度,可以直接和密码学的一些方法结合起来生成加密后的模板,加解密操作非常方便.如图9所示,Hao等人的算法也非常直接,但是效果很好.这种方法采用了双因子认证的思想,使得只有将令牌和虹膜同时提供给系统,才能认证成功,任何一种因子丢失,都不会威胁到系统的安全性.在加密阶段,首先选取一个key,经过Reed-Solomon和Hadamard级联编码后产生一个加密后的2048-bit的密钥,之后与同样为2048-bit的虹膜进行异或操作,所得的结果存储为模板,并且抛弃原始的key.解密阶段把用于比对的虹膜和模板进行异或,然后进行Hadamard和Reed-Solomon级联解码,如果用于比对的虹膜和原始的虹膜来自同一个人,那么经过解密后,$k'=k$.该算法经过了两层编码和解码操作,容错性更强.虽然该算法没有采用特别的方法,但却达到了非常好的效果,在FAR=0的情况下,FRR可以达到0.47%,并且能够产生长度为140比特的密钥.

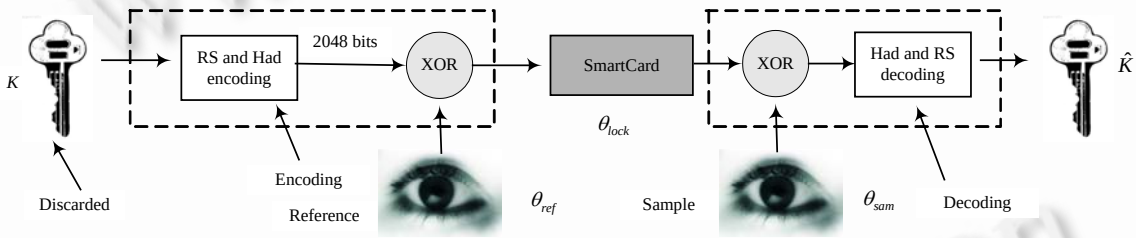


Fig.9 Two-Layer iris encryption flowchart (from Ref.[41])

图 9 双层虹膜加密流程(来自文献[41])

(3) 模糊保险箱(fuzzy vault)方案

这是生物特征加密领域最为经典的实用化方案,很多研究者的工作都是基于这个方案的.

这种算法是Juels和Sudan[42]在模糊承诺方案的基础上提出来的,算法最大的特点就是fuzzy,这个特点很好地把生物特征的模糊性和密码算法的精确性联系了起来.概括地说,这种算法可以分为两个步骤:1) 用户Alice将秘密K放到保险箱(vault)中,并且用无序集A加以锁定;2) 用户Bob使用无序集B尝试访问K(即打开保险箱vault).Bob能够访问到K的充分必要条件是无序集B和A的绝大多数元素重合.

算法的具体实现过程可以描述如下:

a) 加密保险箱:用户 Alice 选择关于 x 的多项式 p 来加密 K,然后计算无序集 A 在多项式 p 上的投影 $p(A)$,这样$(A,p(A))$就构成一个有限点集.然后随机生成一些杂凑点(chaff point)与先前生成的点集一起形成R,这就是所谓的保险箱 Vault,杂凑点对于隐藏秘密 K 是非常必要的,并且其数量要远远大于真实点.

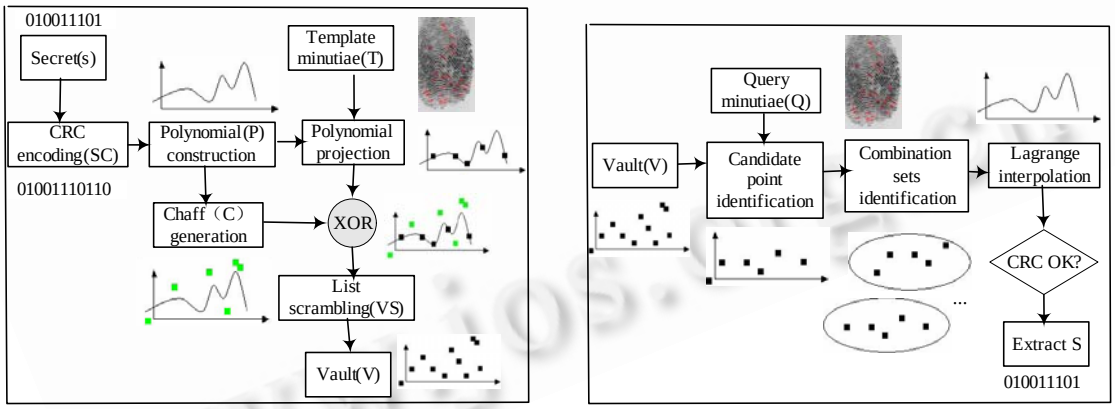
b) 解密保险箱:用户 Bob 使用自己的无序集 B,如果 B 和 A 绝大多数的元素重合,那么 B 中有许多点就会落在多项式 p 上,使用纠错码技术,Bob 就能重构出 p 来,进而获取秘密 K.但是,如果 B 和 A 有相当大比例的元素不重合,那么重构出 p 是相当困难的.

这种算法的安全性是基于多项式重构问题的.之所以特别适用于生物特征数据,是因为它使用无序集(比如指纹的细节点等)工作,并且能够处理集合之间(元素数量和元素本身)的误差.

Clancy等人[43]在Juels工作的基础上提出了指纹保险箱(fingerprint vault)的概念.注册阶段使用用户的 5 枚指纹进行,算法提取指纹细节点的位置作为输入,使用受限的最近邻算法来处理多枚指纹特征之间的对应问题.在考虑指纹按压区域面积和方差d之后,作者把N个杂凑点加入到细节点集中,这些杂凑点距离细节点的距离以及它们相互之间的距离都至少为d,这些点形成了加密后的指纹保险箱.与Juels等人不同,Clancy等人给出了指纹域多项式次数的具体描述.在解密阶段,提取用于比对的指纹细节点特征,使用受限的最近邻算法,寻找到指纹保险箱中对应的点,然后对应的点作为R-S纠错码算法的输入来计算出被加密多项式的正确形式.作者这项工作的贡献在于具体描述了Fuzzy Vault算法在指纹域的实现方法,并且在 20%~30%的拒识率的基础上达到了69-bit的安全性.与文献[39]一样,其弱点也在于假设指纹图像都已经预先配准过,并且也没有报告实验中所使用的指纹图像是否在真实条件下采集.

Yang等人[44−46]使用细节点结构和基于奇异点的配准方法构建了Fuzzy Fingerprint Vault.

Uludag等人[47]基于Fuzzy Vault和Fingerprint Vault提出了更为实用化的Fuzzy Vault for Fingerprint,其基本思想与Juels的Fingerprint Vault一脉相承,但是在一些实现的具体细节上又有所不同.该算法的加密步骤如图10(a)[49]所示.首先使用循环冗余校验(CRC)对秘密S进行处理,就是S尾部加上特定位数的校验码形成SC,然后使用SC按照一定的规则构造多项式函数P.另一方面,提取用于加密指纹模板图像的细节点位置(x,y),级联横坐标和纵坐标即 $x|y$,找到$x|y$在P上的投影点,即$(x|y,P(x|y))$,随机添加一组不在P上并且距离真实点一定距离的杂凑点到保险箱中,就形成了最终的保险箱V.解密步骤如图 10(b)[49]所示.在解密步骤中,首先提取用于比对的指纹图像中细节点位置(x,y),级联横坐标和纵坐标即 $x|y$,然后寻找保险箱V中和它们对应的点,找到若干组待定的点,使用Lagrange插值法重构出相应的多项式,进而用循环冗余校验(CRC)来确定哪一组是初始阶段加密的S.与Clancy的方法相比,该算法使用CRC而不是RS correction code来进行纠错,并且可以达到 15%的拒识率(误识率为 0),可以加密 128 比特的AES密钥,但是相应地也会带来更高的时间复杂度.与前面两种方法一样,该方法所达到的认证性能也是在假设使用的指纹图像预先配准之后做到的,而且并没有给出系统可以达到的安全性水平.



(a) Encoding phase of fuzzy vault for fingerprint

(a) Fuzzy vault for fingerprint 加密过程

(b) Decoding phase of fuzzy vault for fingerprint

(b) Fuzzy vault for fingerprint 解密过程

Fig.10

图 10

鉴于之前所有的方法都使用人工专家配准的方法来完成实验,Uludag等人[48]首先提出了使用计算机自动方法在加密域内对指纹图像进行配准.该方法的基本思想就是从指纹图像中提取Helper Data用以配准,Helper Data的选取标准是既能反映指纹的部分本质特征,又不足以凭借这些特征恢复出原始的指纹图像或者用以识别的其他特征(比如细节点特征).作者首先提取指纹图像的方向场流曲线(orientation field flow curves),方向场流曲线反映了指纹脊线的走向,是指纹的本质特征之一.然后,根据方向场流曲线来估计每一条脊线上的局部曲

率最大点,所得到的曲率值加上所在点的横、纵坐标构成了所谓的Helper Data.由于噪声的影响,所得到的Helper Data可能会在局部不能反映脊线走向,所以有必要滤除那些“伪Helper Data”,只保留曲率值较大并且位于奇异点附近的备选点.这样一组特征既反映了指纹脊线走向这样一种本质特征,又不足以让攻击者仅凭这些不完全的特征反向恢复出指纹原始图像或者细节点特征,符合在加密域内进行配准的思想.得到Helper Data之后,作者使用迭代最近点(iterative closest points,简称ICP)的方法进行配准,得到比对指纹和模板指纹之间的配准参数,进而用到细节点特征中去,就达到了在加密域内自动配准指纹图像的目的.

Nandakumar 等人[50]注意到了普通Fuzzy Vault系统不够安全、易于被潜在的高级用户利用并攻击等弱点,提出了在Fuzzy Vault系统外围添加一层口令(password)保护的想法,并且在新的特征模板中存储的是经过形变的细节点参数,而不是原始数据,这个形变参数与用户所设置的口令相关.密码机制基本上与Fuzzy Vault的安全性独立,使得系统处于双重机制的安全性保护之中,攻击者只有同时攻破两层系统后才能获取到合法用户的信息,从而使得系统的安全性和隐私性有了很大的提高.作者报告的系统性能也比较好,使用了FVC2002-DB2和MSU-DBI进行实验室,分别在n=7和n=10时达到最佳性能(n代表用于构造Fuzzy Vault的多项式次数),与普通的Fuzzy Vault系统相比,经过增强的系统拒识率有一定的提高,但是其代价是算法时间复杂度的提高.

Nandakumar 等人[50]综合了以前一系列的工作,对Fuzzy Vault进行了优化和实现,达到了目前最好的综合性能.性能优化主要体现在以下几个方面:1) 使用可变界限盒的细节点匹配器,替代以前方法中简单地按照欧式距离搜索的方法,对于形变等误差的容错性更好;2) 在细节点表达方式上引入方向,构成一个三元的细节点信息(x,y,θ),其中x和y代表细节点位置,θ代表方向.把细节点信息引入了三维空间中,使得Chaff点的可选位置大大增多,同时增强了系统的安全性;3) 使用细节点局部质量判断函数,将细节点按照质量分数从高到低依次排列,这样大大缩短了解密时的搜索耗时,同时也提高了匹配的成功率;4) 修改了Helper Data提取步骤中的流方向曲线的计算方法,使得提取出的脊线曲率最大点更加精确,提高了配准精度.实验测试选用FVC2002DB2和MSU-DBI两个数据库.结果显示,在FVC2002DB1上系统的性能达到了90%以上;在MSU-DBI的性能也达到了将近90%的水平.与以前的工作相比,认证的准确率方面有了较大幅度的提高.但是,有文献指出,这种实现方法对于原来架构的某些修改,比如使用循环冗余校验CRC代替Reed-Solomon码降低了系统的安全性[51],系统的实际安全性比文献[42]达到的69-bit有所下降,建议使用哈希函数来进行密钥正确性的校验.

Li等人[52]提出了一种基于奇异点拓扑结构的指纹加密域配准方法,较大地提高了配准精度,同时,不泄漏指纹模板的信息.关于这项工作,我们会在实验验证部分进行详细介绍.

Fuzzy Vault逐渐被推广到其他生物特征上[53−55].文献[53]介绍了如何将Fuzzy Vault的思想引入到带有加权的人脸PCA(principal component analysis)特征中来,作者引入了一个所谓的“中间层(intermediate layer)”,使得权值大的特征会构造出更多的点,同时使用了SHA-1函数来对由特征和其相应权值构造信息进行哈希,但是并没有具体的实验验证.文献[54]用两个随机规范正交的矩阵(R_1,R_2)将人脸的PCA特征进行二值映射,得到一定数目的16-bit长度的二值特征,用于Fuzzy Vault的编码和解码.作者考虑了两种情形:1) 不依赖于用户数据,即所有的用户均使用同样的(R_1,R_2)来进行特征二值化;2) 依赖于用户数据,即不同的用户使用不同的(R_1,R_2),亦即双因子认证.实验阶段作者使用ORL人脸数据库进行,在第1种情形下获得最好的EER为5%,而第2种情形下可以达到EER=0的水平.文献[55]将Fuzzy Vault的概念应用于虹膜上,作者使用基于ICA(independent component analysis)的特征提取方法和K均值的模式聚类方法获得了16个27-bit长度的虹膜特征.实验验证阶段使用自建的BERC虹膜数据库,规模是99×10=990幅图像,获得了FAR=0的情况下,FRR=0.775%的性能.

Fuzzy Vault已经成为生物特征模板保护领域最有潜力的方法之一,研究和应用也逐渐广泛,相应的攻击策略也开始受到一些研究者的关注[56−59].文献[56]定性地介绍了生物特征系统易于遭受的几种攻击形式,包括多数据库相关攻击、密钥盗取攻击和混合替代攻击等,并且分别把这些新型的攻击方式应用到Fuzzy Vault和生物特征加密系统中去.文献[57]中针对多数据库相关攻击这种具体的形式进行了实验,使用 200×2=400 枚指纹,通过比较同一个手指对应的两个Vault来得到真实细节点的分布,获得了 59%的成功率,说明Fuzzy Vault系统以大于一半的概率会遭受到数据库相关攻击的威胁,如果使用 3 个或 3 个以上的相关数据库,则成功率会更高.文献

[58]通过数学分析证明了Fuzzy Vault同样不能防范一些比较聪明的暴力攻击,并且给出了改进的建议.文献[59]通过观察Vault中所有点的统计特性来区分真实细节点和Chaff点,认为Chaff点比真实点更容易集中,并且用数学分析和实验验证的手段证明了可以使用远小于暴力攻击的搜索次数来找到真实的细节点.上述所有的攻击,都是由于Vault中包含了真是细节点信息,也就是有一定的熵损(entropy loss),但是如果通过某种变换手段不存储真实细节点,这些攻击也就无从下手了.

2.3.3 密钥生成(key generation method)

上面所述两种机制都是采用生物特征和密钥(Key)进行结合的方式,就是说需要有从外部输入一个随机或有特定含义的Key,然后与生物特征以某种方式结合在一起,一旦生物特征认证成功,原有的Key就会被释放,从而可以用到身份认证等其他场合中去,达到了双因子认证的高度安全性,也是实现物理身份和数字身份统一的比较理想的方式.同时,正是因为这两种机制中所需的Key是从外部输入的,才带来了潜在的安全问题,如果生物特征和Key结合的方式不是十分理想,导致Key在认证过程中起主导作用,那么系统的安全性就是基于Key的,一旦Key丢失,系统即告崩溃.基于以上分析,同时生物特征作为一种近似随机的信号,人们考虑可以直接从这种信号中提取出一个Key,而不采用外部输入的方式.我们称这种方式为密钥生成机制.

Dodis等人[60]提出了Secure Sketch(安全梗概(作者译,可能不十分精准))和Fuzzy Extractor(模糊提取器)两个概念,试图解决把随机的生物特征信号转变成可以应用于任意加密环境的稳定密钥,以达到可靠、安全的认证用户身份的目的.Secure Sketch(安全骨架)从生物特征信号中提取出一定量可以公开的信息,这个操作可以容忍一定程度的误差,一旦输入与原始的模板相似的信号,这些公开的信息可以用来完美重建出原始模板,但是单凭这些信息不足以重构出原始模板.Fuzzy Extractor(模糊提取器)从输入的生物特征信号中提取出近似均匀分布的随机信号R,这样的R可以作为一个Key应用到所有的加密环境中去.

为了构造具体算法,为不同的生物特征信号提供有效的度量标准,Dodis在文中使用了3种测度空间,分别是汉明距(hamming distance)、集合差(set difference)、编辑距(edit distance).在汉明空间下,Dodis把Juels和Wattenberg[24]构造的Fuzzy Commitment看作近似最优的安全梗概,并且使用一般性的构造方法把它改造成近似最优的模糊提取器.在集合空间下,上节提到的Fuzzy Vault可以看作是近似最优的安全梗概算法,作者应用同样的构造方法把它转化成了近似最优的模糊提取器.在编辑空间下,作者定义了从编辑空间到集合空间的变换,从而把集合空间的最优模糊提取器转化到了编辑空间.这是理论性的贡献,并且证明了可以在熵损(entropy loss)满足一定条件的情况下构造最优的安全梗概和模糊提取器.

文献[61–66]也都致力于密钥生成方法的研究.文献[67,68]分别从指纹的FingerCode特征和细节点结构特征中提取鲁棒的密钥,进行了实用化算法的初步尝试,虽然结果不是十分理想,却为这个方向的研究做出了探索性的贡献.文献[69]实现了基于虹膜的模糊提取器,分析了虹膜特征编码之间的差异对正确鉴别性能的影响,设计了重复码和Reed-Solomon码的两层级联纠错编码方案,从虹膜特征中提取出了4 096 bit长度的密钥.

2.3.4 加密算法适用性及性能比较

上面的叙述概括了目前出现的绝大部分生物特征加密算法.从理论上讲,没有任何一种算法能够满足所有生物特征模板保护的要求,也没有任何一种算法能够适用于所有安全级别的要求.所以说,没有完美的生物特征模板保护技术.在对生物特征模板加密时,需要根据不同的生物特征、不同的信号表达形式以及相应的应用场合作出合理的算法选择.表 1 总结了各种生物特征保护的理论和方法针对不同生物特征、不同的信号表达形式、距离测度方式、密钥使用方法、配准模式和典型实现的性能等各方面的比较数据.

Table 1 Comparative data of various biometric template protection methods

表 1 各种生物特征模板保护算法的比较数据

Method	Trait	Signal representation	Distance mesure	Key employing	Alignment	Performance
Biohashing[11]	Finger-Print	WFMTfeature	Hamming distance	Dimension reduction	Without alignment	Best case: *EER*=0, Worst case: *EER*≈30%
Biohashing[12]	Finger-Print	FingerCode[11]	Hamming distance	Dimension reduction	Pre-Alignment	Best case: *EER*≈1%,Worst case: *EER*≈15%
	Face	KL/DCT transform	Hamming distance	Dimension reduction	Pre-Alignment	Worst case: *EER*≈8%,
	Signature	Global&local feature	Hamming distance	Dimension reduction	Pre-Alignment	Best case: EER≈0%,Worst case: EER≈8%
Fuzzy vault[43]	Finger-Print	Minutiae	Set difference	Generating polynomial	Pre-Alignment	*FRR*=20%~30% (*FAR*=0)
Fuzzy vault[46]	Finger-Print	Minutiae & local structure	Set difference	Generating polynomial	Singularity	*FRR*≈10% (*FAR*=0)
Fuzzy vault[48]	Finger-Print	Minutiae	Set difference	Generating polynomial	Helper data	*FRR*≈15% (*FAR*=0)
Fuzzy vault[50]	Finger-Print	Minutiae	Set difference	Generating polynomial	Helper data	*FRR*≈10% (*FAR*=0)
Ang,*et al*.[29]	Finger-Print	Minutiae	Hamming distance	Generating random line	Pre-alignment	*EER*≈17%
Ratha,*et al*.[6]	Finger-Print	Minutiae	Hamming distance	Generating Gaussian function	Singularity	*EER*≈15%
Lee,*et al*.[33]	Finger-Print	Minutiae	Hamming distance	Generating change fuction	Without alignment	*EER*≈5%
Tulyakov, *et al*.[35]	Finger-Print	Minutiae	Hamming distance	Generating hash function	Encrypted data	*EER*≈3%
Hao,*et al*.[41]	Iris	IrisCode	Hamming distance	Generating random vector	Pre-alignment	*EER*≈0.47%

3 算法实现及实验研究

3.1 Biohashing算法的实现和研究

在实验部分,我们将通过对Biohashing算法[9]的实现来说明生物特征加密算法在隐私性、安全性的意义上比传统的生物特征识别要高,前者识别性能也不逊于后者.但是也证实了在极端情况下(B偷取了用户A的身份令牌,并且试图使用A的随机数向量和自己的指纹来伪装成A的身份),Biohashing算法的性能会大为降低.考虑到算法对指纹图像的质量要求比较高,实验选用意大利Blogona大学生物特征实验室开发的指纹合成软件SFinGe2.5 合成的数据库,其中选取 40 个手指,每个手指合成 10 枚指纹,共 400 幅像素为 288×384 的指纹图像.实例图像如图 11 所示.先对合成的图像进行去噪、增强等预处理,然后以奇异点为中心剪裁 128×128 的图像作为Biohashing算法的输入图像.如图 12 所示.

我们分别设计了 4 种类型的匹配实验来验证算法的性能.第 1 种称为真-真匹配(genuine-genuine match),在这种情况下,我们把每个手指的前 4 枚指纹进行融合作为模板,然后与隶属于每个手指的 10 枚指纹进行比对,两者所结合的随机数种子相同,共进行 10×40=400 次比对操作;第 2 种是所谓的假-假匹配(imposter-imposter match),这种情况使用每个手指的第 1 枚指纹作为模板,然后与其他手指的第 1 枚指纹进行比对,且两者结合的随机数种子不同,共需进行 $\sum_{i=1}^{39} i = 780$ 次比对操作;第 3 种是真-假匹配(genuine-imposter match),这种情况把每个手指的前 4 枚指纹进行融合作为模板,分别与属于当前手指的 10 枚指纹进行比对,但是比对的指纹和模板结合的随机数种子不同,共需进行 10×40=400 次比对操作;第 4 种情况称为假-真匹配(imposter-genuine match),这种情况使用每个手指的第 1 枚指纹作为模板,与其他手指的第 1 枚指纹进行比对,但是两者需结合相同的随机数种子,共需进行 $\sum_{i=1}^{39} i = 780$ 次比对操作.在这些实验做完以后,分别绘制归一化的直方图来观察比对结果.

(a) Left rotation type (b) Right rotation type (c) Whorl type

(a) 左旋型 (b) 右旋型 (c) 漩涡型

Fig.11 Fingerprint samples generated by SFinGe

图11 SFinGe合成的指纹图像示例

Fig.12 Fingerprint image ROI after being enhanced and cropped

图 12 经过增强和剪裁后的指纹图像 ROI 示例

假设攻击者B想要获取系统中用户A的资料,并且在最坏的情况下假设B对系统的实现算法非常了解,然后我们考虑安全应用现实中的3种情况:1) B既没有A的指纹信息,也不知道A的随机数向量;2) B拥有A的指纹信息,但是不知道A的随机数向量;3) B没有A的指纹信息,但是知道A的随机数向量.这3种情况下我们分别考察系统的安全防护性能,如图13所示.由图中我们很容易看出,A和B两种情况下算法的表现很好,但是情况C下算法就不能很好地区分两种分布,这说明如果用户的随机数向量(也就是身份令牌)丢失,那么系统安全很有可能会受到威胁.正如我们在描述Biohashing算法中所提到的,这说明在这个算法中随机数向量所起的作用要比生物特征大,从某种意义上说这与单纯使用令牌进行身份认证没有太大的差别,没有体现出使用生物特征进行身份特征的优势.之所以会出现上面的情况,我们分析是由于算法所采用的特征是指纹的小波-傅立叶梅林变换特征(WFMT),这种特征属于全局特征,而众所周知,大部分指纹识别算法的优势在于指纹的细节特征(细节点、汗孔等),所以会导致指纹的类间差很小,不能很好地区分不同用户的指纹.我们考虑如果用更能体现指纹类间差的特征来替换原有特征,则算法的性能可能会表现得好一些,这个想法有待进行进一步的实验加以证实.

3.2 Fuzzy Vault算法研究和改进

我们实现了Nandakumar等人[50]的Fuzzy Vaul算法,并且在以下几方面作了改进:1) 使用SHA-1 哈希函数[70]替换CRC校验,提高系统的安全性能;2) 利用局部图像质量和脊线结构相结合的方式来筛选细节点,从而保证模板中细节点的个数和质量;3) 提出一种基于奇异点邻近拓扑结构的方法来进行加密域内的配准.

图 14 显示了基于奇异点拓扑结构的配准方法.随着指纹顺时针旋转$\Delta\theta$的角度,以中心点P为圆心的拓扑结构中脊线上各个采样点s_i也随之以同样的角度旋转.可以看出,虽然s_i的位置和方向场θ_i都发生了改变,但是P和s_i之间的连线距离l_i,以及θ_i与连线l_i之间的夹角β并没有发生变化.其中,由几何知识可知,模板指纹与查询指纹之间对应的两个夹角之间的差值也是相同的.

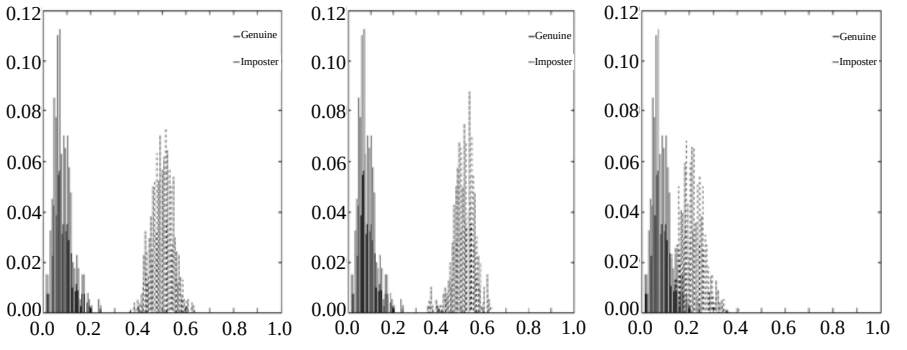


Fig.13 Biohashing's performance in three cases

图 13 3 种情况下系统的安全防护性能表现

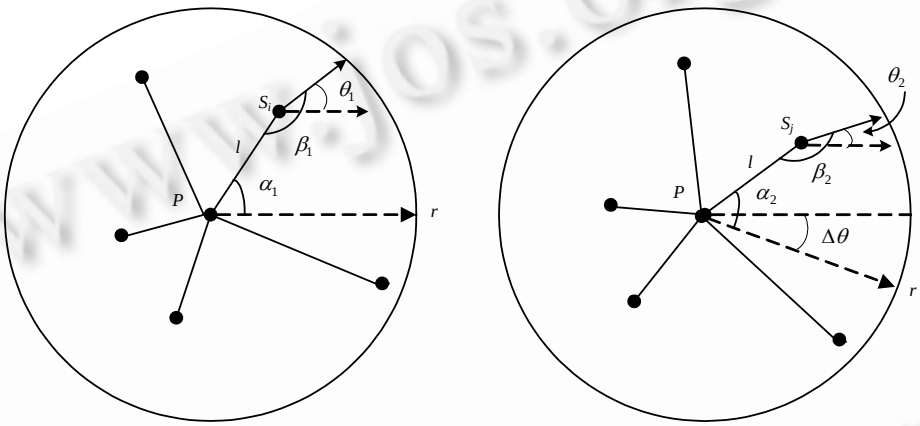


Fig.14 Rotation alignment based on core point structure

图 14 基于中心点结构的旋转配准

$$\alpha_1-\alpha_2=\theta_1-\theta_1=\Delta\theta \tag{6}$$

因此,提取向量 H 作为 Helper Data,H 的定义为

$$H=\{l_i,\alpha_i,\beta_i\}_{i\le n} \tag{7}$$

其中,α_i 为 l_i 的方向,n为采样点的个数.得到Helper Data之后,对于模板Helper Data向量集H_T和查询指纹向量集H_Q,采用Luo等人[71]提出的弹性限界盒的方法进行配准,求出偏转角度$\Delta\theta$,具体步骤为:

① 在H_T中,从采样圆的 0°角开始,沿逆时针方向旋转,将采样点依次编号为s_i.从s_1开始,遍历H_Q中所有的采样点 s,根据弹性限界盒找出能够与$\{l_i,\alpha_i,\beta_i\}$相匹配的采样点;

② 完成遍历,在找到所有能够匹配的杆结构之后,将其中一对可以匹配的杆配准,求出此时的偏转角$\Delta\theta$,将查询指纹中其他所有杆同时偏转$\Delta\theta$,记录能够与模板指纹中匹配上的采样点的数量;

③ 能够使最多数目的采样点匹配上的角度α,并通过比较查询指纹和模板指纹的α之间的差值得出旋转角度$\Delta\theta$,就是最终求出的指纹旋转参数.

实验采用FVC2002 DB2,由于本文算法可以仅用一幅指纹图像注册,并用一幅指纹图像进行查询即可完成配准和解密运算,也可以用同一个手指的两幅不同图像进行融合注册,用一幅指纹图像进行查询.因此,在加、解密实验中采用一对一和二对一的加解密实验来测试Fuzzy Vault算法性能.多项式的阶数选择对能够保存密钥的长度和安全性有重要的影响.例如,Nandakumar[50]等人指出,当n=8 时,可以对长度为 128 比特的密钥加密.与此同时,由于在解密过程中如果查询指纹和模板指纹有n+1 个细节点匹配成功,则Fuzzy Vault解密成功,所以n还

对Fuzzy Vault算法的错误率有很大的影响.对算法在不同阶数情况下进行了多次比较实验,综合考虑算法的安全性和比对性能.

在实验中,通过不同的场景设计分别测试本文所提出算法的识真率(genuine accept rate,简称 GAR)和误识率(false accept rate,简称 FAR).由于指纹模板保护技术要求的特殊性,本算法对于指纹模板保护安全性要求很高,所以要求误识率极低才能够保证算法的安全性.因此,相对于普通 FVC 测试标准而言,对于相似度比对的门限阈值设置较高,在不同测试环境下得到的 FAR 都非常低,这样才能够达到有效保护模板的目的.表 2 给出了我们的算法在 FVC2002 DB1 库上的实验结果.

Table 2 Fingerprint fuzzy vault's experimental results on FVC2002 DB2

表 2 FVC2002 DB2 上指纹 Fuzzy Vault 加解密实验

	n=7		*n*=8		*n*=9	
	GAR (%)	FAR (%)	GAR (%)	FAR (%)	GAR (%)	FAR (%)
Our method (1template,1query)	92	0.30	92	0.06	90	0.02
Our method (2template,1query)	95	0.34	95	0.09	93	0.04
Ref.[50]'s method (1template,1query)	91	0.13	91	0.01		
Ref. [50]'s method (2template,1query)	95	0.12	94	0.02		
	n=10		*n*=11			
	GAR (%)	FAR (%)	GAR (%)	FAR (%)		
Our method (1template,1query)	89	0.01	87	0		
Our method (2template,1query)	91	0.03	89	0		
Ref.[50]'s method (1template,1query)	86	0				
Ref.[50]'s method (2template,1query)	88	0				

4 结论和展望

本文对生物特征模板保护技术出现的背景、理论依据等作了比较详细的阐述,较为完整地介绍了当前比较流行和实用的算法.国内外的研究者在这个新兴的交叉领域已经取得了一定的研究成果,而且还在逐步地完善当中.生物特征模板保护技术具有很大的潜力和优势,能够满足商业机构和政府组织等对身份认证和信息安全方面的高级需求,但是要想做到更为精准、可信,还有很多的工作要做,包括进一步完善现有的加密方案以及提出更加合理的新方案,还要开发出更多的实际系统来验证这个理论在实践中的有效性.

References:

[1] Tian J, Yang X. Biometric Recognition Theory and Application. Beijing: Publishing House of Electronics Industry, 2005 (in Chinese).

[2] Results in FVC2006. http://bias.csr.unibo.it/fvc2006/

[3] Cappelli R, Lumini A, Daio D, Maltoni D. Fingerprint image reconstruction from standard templates. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2007,29(9):1489−1503.

[4] Maltoni D, Maio D, Jain A, Prabhakar S. Handbook of Fingerprint Recognition. New York: Springer-Verlag. 2003. 281−283.

[5] Ratha N, Connell JH, Bolle RM. An analysis of minutiae matching strength. In: Josef B, Fabrizio S, eds. Proc. of the Int'l Conf. on Audio and Video-based Biometric Person Authentication. Berlin: Springer-Verlag, 2001. 223−228.

[6] Ratha N, Chikkerur S, Connell J, Bolle R. Generating cancelable fingerprint templates. IEEE Trans. on Pattern Analysis And Machine Intelligence, 2007,29(4):561−572.

[7] Uludag U, Pankanti S, Prabhakar S, Jain A. Biometric cryptosystems: Issues and challenges. Proc. of the IEEE, 2004,92(6): 948−960.

[8] Cavoukian A, Stoianov A. Biometric Encryption: A positive-sum technology that achieves strong authentication, security and privacy. Technical Report, Office of the Information and Privacy Commissioner of Ontario, 2007.

[9] Tomko G, Soutar C, Schmidt G. Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, 1996.

[10] Wang X, Tian J, Wu Y. The application in network security of secure cryptosystem scheme integrated with automatic fingerprint authentication. Computer Application, 2000,2:53−54 (in Chinese with English abstract).

[11] Jin A, Ling D, Goh A. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition ,2004,37:2245−2255.

[12] Lumini A, Nanni L. An improved BioHashing for human authentication. Pattern Recognition, 2007,40:1057−1065.

[13] Jain A, Prabhakar S, Hong L, Pankanti S. FingerCode: A filterbank for fingerprint representation and matching. In: Baldwin T, Sipple RS, eds. Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition, Vol.2. New Jersey: IEEE Computer Society. 1999. 187−193.

[14] Jin A, Goh A, Ling D. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2006,28(12):1892−1901.

[15] Nanni L, Lumini A. Empirical tests on BioHashing. Neurocomputing, 2006,69(16-18):2390−2395.

[16] Connie T, Jin A, Goh A, Ling D. PalmHashing: A novel approach for dual-factor authentication. Pattern Analysis & Applications, 2004,7(3):255−268.

[17] Jin A, Ling D. Cancellable biometerics featuring with tokenised random number. Pattern Recognition Letters, 2005,26(10): 1454−1460.

[18] Nanni L, Lumini A. Random subspace for an improved BioHashing for face authentication. Pattern Recognition Letters, 2008,29(3): 295−300.

[19] Jin A, Ling D, Goh A. Personalised cryptographic key generation based on FaceHashing. Computers & Security, 2004,23(7): 606−614.

[20] Jin A, Ling D, Goh A. An integrated dual factor authenticator based on the face data and tokenised random number. In: Proc. of the ICBA 2004. LNCS 3072, 2004. 117−123.

[21] Ling D, Jin A, Goh A. Eigenspace-Based face hashing. In: Proc. of the ICBA 2004.LNCS 3072, 2004. 195−199.

[22] Ling D, Jin A, Goh A. Biometric Hash: High-Confidence face recognition. IEEE Trans. on Circuits And Systems for Video Technology, 2006,16(6):771−775.

[23] Lumini A, Nanni L. An advanced multi-modal method for human authentication featuring biometrics data and tokenised random numbers. Neurocomputing, 2006,69(13-15):1706−1710.

[24] Jin A, Toh K, Yip W. 2*N* Discretisation of biophasor in cancellable biometrics. In: Proc. of the ICB 2007. LNCS 4642, 2007. 435−444.

[25] Jin A, Yip W, Lee S. Cancellable biometrics and annotations on BioHash. Pattern Recognition, 2008,41(6):2034−2044.

[26] Maio D, Nanni L. Multihashing, human authentication featuring biometrics data and tokenized random number: A case study FVC2004. Neurocomputing, 2005,69(1-3):242−249.

[27] Lumini A, Nanni L. An advanced multi-modal method for human authentication featuring biometrics data and tokenised random numbers. Neurocomputing, 2006,69(13-15):1706−1710.

[28] Nanni L, Lumini A. A multi-modal method based on the competitors of FVC2004 and on palm data combined with tokenised random numbers. Pattern Recognition Letters, 2008,29(9):1344−1350.

[29] Ang R, Rei S, Luke M. Cancelable key-based fingerprint templates. In: Proc. of the ACISP 2005. LNCS 3574, 2005. 242−252.

[30] Ratha N, Connell J, Bolle R, Chikkerur S. Cancelable biometrics: A case study in fingerprints. In: Proc. of the 18th Int'l Conf. on Pattern Recognition (ICPR 2006). New Jersey: IEEE Computer Society, 2006. 370−373.

[31] Farooq, F. Bolle, R.M. Tsai-Yang Jea. Ratha, N. Anonymous and revocable fingerprint recognition. In: Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2007). 2007. 1−7.

[32] Farooq F, Ratha N, Jea T, Bolle R. Security and accuracy trade-off in anonymous fingerprint recognition. In: Proc. of the 1st IEEE Int'l Conf. on Biometrics: Theory, Applications, and Systems. 2007. 1−6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4401917&isnumber=4401902

[33] Lee C, Choi J, Toh K, Lee S, Kim J. Alignment-Free cancelable fingerprint templates based on local minutiae information. IEEE Trans. on Systems, Man, and Cybernetics—Part B: Cybernetics, 2007,37(4):980−992.

[34] Tulyakov S, Farooq F, Govindaraju V. Symmetric hash functions for fingerprint minutiae. In: Singh S, Singh M, Apté C, Perner P, eds. Proc. of the Int'l Workshop on Pattern Recognition for Crime Prevention, Security and Surveillance. Berlin: Springer-Verlag, 2005. 30−38.

[35] Tulyakov S, Farooq F, Mansukhani P, Govindaraju V. Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters, 2007,28(16):2427−2436.

[36] Jain A, Ross A, Pankanti S. Biometrics: A tool for information security. IEEE Trans. on Information Forensics and Security, 2006, 1(2):125−143.

[37] Moon D, Gil Y, Ahn D, Pan S, Chung Y, Park C. Fingerprint-Based authentication for USB token systems. In: Chae K, Yung M, eds. Proc. of the WISA 2003. LNCS 2908, Berlin: Springer-Verlag, 2004. 355−364.

[38] Soutar C, Roberge D, Stoianov A, Gilroy R, Vijaya K. Biometric encryption. ICSA Guide to Cryptography, McGraw-Hill, 1999, http://www.bioscrypt.com/assets/Biometric_Encryption.pdf

[39] Davida G, Frankel Y, Matt B. On enabling secure applications through off-line biometric identification. In: Proc. the IEEE Symp. Privacy and Security, New Jersey: IEEE Computer Society, 1998. 148−157.

[40] Juels A, Wattenberg M. A fuzzy commitment scheme. In: Proc. of the 6th ACM Conf. Computer and Comm. Security (CCCS). New York: ACM, 1999. 28−36.

[41] Hao F, Anderson R, Daugman J. Combining crypto with biometrics effectively. IEEE Trans. on Computers, 2006,55(9): 1081−1088.

[42] Juels A, Sudan M. A fuzzy vault scheme. In: Lapidoth A, Teletar E, eds. Proc. IEEE Int'l Symp. on Information Theory. Institute of Electrical and Electronics Engineers, Inc., 2002. 408.

[43] Clancy T, Kiyavash N, Lin D. Secure smartcard-based fingerprint authentication. In: Proc. of the ACMSIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop. Association for Computing Machinery, Inc., 2003. 45−52.

[44] Yang S, Verbauwhede I. A secure fingerprint matching technique. In: Bebis G, Bourbakis N. Proc. of the WBMA 2003. Association for Computing Machinery, Inc., 2003. 89−94.

[45] Yang S, Verbauwhede I. Secure fuzzy vault based fingerprint verification system. In: Proc. of the Record of the 28th Asilomar Conf. on Signals, Systems and Computers. Institute of Electrical and Electronics Engineers Computer Society, 2004. 577−581.

[46] Yang S, Verbauwhede I. Automatic secure fingerprint verification system based on fuzzy vault scheme. In: Proc. of the IEEE Int'l Conf. on Acoustics, Speech, and Signal (ICASSP 2005), Vol.5. Institute of Electrical and Electronics Engineers Inc., 2005. 609−612.

[47] Uludag U, Pankanti S. Jain A. Fuzzy Vault for Fingerprints. In: Kanade T, Jai AK, Ratha NK. Proc. of the 5th Int'l Conf. on AVBPA. Berlin: Springer-Verlag, 2005. 310−319.

[48] Uludag U, Jain A. Securing fingerprint template: Fuzzy vault with helper data. In: Bhanu B, Ratha N. Proc. of the 2006 Conf. on Computer Vision and Pattern Recognition Workshop (CVPRW 2006). New Jersey: IEEE Computer Society 2006. 163.

[49] Nandakumar K, Nagar A, Jain A. Hardening fingerprint fuzzy vault using password. In: Lee SW, Li SZ. Proc. of the ICB 2007. LNCS 4642, Berlin: Springer-Verlag, 2007. 927−937.

[50] Nandakumar K, Jain A, Pankanti S. Fingerprint-Based fuzzy vault: Implementation and performance. IEEE Trans. on Information Forensics and Security, 2007,2(4):744−757.

[51] Li Q, Liu Z, Niu X. Analysis and problems on fuzzy vault scheme. In: Proc. of the Int'l Conf. on Intelligent Information Hiding and Multimedia Signal (IIH-MSP 2006). New Jersey: IEEE Computer Society, 2006. 244−250.

[52] Li J, Tian J, Yang X, Shi P, Li P. Topological structure-based alignment for fingerprint fuzzy vault. In: Proc. of the Int'l Conf. on Pattern Recognition, 2006.

[53] Nyang D, Lee K. Fuzzy Face Vault. How to implement fuzzy vault with weighted features. In: Proc. of the Universal Access in HCI, (HCII 2007), LNCS 4554, Berlin: Springer-Verlag, 2007. 491−496.

[54] Wang Y, Plataniotis K. Fuzzy vault for face based cryptographic key generation. In: Proc. of the Biometrics Symp. Berlin: Springer-Verlag, 2007. 1−6.

[55] Lee Y, Bae K, Lee S, Park K, Kim J. Biometric key binding: Fuzzy vault based on iris images. In: Lee SW, Li SZ eds. Proc. of the ICB 2007. LNCS 4642, Berlin: Springer-Verlag, 2007. 800−808.

[56] Scheirer W, Boult T. Cracking fuzzy vaults and biometric encryption. In: Proc. of the Biometrics Symp. 2007. 1−6.

[57] Kholmatov A, Yanikoglu B. Realization of correlation attack against the fuzzy vault scheme. In: Proc. of the 2008 SPIE/ Biometrics, Security, Forensics, Steganography, and Watermarking of Multimedia Contents. 2008. http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.92.250&rep=rep1&type=pdf

[58] Mihailescu P. The fuzzy vault for fingerprints is vulnerable to brute force attack. http://arxiv.org/abs/0708.2974v1

[59] Chang E, Shen R, Teo F. Finding the original point set hidden among chaff. In: Proc. of the ASIACCS 2006. New York: ACM, 2006. 182−188.

[60] Dodis Y, Ostrovsky R, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Cachin C, Camenisch J, eds. Proc. Eurocrypt. Berlin: Springer-Verlag, 2004. 2004. 523−540.

[61] Dodis Y, Katz J, Reyzin L, Smith A. Robust fuzzy extractors and authenticated key agreement from close secrets. Advances in Cryptology-Crypto, 2006. 232−250.

[62] Buhan I, Doumen J, Hartel P, Veldhuis R. Fuzzy extractors for continuous distributions. In: Bao F, Miller S. Proc. of the ASIACCS 2007. New York: ACM, 2007. 353−355.

[63] Boyen X. Reusable cryptographic fuzzy extractors. In: Proc. of the 11th ACM Conf. on Computer and Communications Security (CCS 2004). 2004. http://eprint.iacr.org/2004/358/

[64] Boyen X, Dodis Y, Katz J, Ostrovsky R, Smith A. Secure remote authentication using biometric data. In: Cramer R, ed. Proc. of Advances in Cryptology 24th Annual International Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005). Springer-Verlag, 2005. 147−163.

[65] Li Q, Sutcu Y, Memon N. Secure sketch for biometric templates. In: Lai XJ, Chen KF. Proc. of Advances in Cryptology 12th Int'l Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2006). 2006. 99−113.

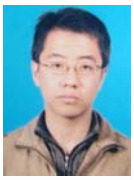
[66] Sutcu Y, Li Q, Memon N. Protecting biometric templates with sketch: Theory and practice. IEEE Trans. on Information Forensics and Security, 2007,2(3):503−512.

[67] Tong V, Sibert H, Lecoeur J, Girault M. Biometric fuzzy extractors made practical: A proposal based on FingerCodes. In: Lee SW, Li SZ. Proc. of the ICB 2007. LNCS 4642, Berlin: Springer-Verlag, 2007. 604−613,

[68] Arakala A, Jeffers J, Horadam K. Fuzzy extractors for minutiae-based fingerprint authentication. In: Lee SW, Li SZ. Proc. of the ICB 2007. LNCS 4642, Berlin: Springer-Verlag, 2007. 760−769.
[69] Zhang F, Feng D, Sun Z. An iris authentication scheme based on fuzzy extractor. Journal of Computer Research and Development, 2008,45(6):1036−1042 (in Chinese with English abstract).
[70] Menezes A, Oorschot P. Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.
[71] Luo X, Tian J, Wu Y. A Minutia Matching Algorithm in Fingerprint Verification. In: Proc. of the 15th Int'l Conf. on Pattern Recognition (ICPR 2000). New Jersey: IEEE Computer Society, 2000. 833−836.

附中文参考文献:

[1] 田捷,杨鑫.生物特征识别技术理论与应用.北京:电子工业出版社,2005.
[10] 王星明,田捷,武岩.融合自动指纹认证的安全密码体制在网络安全中的应用.计算机应用,2000,2:53−54.
[69] 张凡,冯登国,孙哲男.一种基于模糊提取的虹膜鉴别方案.计算机研究与发展,2008,45(6):1036−1042.



李鹏(1984－),男,河北武安人,博士生,主要研究领域为自动指纹识别技术,生物特征加密技术.

时鹏(1980－),男,博士生,主要研究领域为自动指纹识别技术,生物特征加密技术.

田捷(1960－),男,博士,研究员,主要研究领域为医学图像处理,生物特征识别.

张阳阳(1985－),女,博士生,主要研究领域为自动指纹识别技术.

杨鑫(1972－),女,博士,副研究员,主要研究领域为生物特征识别,生物特征加密技术.