计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20190371
57(5):1003-1021,2020

生物特征识别模板保护综述

王会勇[1,4] 唐士杰[2] 丁 勇[3,4] 王玉珏[3,4] 李佳慧[1,4]
[1](桂林电子科技大学数学与计算科学学院 广西桂林 541004)
[2](桂林电子科技大学电子工程与自动化学院 广西桂林 541004)
[3](桂林电子科技大学计算机与信息安全学院 广西桂林 541004)
[4](广西密码学与信息安全重点实验室(桂林电子科技大学) 广西桂林 541004)
(why608@163.com)

Survey on Biometrics Template Protection

Wang Huiyong[1,4], Tang Shijie[2], Ding Yong[3,4], Wang Yujue[3,4], and Li Jiahui[1,4]
[1](*School of Mathematics & Computing Science, Guilin University of Electronic Technology, Guilin, Guangxi* 541004)
[2](*School of Electronic Engineering & Automation, Guilin University of Electronic Technology, Guilin, Guangxi* 541004)
[3](*School of Computer Science & Information Security, Guilin University of Electronic Technology, Guilin, Guangxi* 541004)
[4](*Guangxi Key Laboratory of Cryptography and Information Security* (*Guilin University of Electronic Technology*), *Guilin, Guangxi* 541004)

Abstract Biometric authentication (BA) has become an important means of identity authentication. However, many BA systems deployed at present do not take enough consideration in protecting the security and privacy of user's biometric data, which has become a main obstacle to the popularization and application of the BA technology. BA systems may face various attacks from software or hardware implementations, among which, template attack is the main consideration. Many technical literatures have been devoted to dealing with this type of attacks. However, existing review literatures suffer from incomplete descriptions or conflicting discussions. In order to systematically summarize the attacking and protection technologies against biometric templates, some related concepts of the BA system is introduced at first, as well as the architecture of a BA system and the connotation of BA security and privacy. Then, template protection technologies for a BA system are classified into two main categories for description: the transformation-based methods and the crypto-based methods, which solves some conflictions in existing literatures. Afterwards, some classical methods and emerging technologies in each category are expounded and analyzed, as well as some subsequent evaluations and improvements. Finally, several major difficulties and the corresponding possible solutions for building a secure BA system are pointed out.

Key words biometric authentication; data security; privacy protection; template protection; review

收稿日期:2019-06-11;**修回日期**:2019-09-19

基金项目:国家自然科学基金项目(61772150,61862012,61802083,61962012);广西自然科学基金项目(2018GXNSFDA281054,2018GXNSFAA281232);广西重点研发计划项目(AB17195025);广西密码学与信息安全重点实验室开放课题(GCIS201622,GCIS201702)

This work was supported by the National Natural Science Foundation of China (61772150, 61862012, 61802083, 61962012), the Natural Science Foundation of Guangxi Autonomous Region of China (2018GXNSFDA281054, 2018GXNSFAA281232), the Guangxi Key Research and Development Program (AB17195025), and the Open Project of Guangxi Key Laboratory of Cryptography and Information Security (GCIS201622, GCIS201702).

通信作者:丁勇(stone_dingy@126.com)

摘 要 生物特征识别(biometric authentication, BA)已经成为一种重要的身份鉴别手段,但当前部署的很多BA系统在保护用户生物特征数据的安全性和隐私性方面考虑不足,成为阻碍BA技术推广应用的一个关键障碍.BA系统可能面临来自软件和硬件的多种攻击,针对生物特征模板的攻击是其中最常见的一种.已经有很多技术文献致力于应对这种类型的攻击,但现有的综述性文献存在论述不全面或内容冲突等问题.为系统总结针对生物特征模板的攻击与保护技术,首先介绍了BA系统的相关概念、体系架构以及安全性与隐私性的内涵,然后阐述了BA系统面临的典型模板攻击方法.随后,将BA系统模板保护技术归纳为基于变换的方法和基于加密的方法2个类别,阐述并分析了每个类别中的经典方法与新兴技术.最后,指出了构建安全BA系统可能面临的几个主要困难与可能的解决思路.

关键词 生物特征识别;数据安全;隐私保护;模板保护;综述

中图法分类号 TP391.41

随着互联网与电子商务的发展,日常生活中有越来越多的场景需要对用户进行身份鉴别,如机场安检、登录银行系统、解锁手机等.

传统的身份鉴别手段主要有2种:1)根据持有物,如各种证件;2)根据用户了解的信息,如语音口令或数字密码.但这2种方式都存在明显缺陷,如证件容易丢失、密码容易忘记等.生物特征识别(biometric authentication, BA)技术能够有效解决上述问题,因而在近年来得到快速发展与应用.

生物特征识别是指"为进行身份识别而采用自动技术对个体生理特征(如指纹、掌纹、虹膜、人脸、脑电波等)或个人行为(如步态、字迹、声音、键盘敲击习惯等)特点进行提取,并将这些特征或特点与数据库中已有的模板数据进行比对,从而完成身份认证或识别的过程"[1].

自20世纪70年代指纹识别技术被成功应用[2]以来,BA技术获得了快速发展,目前已在世界范围内得到广泛应用.但与此同时,BA系统的数据安全与隐私保护问题却一直没有得到良好解决,成为阻碍该技术获得快速推广应用的一个主要障碍[3].

世界范围内已经发生了多起由生物特征数据泄露或隐私泄露引起的安全事件,引起了众多关注.例如在2019年2月美国旧金山市公布了一项立法法案,使得该市成为美国首个禁止人脸识别技术的城市,其主要理由是该技术可能威胁到个人的隐私信息安全,同时存在种族歧视嫌疑[4].

生物特征信息泄露的后果是非常严重的.这是因为生物特征具有唯一性和不可更改性,一旦泄露,被窃取的生物特征几乎永远无法再用,其危害性比丢失身份证等传统身份鉴别媒介大得多.

近年来,众多研究者对BA系统的数据安全与隐私保护问题进行了研究,重点聚焦于生物特征模板保护工作.也出现了多篇综述性文献,但很多综述文献的内容不系统,或者比较陈旧,甚至存在冲突内容.因此,本文拟对近年来出现的针对BA系统的模板攻击及其应对性技术文献进行综述,希望为相关研究者提供有价值的参考.

本文首先概述BA系统面临的安全性与隐私保护问题,主要包括BA系统的一般框架、安全性与隐私保护的内涵,以及当前BA系统面临的主要风险;然后介绍国内外学者在应对BA系统面临的主要威胁——生物特征模板攻击方面的研究进展与代表性技术方案;最后对此类研究面临的困难和解决思路提出展望.

1 BA系统的数据安全性隐私保护

1.1 BA系统的一般架构

一个典型的BA系统是带有生物特征采集设备的访问控制系统[1],基本工作模式包含注册与比对2个过程.在注册阶段,用户通过采集设备读取生物特征,并生成模板特征存入数据库;在比对阶段,系统调用采集设备对用户的相应生物特征进行再次采集并生成新鲜特征,然后与数据库中存储的模板特征进行比对,根据2个特征的相似度确定用户身份.

根据识别的任务和目的,BA系统可以分为2类[5](如图1所示):验证系统(verification)和搜索(或检索)系统(identification),而"生物特征识别"一般是对这2类任务的统称.

验证系统的任务是对用户提供的身份进行核实,以确定该用户的身份是否与其声称的身份一致.此类系统常被用作某些系统的准入机制(如利用指纹认证解锁手机和门禁系统等),一般需将用户的特征数据与数据库中的特定记录进行1对1比对.而

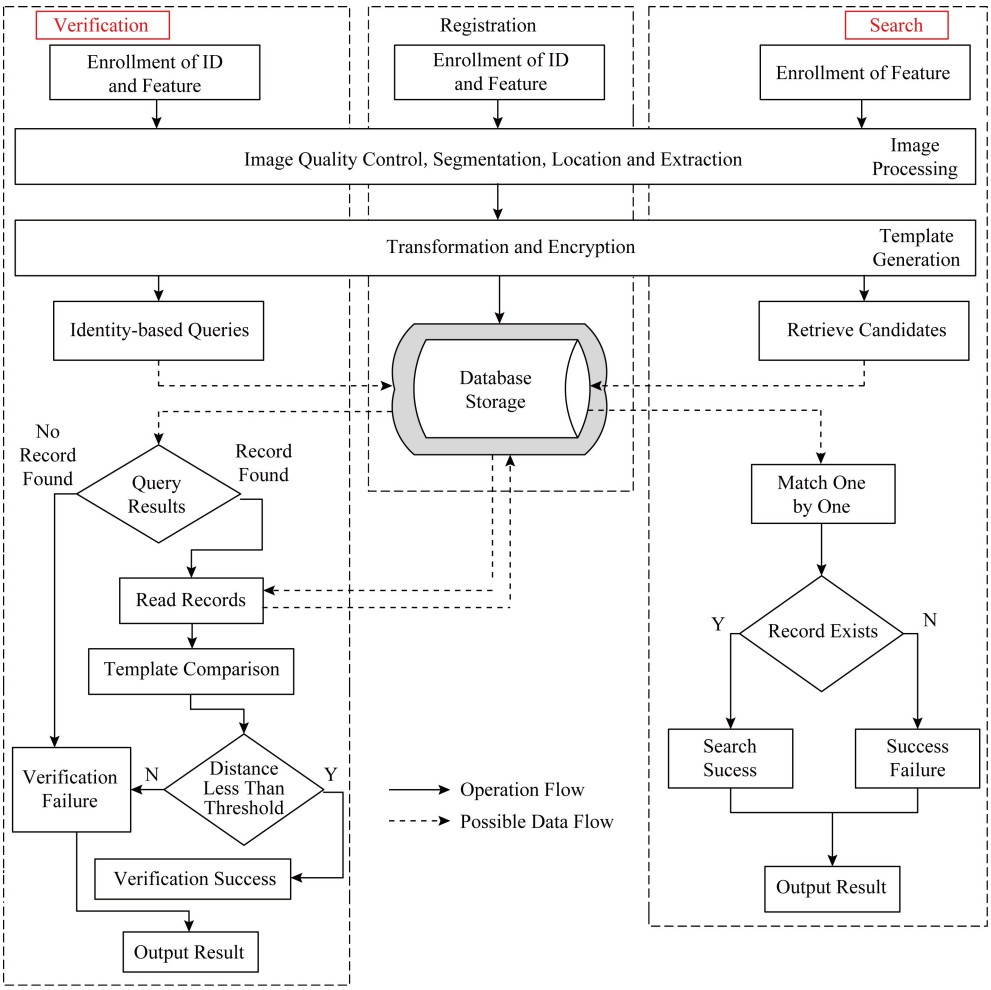

Fig. 1 Authentication and search task flow of BA system

图 1 BA 系统的认证与搜索任务流程

搜索系统的任务是在不了解用户身份的情况下利用其生物特征在数据库中查找其身份,通常需要将用户数据与数据库中的多个记录进行 1 对 N 比对,因而工作量和难度一般比验证系统大.此类系统大多用于被动方式,如在公共环境下对特定人员的身份进行甄别等.

BA 系统的决策结果一般有 2 种[6]:合法用户与非法用户(或匹配与不匹配).这 2 种决策过程都可能出错或不出错,因而共有 4 种可能的结果.通常用错误接受率(即假冒者被判定为合法用户的概率)和错误拒绝率(即合法用户被判定为假冒者的概率)来表征 BA 系统的正确性.

1.2 数据安全与个体隐私的内涵

在信息科学领域,数据安全是一项基本要求,其基本内涵是保证只有授权用户才能使用数据.而个体隐私安全则是近年来随着云计算的发展逐渐产生的一种新需求,基本内涵是保证数据只能被设定的个体用于设定的目的.Campisi[7]认为:个体隐私的内涵主要包括决策隐私、空间隐私、故意隐私及信息隐私 4 个方面,如图 2 所示,其中信息隐私是主要考虑.

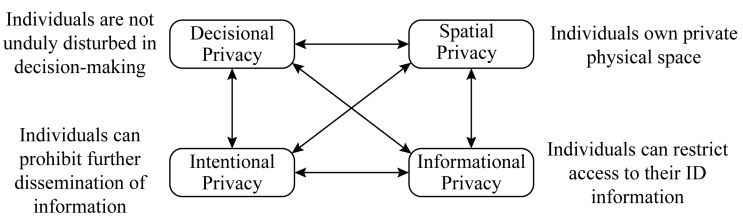

Fig. 2 The main connotation of individual privacy

图 2 个体隐私的主要内涵

1.3 BA 系统面临的安全与隐私风险

在 BA 系统中,生物特征本质上是一种便携式“密钥”.但这种密钥却面临着比传统密钥更大的风险,因为“生物特征不是秘密”[8],很难杜绝数据泄露.

Ratha 等人[9]、Tuyls 等人[10]和 Campisi[7]认为 BA 系统面临的主要风险(如图 3 所示)来自 3 个方面[11]:

1) 原始数据泄漏.有些生物特征无法完全保密,如人脸、声音、体态等,很容易被攻击者秘密采集.其他一些生物特征(如虹膜、静脉等)的窃取难度虽然稍大,但也很难杜绝恶意采集.而泄露的原始数据可能成为伪造攻击(spoofing)的工具.

2) 模板攻击.当前的很多 BA 系统无法提供对用户生物特征模板的有效保护,在数据传输或保存过程存在模板泄露风险,而从泄露的模板恢复出原始数据是可能的.

3) 联系攻击.如果用户使用同一个生物特征登录多个 BA 系统,其存储在不同系统中的特征模板可能是相同的或可以匹配成功的.这可能允许攻击者利用某个系统的新鲜模板登录另一个系统,或从不同模板之间的联系推测出有效模板或用户身份.

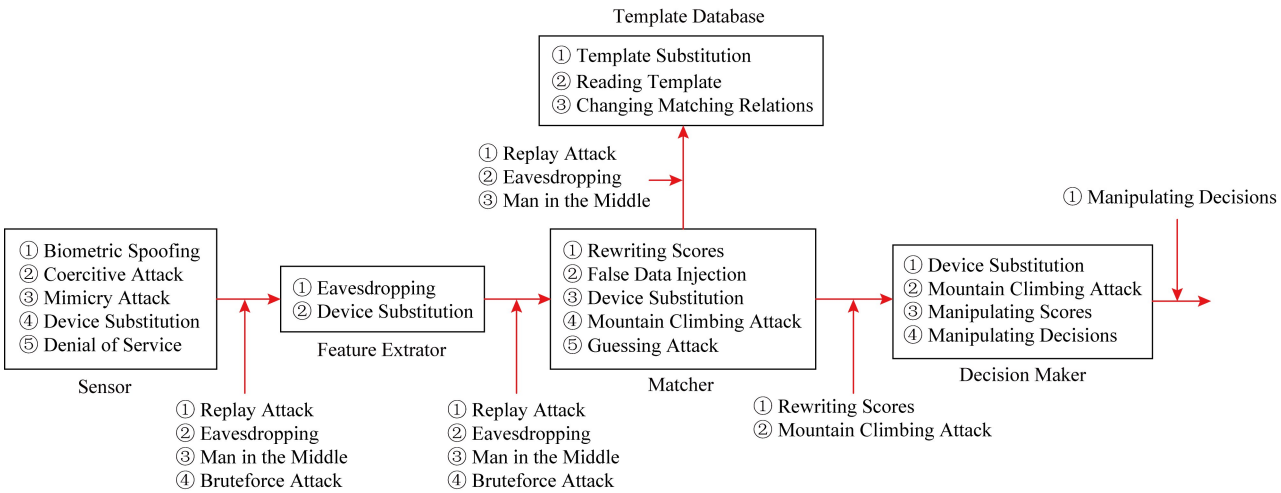

Fig. 3 Attacking points and patterns in general BA systems

图 3 一般 BA 系统的攻击点与攻击模式

Pagnin 等人[5]对上述攻击进行了具体阐述(如图 4 所示).其中,样本恢复攻击的目的是获得能够通过认证的用户特征,以实施欺诈攻击或暴力破解;模板恢复攻击旨在获得数据库中存储的用户模板;而对用户进行追踪和识别的主要方法是记录并分析用户在不同时间登陆 BA 系统或登录不同 BA 系统时的身份与模板的对应关系,以找到模板与用户的联系.

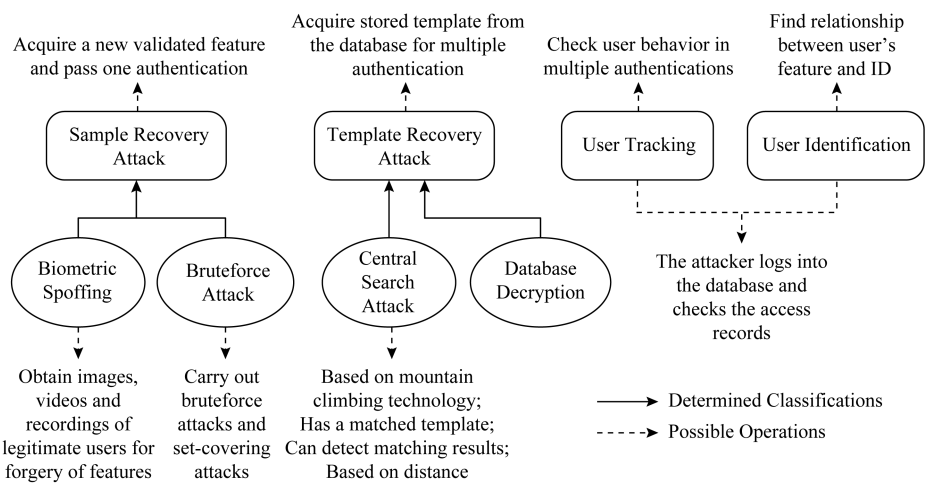

Fig. 4 Classification of attacks on BA systems

图 4 针对 BA 系统的攻击分类

与生物特征使用相关的隐私担忧主要有3种[5,7]:

1) 未经允许收集和分享生物特征;将生物特征用于未授权目的(即功能蠕变).

2) 利用生物特征推测个体状况,如种族、性别、健康状况.

3) 利用生物特征精准追踪个体等.

1.4 针对BA系统的保护工作概述

近年来有众多学者参与到BA系统的保护工作中,积累了丰富的研究成果:有旨在研究现有BA系统脆弱性的工作[12-17];有构建新的保护方案和技术的论文[18-21]和书籍[7,22-25];也有旨在讨论商业系统客观评估通用框架[26-27]的文献.

同时,出现了一些面向生物特征和一般信号处理的教程、会议[28-29]和讲习班以及以研究脆弱性评估为目标的竞赛组织[30-31]和评估团体与实验室[32-33]等.

BA系统面临的安全与隐私威胁[34-35]主要来自于间接攻击和直接攻击.间接攻击是在系统内部执行的,如黑客或内部人员操纵特征提取器或模板生成器、修改模板数据库等,可以通过多种措施来预防,如防火墙、防病毒软件、入侵检测和加密等,工作重点在于保护生物特征模板的安全性.直接攻击主要是指生物特征欺诈(spoofing),其主要攻击目标是传感器,因此很难用数字保护机制来对抗.

2 生物特征模板攻防技术

通常认为,对生物特征模板的未授权访问是对用户数据的最大威胁[10],因为安全的生物特征模板存储方案可以抵抗针对信道和数据库的多种攻击.因此,构建安全高效的生物特征模板存储方案(包括保密比对过程)是保护BA系统安全性与隐私性的关键.

由ISO/IEC 24745标准[36]和文献[37]可知,一个良好的生物特征模板存储方案应具有4个特性:

1) 可更新性.即能够撤销被泄露的生物特征模板,并基于相同的生物特征生成新的模板.

2) 多样性.重新生成的生物特征模板不能与被撤销的(来自同一生物特征的)模板成功匹配.

3) 安全性.应保证从生物特征模板获得原始生物特征数据是不可能的,至少在计算上是复杂的.

4) 模板存储方案不应该使生物特征识别性能(如错误拒绝率、错误接受率)有较大下降.

2.1 针对生物特征模板的攻击

Pagnin等人[5]认为:在不破坏BA系统的前提下,针对BA系统的模板恢复攻击主要有2种方式.

1) 利用爬山技术[38]实施的中心搜索攻击.这种攻击需要3个条件:攻击者拥有一个已经匹配成功的生物特征模板;攻击者能够得到每次测试的结果,即匹配是否成功;比对过程是基于距离的.

该过程的直观原理如图5所示.其中,用户的生物特征用$\boldsymbol{Z}_{10}^{2}$中的向量表示,即该向量由2个组件构成(分别用横坐标和竖坐标表示其取值),并取距离阈值为2.但这些数值仅是为了更清晰地显示其原理,与实际系统中的参数无关.

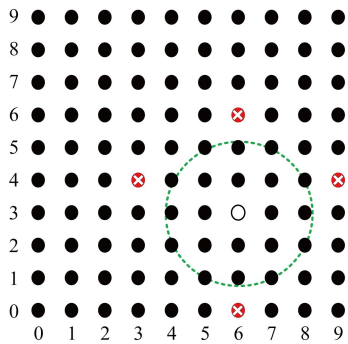

Fig. 5 Central search attack towards biometric template

图5 针对生物特征模板的中心搜索攻击原理

设数据库中存储的模板b对应点(6,3),而已经通过认证的一个模板b'对应点(6,4),显然虚线圆圈内的点是能够匹配成功的点.敌手从点b'(6,4)开始匹配实验,若成功则将第1个组件值加1(向右移动1),并继续实验.当被拒绝时,即实验到点(9,4)(最右侧带乘号的点)时,敌手会知道上一个实验点是接受圈内该方向的最后一个点.然后敌手重新从点b'开始,向左侧重复实验,直到被拒绝.随后,敌手对第2个组件值做相同的测试(上下方向).最后,敌手能够找到接受圈的4个边界点的坐标,从而能够计算出其中心的坐标,即找到数据库中存储的生物特征模板的数字表示.

这种模板恢复攻击非常有效,因为它需要的匹配尝试次数与生物特征向量的长度呈线性关系[39].

2) 获得数据库的控制权并使用暴力攻击解密模板.由于抵抗暴力攻击是所有安全模板存储方案的基本目标,因而简单暴力攻击成功的可能性很小.

2.2 模板保护技术

近年来,学者们提出了多种生物特征模板保护

技术(biometric protection, BP),也出现了多个综述性文献,但有些文献对某些技术、方案的命名和分类存在分歧,也有部分文献的系统性较差.经过整理,我们认为现有的 BP 技术可分为 2 类:基于特征变换的方法和基于特征加密的方法,如图 6 所示:

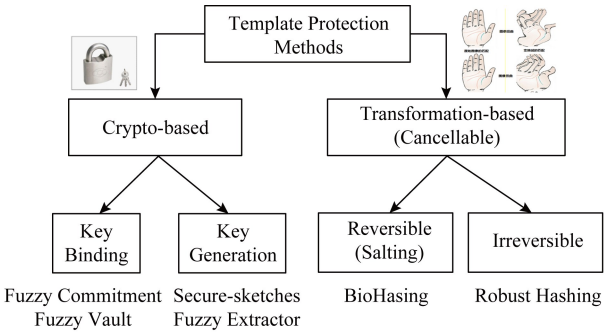

Fig. 6 Classification and representations of BP technologies

图 6 BP 方法的分类与代表性技术

2.2.1 基于特征变换的模板保护方法

此类方法也被称为可撤销(cancellable)的模板保护方法[39],需要用某种变换函数对生物特征或其模板进行变换,并在变换域进行匹配,如图 7 所示.根据所用的变换是否可逆,此类方法又可以分为 2 类:

1) 基于可逆变换的方法.此类方法被有些文献称为加盐法(salting)[40]或生物特征散列法(biohashing)[39,41],是 Jin 与 Teoh 等人[42]于 2004 年首次提出的,并被用于指纹识别.随后,该类算法被应用于人脸、掌纹、虹膜、指纹、签名等认证过程.

生物特征散列法的主要优点是错误接受率较低、可移植性高、模板可更换,主要缺陷在于安全性能不足,因为在此类方案中模板的安全性取决于对变换函数参数的保护.Lumini 等人[43]指出:如果用户密钥丢失,生物散列法的整体效率和安全性将有很大下降.

Jin 等人提出的用于指纹认证的生物散列法[44]的基本流程为:首先求取指纹方向场,获得指纹中心;其次,对指纹图像做小波变换、Fourier 变换和梅林变换,得到指纹图像的 Wavelet-Fourier-Mellin 变换特征;然后将得到的特征向量投影到一个正交随机矩阵中,并经过阈值量化生成一组 BioCode 码作为指纹特征模板.认证时,通过计算存储的 BioCode 模板和新鲜 BioCode 模板的海明距离来决定是否通过认证.

2) 基于不可逆变换的方法.此类方法由 Ratha 等人[9]于 2001 年提出并被用于指纹模板保护(可撤销的模板保护方法起初只表示基于不可逆变换的方法,但后来被赋予更广泛的含义,即基于变换的模板保护方法).其基本思想是用一个参数可调的不可逆变换对生物特征进行变换,并将变换后的特征作为模板.如果模板泄露,可以通过修改变换函数的参数生成一个新的模板.在此类方法中,模板的安全性取决于根据逆变换获得原始生物特征的难度.此类方法所需的变换函数必须满足 3 个条件:必须是不可逆的;应具有局部光滑但全局不光滑的特性;对每个细节点的变化幅度不能太小.基于不可逆变换的代表方案主要有 2 个:

① Ratha 等人[44]提出了 3 种用于生成生物特征模板的不可逆变换:笛卡儿变换、极坐标变换和表面褶皱变换.在笛卡儿变换中,指纹图像的每个细节点被映射到一个矩形表中的特定位置;在极坐标变换中,指纹图像被映射到一个扇形区域中;表面褶皱变换则是利用电势场函数(式(1))或二维高斯函数对指纹细节点进行变换.实验证明褶皱变换的整体表现最好.

方案中给出的电势场(向量值)函数的定义为

$$F(z)=\sum_{i=1}^{K}\frac{q_i(z-z_i)}{|(z-z_i)|^3}, \tag{1}$$

其中,$z=x+iy$ 为电荷位置.显然电荷的位置与强度取决于随机密钥 $z_1,z_2,\cdots,z_K,q_1,q_2,\cdots,q_K$.

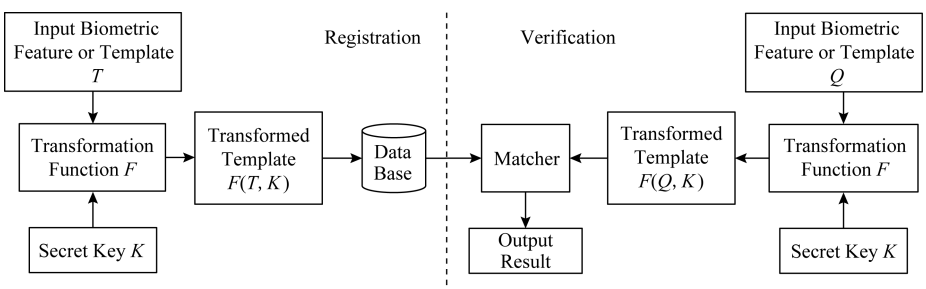

Fig. 7 Flow of transformation-based BP methods

图 7 基于特征变换的模板保护方案流程

平移的大小由该函数的模$|F(z)|$决定,而平移方向由以下平移方向(相位)函数(式(2))决定:

$$\Phi(x,y)=\frac{1}{2}\arg\left\{\sum_{i=1}^{K}\frac{q_i(z-z_i)}{|(z-z_i)|^3}\right\}. \quad (2)$$

所用二维高斯函数的定义为

$$F(z)=\sum_{i=1}^{K}\frac{\pi_i}{|2\pi\boldsymbol{\Lambda}_i|}\exp\{-\frac{1}{2}(z-\mu_i)^{\mathrm{T}}\boldsymbol{\Lambda}_i^{-1}(z-\mu_i)\},$$

其中,$z=x+iy$ 表示位置.权值 π_i、协方差矩阵 $\boldsymbol{\Lambda}_i$ 和核的中心 u_i 显然由随机密钥决定.

平移的大小由该函数的模$|F(z)|$决定,平移方向由相位函数

$$\Phi_F(z)=\frac{1}{2}\arg\{\nabla F\}+\Phi_{\mathrm{rand}}$$

决定,其中 Φ_{rand}为一个随机相位偏移.

由此可得到指纹细节点的位置与方向变换公式:

$$X'=x+K|G(x,y)|+K\cos(\Phi_F(x,y)),$$

$$Y'=y+K|G(x,y)|+K\sin(\Phi_F(x,y)),$$

$$\Theta'=\mathrm{mod}(\Theta+\Phi_G(x,y)+\Phi_{\mathrm{rand}},2\pi),$$

其中 x,y,Θ 分别表示变换之前细节点的横坐标、纵坐标和方向角,而 X',Y',Θ'分别表示变换之后细节点的横坐标、纵坐标和方向角,Φ_G 为 G 的相位函数.

众多学者对上述方案进行了研究与改进.Feng 等人[45]认为该方案所构建的映射关系很难抵御多重记录攻击或暴力攻击,因为在大部分映射区域内,其函数关系为一一映射,即不可逆的信息非常有限.要获得更高的安全性能,必须增加映射中多对一区域的比例,但这样做会导致认证性能出现下降.Chikkerur 等人[46]利用正交变换构造了一种不依赖于注册的可撤销指纹模板生成方案,获得了良好的鲁棒性,能够抵抗重放攻击,但识别性能不高.Maiorana 等人[47-48]提出了基于卷积算子的不可逆变换集合,原则上可以作用于所有能够被表征为序列集合的生物特征.

② 近年来,布隆过滤器(Bloom filters)[49]成为构造可撤销的生物特征模板方案所需的不可逆变换的一个有力工具.

布隆过滤器实质上是一种用于表征集合的空间效率很高的随机数据结构,允许向集合添加元素并检测一个元素是否在集合中.其主要缺点是误识率较高,且无法删除元素.

标准布隆过滤器的工作原理如图 8 所示:

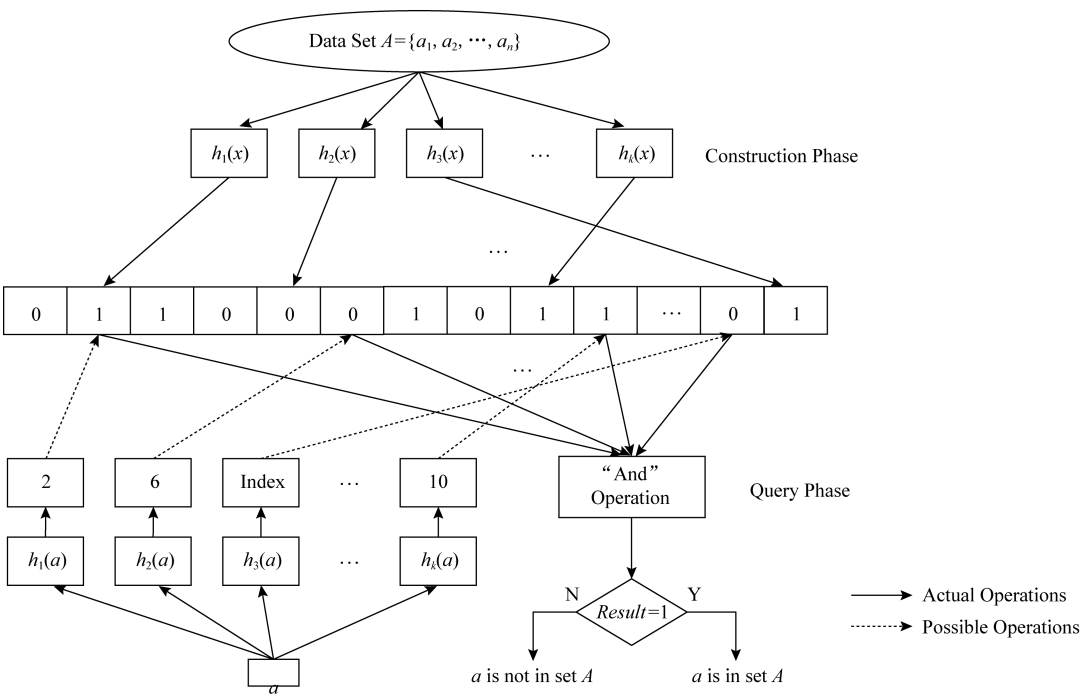

Fig. 8 Principle of standard Bloom filters[49]

图 8 标准布隆过滤器[49]的工作原理

布隆过滤器的组件包含一个长度为 m 的二进制向量 $\boldsymbol{V}$(所有位初始值为 0)和 k 个($k\leqslant n$)相互独立的散列函数 $h_1,h_2,\cdots,h_k$,每个散列函数能够按均匀分布将集合 $A=\{a_1,a_2,\cdots,a_n\}$的某个元素映射到 $\boldsymbol{V}$ 的某个位.

若要向集合 A 添加一个元素 a,需先计算索引:

$h_1(a),h_2(a),\cdots,h_k(a)$,并将向量 $\boldsymbol{V}$ 的第 $h_i(a)$ 位($i=1,2,\cdots,k$)的值置为 1.

若要搜索一个元素 b 是否在集合 A 中,同样需要先计算 $h_1(b),h_2(b),\cdots,h_k(b)$,然后检查向量 $\boldsymbol{V}$ 中第 $h_i(b)$ 位($i=1,2,\cdots,k$)的值是否全为 1(只要对这些位的值做“与”运算即可,若结果为 1,则证明这些位的值全为 1).如果这些位置的值全为 1,则说明 $b\in A$;否则说明 $b\notin A$,或出现了假真(false positive)错误.

Rathgeb 等人[50]提出了基于布隆过滤器的可撤销模板生成方法,并将其应用于虹膜特征模板的保护.其基本思想是注册时根据用户的特征向量生成布隆过滤器向量,如文献[50]中图 1 所示,基本步骤为:

步骤 1. 将原始生物特征表示为一个 $N\times M$ 的二进制矩阵 $\boldsymbol{J}$;

步骤 2. 将矩阵 $\boldsymbol{J}$ 分块,其中水平方向分为 l 块(即每块宽为 M/l 列),垂直方向分为 N/ω 块(即每块高为 ω 行),则矩阵 $\boldsymbol{J}$ 被划分为 $l\times N/\omega$ 块;

步骤 3. 初始化 $l\times N/\omega$ 个长度为 2^{ω} 的二进制布隆过滤器向量,将这些向量的所有位置 0,并取定散列函数 $h_1,h_2,\cdots,h_k$;

步骤 4. 将 $\boldsymbol{J}$ 的每个子块 $\boldsymbol{J}_{ij}$($i=1,2,\cdots,l$;$j=1,2,\cdots,N/\omega$)的每列(一个 ω 位的二进制数)转换为十进制数 a_{ijp}($p=1,2,\cdots,M/l$);

步骤 5. 计算 $h_1(a_{ijp}),h_2(a_{ijp}),\cdots,h_k(a_{ijp})$,其中,($p=1,2,\cdots,M/l$),并将与此子块 $\boldsymbol{J}_{ij}$ 对应的(第 j 个)布隆过滤器的第 $h_1(a_{ijp}),h_2(a_{ijp}),\cdots,h_k(a_{ijp})$位的值全置 1,最终得到 $l\times N/\omega$ 个布隆过滤器向量;

步骤 6. 将上述结果存为模板,或将其按列链接为长度为 $2^{\omega}\cdot(l\times N/\omega)$的特征向量后存为模板 b.

认证时,用同样方式生成新鲜特征模板 b',然后计算这 2 个向量的海明距离 $HD(b,b')$,并按如下方式计算其“不近似”程度:

$$DS(b,b')=\frac{HD(b,b')}{|b|+|b'|}.$$

最后将该值与设定的阈值比较,即可判定认证是否成功.

由于采用了散列运算,并可能将多个数字映射到布隆过滤器的同一个位置,因此上述算法实质上构成了一种不可逆映射.包括 Rathgeb 等人在内的多位研究者对该方案进行了分析和改进.

Rathgeb[51]在 2014 年将上述方法进行了扩展,使其具备了数据压缩功能,并声称能够完成高效的生物特征“识别”任务.2015 年 Rathgeb 又将该算法推广到多生物特征(人脸和虹膜)模板的保护中.但文献[52]的分析表明上述 2 个方案不具备不可链接性,而文献[53]指出文献[50]的方案存在泄漏数据的可能性.为克服上述问题,Gomez 等人[54]对原始的布隆过滤器进行了重新设计,提出了一个额外步骤“保结构的特征重置(structure preserving feature rearrangement)”,获得了比原始方案更好的识别性能,并能够抵抗交叉匹配攻击.

3) “蜜糖模板(honey template)”是 2015 年出现的另一种生物特征模板保护技术,由 Yang 等人[55]提出并被用于人脸识别[56],旨在抵抗伪造攻击并检测生物特征模板数据库可能发生的数据泄露.其基本架构如图 9 所示,基本工作流程包括注册流程和认证流程:

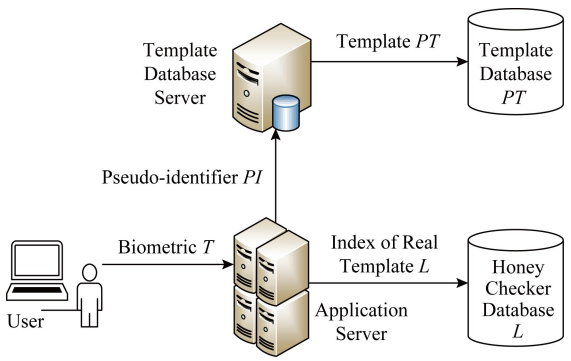

Fig. 9 Architecture of the “honey template” scheme[55]

图 9 “蜜糖模板”方案[55]基本架构

注册流程:

① 根据用户的真实生物特征生成一个“糖模板 ST(sugar template)”,然后根据 $k-1$ 个假特征生成 $k-1$ 个“蜜模板 HT_j(honey template)”,其中 $j=1,2,\cdots,k-1$;

② 将上述 k 个模板的存储单元地址打乱,以掩藏真实模板的地址,并将这 k 个模板用 k 个伪标识符 PI_j 表示,其中 $j=1,2,\cdots,k-1$;

③ 将集合 $PT=\{AD,PI_1,PI_2,\cdots,PI_2\}$ 定义为该用户的模板,其中 AD 为可能存在的辅助信息;

④ 将 PT 存储到模板数据库,并将 ST 的索引号 L 记录到“蜜检测数据库(honey checker database)”,要求这 2 个数据库可以根据用户的身份索引号相互关联.

认证流程:

① 应用服务器根据用户身份从模板数据库取

出与待认证用户对应的辅助信息 AD,并用与注册过程相同的方式生成一个伪标识符 PI^*,将其发送给模板数据库服务器;

② 模板数据库服务器将 PI^* 与该用户的所有 k 个模板进行比对,找出相似度最高的一个,并将其索引号 idx 返回应用服务器;

③ 应用服务器从"蜜检测服务器"搜索出与用户身份对应的索引号 L,并将 idx 与 L 进行比对.若 $idx=L$,则应用服务器给出验证通过的结论.否则就意味着有人利用从"蜜模板"计算出的原始图像来挑战系统,也就意味着该用户的生物特征数据发生了泄露.

2017 年 Martiri 等人[57]又基于"蜜糖模板"和布隆过滤器提出了一个一般性的模板保护方案,能够提供不可链接性和不可逆性,并能够抵御欺诈攻击.该方案已经被用于构建一个公开的多生物特征数据库 BioSecure Multimodal[58].

2.2.2 基于生物特征加密(BC)的模板存储方法

基于生物特征加密的模板存储方法将加密后的生物特征数据存储为模板,由加拿大学者 Tomko 等人[59]于 1996 年提出.大多数 BC 系统需存储一些与生物特征相关的公开信息(通常被称为辅助数据,helper data[60]),用于重构或生成密钥.辅助数据虽与生物特征相关,但不能泄露关于生物特征的任何显著信息.根据辅助数据的生成方式,BC 系统主要包括密钥生成(key-generation)系统和密钥绑定(key-binding)系统 2 类.

1) 密钥生成方法,即在注册时从生物特征数据直接生成密钥,并将密钥保存于数据库中,在认证时按同样的方法由生物特征生成密钥,然后通过比对密钥实现身份认证.这种方法的主要优点是可移植性强,主要困难在于密钥的获取,因为处理生物特征数据类内变化性是一个困难,可能导致密钥生成方法的识别性能出现较大幅度下降[61].此类方案较难构造,也很难满足多样性要求.

现有的相关文献主要致力于从有噪声的生物特征数据获得鲁棒的密钥.最早的密钥生成方案在 2002 年由 Monrose 等人[62]提出,旨在将用户敲击键盘的特征用于密钥生成,以增强密钥的可靠性.随后,文献[63-64]进一步研究了如何根据声音特征生成密钥;Goh 等人[65-66]等则利用卷积神经网络和循环神经网络等方法从人脸特征生成密钥;Vielhauer 等人[67-68]、Feng 等人[69]和 Tanwar 等人[42]研究了从签名生成密钥的方法;Kuan 等人[70]提出并总结了将随机令牌与签名结合以生成密钥的方法;Rathgeb 等人[71]和 Akdogan 等人[72]则研究了基于虹膜的密钥生成方法.

密钥生成方法的代表性方案是模糊提取器(fuzzy extractor)方案和安全概略(secure sketch,也译作安全骨架)方案[73].安全概略方法从生物特征提取一些可以公开的信息,当输入与原始模板相似的信号时,可以根据这些公开信息完美恢复原始生物特征模板.而模糊提取器能够从输入的生物特征信号提取近似均匀分布的随机信号密钥.

为了给不同的生物特征提供有效的度量标准,Dodis 等人给出了 3 种不同的距离:海明距离、集合差(set difference)和编辑距离(edit distance).在海明距离下,由 Juels 和 Wattenberg[74]构造的模糊承诺方案可以被看作一个近似最优的安全概略,且可以通过一般性的构造方法将其改造成近似最优的模糊提取器.在集合差度量下,由 Juels 等人[75]构造的模糊保险箱方案可以被看作一个近似最优的安全概略,且也可以利用一般性构造方法将其转化成一个近似最优的模糊提取器.另外,他们还定义了从编辑距离到集合差的变换,从而可以将集合空间的最优模糊提取器转化到编辑空间.

2) 密钥绑定方法.此类方法最早由 Soutar 等人[76]于 1999 年提出.其基本思想是在加密阶段将随机生成的密钥与生物特征数据绑定在一起.在注册阶段,选择一个与生物特征相互独立的密钥,并将该密钥与生物特征模板以某种方式"绑定"在一起,从而产生一些可以公开的"辅助"数据.在识别阶段,将待认证的生物特征与辅助数据相结合,就可以释放出密钥,从而解密存储的生物特征模板并完成比对.

此类系统需要保证从辅助数据很难获得原始的生物特征或密钥,因此能够满足不可逆的要求.另外,利用不同的密钥与同一生物特征绑定可以生成不同的模板,因此满足了可撤销和不可链接的要求.又因为利用了纠错码技术,此类方法能够较好地处理生物特征数据类的内在变化,因此容错性较好.但此类方法很难应用于成熟的或专用的匹配器,因而很难获得较高的匹配准确率.

在已有的密钥绑定系统中,Bioscrypt 方法[77-78]、模糊承诺(fuzzy commitment, FC)[79]和模糊保险箱(fuzzy vault, FV)[75]是最有代表性的方案.

① Bioscrypt 方法是生物特征加密领域最早的实用化算法之一.其基本思想是将生物特征样本与

一个预定义的随机密钥进行绑定,得到一个 phase-phase 值.如果认证成功,上述 phase-phase 值将被解密,以释放出密钥.但该算法要求对指纹图像预先配准,且没有给出拒识率和误识率等关键信息.

② 模糊承诺(FC)方案是由 Juels 和 Wattenberg[79] 在 1999 年提出的.这种方案的基本思想是将纠错码技术用于生物特征表示,以体现生物特征的"模糊性".该方案借用了比特承诺方案[80] 中的承诺和证据概念,包含 2 个基本步骤:承诺和解承诺.

承诺步骤为:

步骤 1. 从某种纠错码体系选择一个与生物特征向量 ω 等长度的码字 c,并定义两者的偏差 $\delta=c-\omega$;

步骤 2. 给出承诺$\{\text{Hash}(c),\delta\}$.

解承诺步骤为:

步骤 1. 用户输入新鲜生物特征 ω';

步骤 2. 按 $c'=\omega'-\delta=\omega'-\omega+c$ 求新码字 c';

步骤 3. 判断:如果生物特征模板 ω 与 ω' 差别不大,经过纠错码的处理,能够得到 $c=c'$,因此可以通过检验 $\text{Hash}(c)$ 与 $\text{Hash}(c')$ 是否相等来判断新鲜特征模板与存储的模板是否属于同一用户.

该算法要求将生物特征表示为二进制序列,且要求对应分量的排列顺序保持一致,因此较适合于具有规范编码的生物特征,如具有较为规范的 IrisCode(固定长度 2 048 b)编码结构的虹膜特征.Hao 等人[81] 在 2006 年设计并实现了一套虹膜加密方案,采用了双因子认证思想,即必须提供正确的令牌和虹膜特征才能通过认证.该方案取得了良好的识别效果:在错误接受率为 0 的前提下,错误拒绝率为 0.47%.其基本流程如图 10 所示:

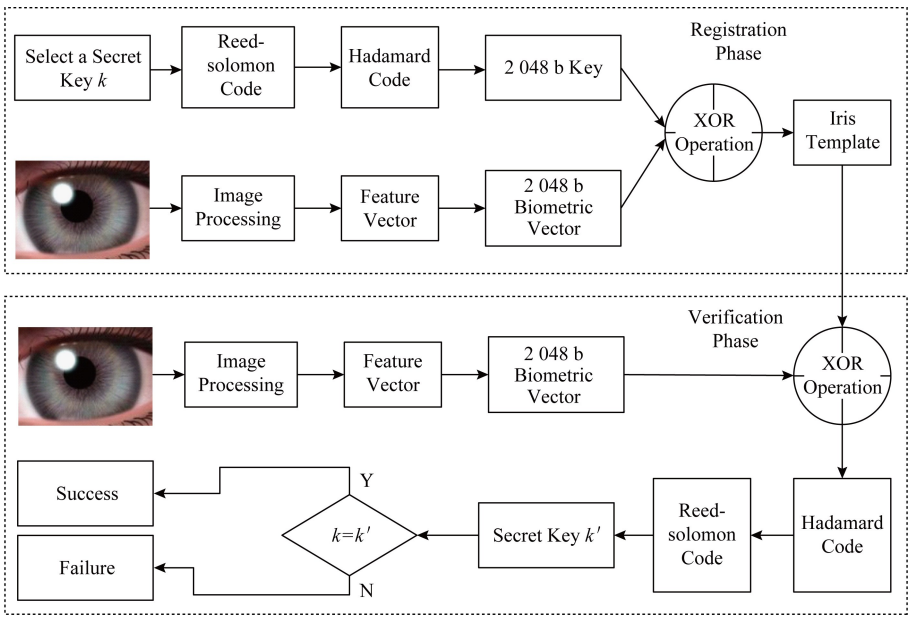

Fig. 10 The basic process of Hao's scheme[81]

图 10 Hao 方案[81] 的基本流程

之后,FC 技术被用于多种生物特征识别方案中:Van 等人[82] 提出了基于真值(real-valued)脸特征的 FC 方案;Teoh 等人[83]、Shi 等人[84] 提出了基于指纹的 FC 方案;Maiorana 和 Campisi 等[85-86] 提出了基于签名的 FC 方案等.近期,FC 技术也被用于物联网设备的保护[87-88] 中.

3) 模糊保险箱(FV)方案是生物特征加密领域最经典的实用化方案之一,由 Juels 和 Sudan[75] 在 2006 年提出.该方案基于无序集构造,因而特别适用于无序生物特征的识别.方案包含 2 个步骤(如图 11 所示).

① 用户 1 选择一个多项式 $p(x)$ 并用其加密密钥 K,然后计算无序集合 A 在多项式 $p(x)$ 上的投影 $p(A)$,生成有限点集$(A,p(A))$.随后,用户 1 随机生成远多于真实点的杂凑点(chaff points)并将其加入$(A,p(A))$,从而构造出保险箱(vault).

② 如果用户 2 拥有另一个无序集合 B,且 B 与 A 有大多数元素重合,则 B 中的很多元素可以落在多项式 p 上.借助于纠错码技术,用户 2 可以重构出多项式 p,从而取出密钥 K.若集合 B 与 A 的重合元素不多,则很难重构出 p.

在上述工作的基础上,Clancy 等人[89]、Yang

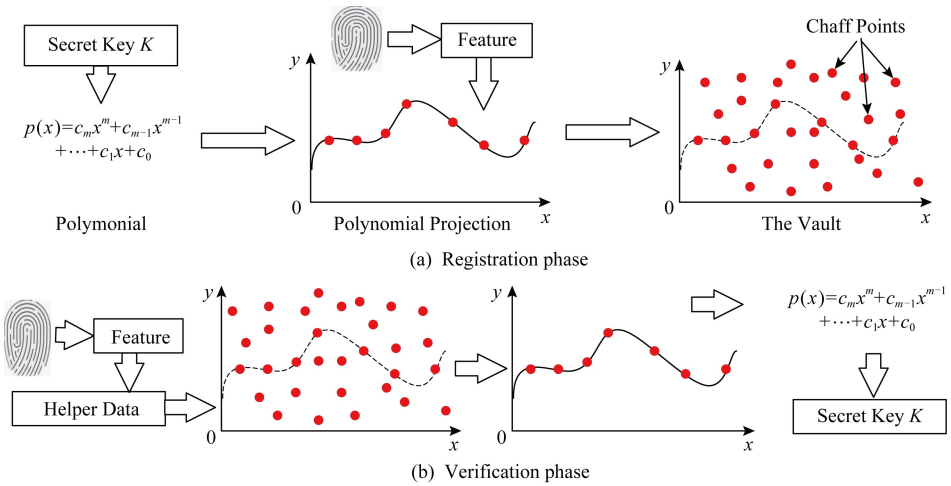

Fig. 11 Principle of the fuzzy vault scheme[75]

图 11 模糊保险箱方案[75]原理

Shenglin 等人[90-91]、Uludag 等人[92-93]、Nandakumar 等人[94]分别构建了指纹保险箱.其中,Uludag 等人的方案未使用纠错码技术,而是使用了循环冗余校验技术,在误识率为 0 的前提下,可以达到 15%的拒识率.

上述方案的一个共同不足是仍然需要对指纹图像进行预先配准,因而有些后续文献致力于提高 FV 方案配准算法的性能[95],或构造无需配准的指纹 FV 方案[96].另外,也有一些文献致力于改进杂凑点的生成方式[97-99]或多项式的生成方式[100]来提升 FV 方案的安全性和效率.其中,Wu 等人[99]的方案使用有序的杂凑点来生成保险箱,从而可以有效利用生物特征的顺序信息,获得了良好的安全性和效率.到目前为止,FV 方案已经被应用到指纹、人脸[101]、虹膜[102-103]、掌纹[104-105]、签名[106]等多种 BA 方案中.

4) 近年来,随着安全多方计算(SMC)[107]技术的发展,安全两方计算成为构造具有隐私保护特性的 BA 系统的一种新手段[108-109].由于此类系统所需的密钥通常不由生物特征直接生成,因此常将其归类于密钥绑定系统[110].

构造适用于 BA 系统的 SMC 方案的密码学工具主要有[11]:同态加密(homomorphic encryption, HE)[111-112]、不经意传输(oblivious transfer, OT)[113]、乱码电路(garbled circuits, GC)[114]和可验证计算(verifiable computation, VC)[115].其中,基于 HE 技术的 BA 系统呈现良好的研究与应用前景.

HE 系统允许对加密数据进行计算,且能由计算后的结果解密得到对相应明文的计算结果,即满足 $Dec(Enc(m_1)\otimes(Enc(m_2))=m_1\oplus m_2$.其中⊕和⊗分别表示明文空间和密文空间中的 2 种运算,*Enc* 和 *Dec* 分别表示加密与解密算法.若系统允许⊕为任意运算,且可以进行任意次⊕运算,则称该方案为一个全同态加密(FHE)方案[112,116-119].

基于 HE 技术的生物特征认证的基本思路是利用 HE 技术的"保密计算"功能实现对生物特征的"保密比对"."认证"过程的一般流程如图 12 所示:

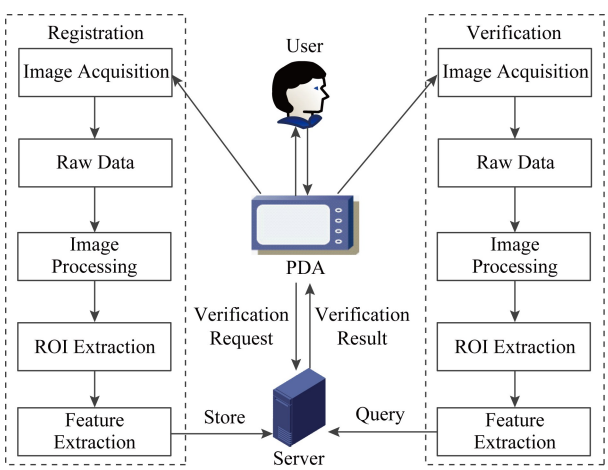

Fig. 12 General flow of HE based biometric verification

图 12 基于同态加密的生物特征"认证"的一般流程

这种架构的 3 个优点非常明显:

① 可以保证在信道中传输的数据和数据库中存储的数据都是密文,即使泄露也不会导致用户的原始生物特征丢失.

② 该架构所用密钥可以与生物特征无关,无法根据生物特征推断出所用密钥.

③ 如果模板泄露,可以用不同密钥对生物特征进行再次加密得到新的模板.新模板与已丢失的模板匹配成功的概率非常小,这是因为它们是用不同的密钥加密得到的.这就满足了文献[9]提到的模板"可更新"和"多样性"的要求.

但由于 HE 技术的发展比较缓慢,基于该技术的 BA 研究直到 2009 年才开始大量涌现,且因为当前 FHE 技术的整体效率仍未达到实用标准,基于 FHE 技术构造的 BA 方案仍然较少[120],单同态技术[121-123]仍然是主要选择.其中较有代表性的工作有:

2010 年 Mauro 等人[124]提出了基于 Pailler 方案的指纹认证系统.该方案利用 Fingercode 表征指纹特征,用平方欧氏距离作为度量.相似的方法已经被应用在人脸识别[125]、虹膜识别[126]等工作中.2012 年,Wong 等人[127]采用 ElGamal 方案实现了虹膜的保密认证,这是首次使用乘法同态算法完成认证.2013 年,Bringer 等人[128]分析了用加法同态技术完成人脸、指纹和虹膜认证的方法,并对基于加法同态的生物特征认证做了总结.此外,另外一些 HE 技术也被用于 BA 方案的构造,如基于 Blum-Goldwasser 系统的方案[129]、基于 Goldwasser-Micali 的方案[130]和基于 RSA 系统的方案[131]等.Ali 等人[132]对基于 RSA 加密算法的生物认证进行了综述,并将其应用到人脸、虹膜、掌形和指纹中.

也有学者将 HE 技术应用到多模态(multimodal)生物特征识别中,如 Barrero 等人[133]、Yildiz 等人[134]将多种 HE 算法结合,实现了多生物特征的融合认证,获得了较好的识别效率和安全性.最近,Salem 等人[21]利用 HE 技术和转移学习(transfer learning)构造了一个基于云的、具有隐私保护特性的安全多方 BA 系统"DeepZeroID",在虹膜和指纹的组合实验中,获得了 95.47%的综合识别准确率.

2016 年 Jong 等人[135]利用具有乘法同态性的 ElGamal 加密方案构造了一个掌纹认证方案.虽然该方案的整体性能并不突出,但提出了 1 个有潜力的过程.该方案的基本过程为:

① 注册时,采用 Garbor 滤波等技术,从掌纹照片获取掌纹特征,表示为二进制特征向量 $\boldsymbol{X}$;

② 根据特征向量 $\boldsymbol{X}$ 构造一个与其等长的整数向量 $\boldsymbol{X}'$.具体方法为:取 2 个不同的素数 a 和 b,若向量 $\boldsymbol{X}$ 中的某位为 0,则将 $\boldsymbol{X}'$中的对应位置为 a,否则将其置为 b;

③ 用 ElGamal 方案对向量 $\boldsymbol{X}'$逐位加密,得到密文向量 $\overline{\boldsymbol{X}}$,将其存为模板;

④ 认证时,用户再次按步骤①②录入掌纹,客户端经计算得到密文特征向量 $\overline{\boldsymbol{Y}}$;

⑤ 在保密状态下计算向量 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的海明距离,具体做法为:将向量 $\overline{\boldsymbol{X}}$ 与 $\overline{\boldsymbol{Y}}$ 的对应分量分别相乘,得到向量 $\overline{\boldsymbol{XY}}$.然后将 $\overline{\boldsymbol{XY}}$ 解密得到向量 $\boldsymbol{T}$,并将 T 的每个分量对 $a\cdot b$ 取模.若某个分量的取模结果为 0,则意味着向量 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的对应比特位的值不同,否则其值相同.

其保密比对过程的正确性是显而易见的.由于 ElGamal 方案具有乘法同态性,向量 $\boldsymbol{T}$ 的每个分量应为向量 $\boldsymbol{X}'$与 $\boldsymbol{Y}'$的对应分量的乘积.若 $\boldsymbol{T}$ 的某个分量对 $a\cdot b$ 取模的结果为 0,说明向量 $\boldsymbol{X}'$与 $\boldsymbol{Y}'$的对应分量的值不同(不可能同时为 a 或为 b,否则其对 $a\cdot b$ 取模的结果必不为 0).

该方案的主要优点在于:①使用了二进制形式的特征向量,并使用海明距离度量掌纹特征的相似度,相较于使用实数或整数特征向量方案的计算复杂度更低.②为进一步降低计算复杂度,采用了随机投影法[136]对数据进行降维,在不显著降低识别性能的前提下获得了较好的效率.但该方案也存在明显不足:①在用 ElGamal 方案对特征向量加密之前,采用了固定映射将二进制特征向量 $\boldsymbol{X}$ 映射为整数特征向量 $\boldsymbol{X}'$,这种构造为比对攻击留下了可乘之机.②提取出的掌纹特征向量质量不佳,导致方案的整体性能较差.

为克服上述方案的不足,王会勇等人[137]、高志强等人[138]分别提出了基于掌纹脊线和图像简单二值化的特征向量生成法,均获得了良好的性能:前者在明文比对过程中几乎取得了 100%的识别准确率;后者的识别准确率约为 99.5%,但效率较高,并将文献[135]方案中的固定映射方式变为多映射方式,消除了比对攻击的隐患.最后,针对不同的特征提取方法、数据降维方法、特征向量大小和阈值进行了多组对比实验.结果表明:经过加解密操作后,在特征向量为 1 000 维、阈值取为 0.23 时,能够取得最佳性能:约 97.5%的正确识别率和 3%的等错误率.

2.3 针对生物特征检索的模板保护技术

在考虑模板保护的前提下,现有的 BA 方案几乎都不适用于"检索方案".主要有 2 个原因:

1)"检索"任务的难度远大于"认证"任务,导致现有方案的效率远未达到实用要求.例如,在张璐等人[139]对模糊保险箱算法[75]的改进工作中,即使不考虑图像校准时间(占用了算法的大部分时间),实现一次指纹模糊保险箱算法所需的时间约为 0.25 s.

这种表现对于“认证”任务来说是可以接受的,但对自动检索任务显然是不实用的.

2) 对基于“密钥绑定”的模板存储方案来说,“检索”任务还存在密钥协调困难,即要求必须使用同一个密钥加密存储的模板和新特征,才能进行有效比对.这是因为当前用于 BA 系统的加密技术均是单密钥的,因而对基于不同密钥的 2 个密文做计算是没有意义的.但在搜索任务中很难实现密钥协调,因为搜索任务的典型场景是待搜索人的身份未知,如果要将加密未知用户生物特征所用的密钥与加密模板所用的密钥统一起来,密钥管理的负担将会很大.

正是由于这些原因,当前以“检索”为目标的方案非常少,这一结论可以从过去 2009-01-01—2019-04-20 的 10 年中,中国知网与 Web of Science 网站收录的相关论文数量看出,如图 13 所示:

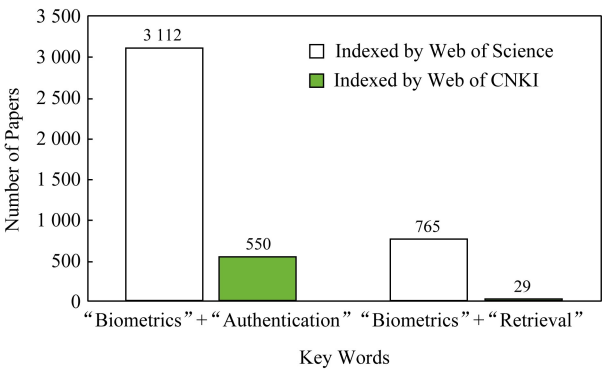

Fig. 13 Number of related papers indexed by Web of Science and CNKI from 2009-01-01 to 2019-04-20

图 13 2009-01-01—2019-40-20 Web of Science 与中国知网收录的相关论文数量

3 构建安全 BA 系统的 3 个困难与解决思路

3.1 构建安全 BA 系统的 3 个困难

虽然已经存在很多技术方案来保护 BA 系统的安全性与隐私性,但实际部署的大多数系统仍然是用传统手段(硬件隔离、身份控制机制等)加以保护的.其主要原因是现有的具有隐私保护特性的 BA 系统的整体性能仍不能满足实际需要,尤其是大规模应用的需要.主要有 3 个典型困难:

1) 生物特征识别一般具有很强的时效性,而对生物特征的混淆或加解密操作会对系统性能造成较大拖累.

2) 基于生物特征加密的认证方案存在密钥管理难题:如果设立密钥管理中心,会带来效率和安全性方面的负担,且现有方案要求密钥中心参与解密,更增加了数据泄露的风险.但如果不设立密钥中心,就需要将密钥交由服务器或客户端保管,都存在密钥泄露或遗失风险.

3) 如 2.3 节所述,生物特征“搜索”任务的难度远大于“认证任务”,因而上述绝大多数方案都是针对“认证”任务构造的,不适应于“搜索”任务.

3.2 解决思路与展望

针对上述困难,现有文献的主要解决思路有 3 种[11]:

1) 将加解密模块硬件化是解决 BA 系统效率不足问题的一种可行思路.另外,基于硬件的两方安全比对也是解决密钥管理难题的一种可能方法.

2) 采用新技术手段来构造 BA 系统,如多模态 BA 技术[25,140]、差分隐私技术[141]等.

3) 在构造具有隐私保护特性的“搜索”方案时,可以首先构造某些“弱化”的实用方案,如:可考虑加密存储用户的特征模板,但以明文形式记录新录入的用户特征,并设计实现“密文”与“明文”的比对方案.相对于“密文”与“密文”的比对方案,“密文”与“明文”的比对方案更容易构造,且更容易获得较高效率,也能满足特定场景下的搜索需要.

4 总 结

本文对生物特征识别系统面临的模板攻击和相应的保护方法相关文献进行了综述.

首先对 BA 系统的一般理论、体系架构及安全与隐私的基本概念做了介绍;然后对保护 BA 系统用户数据安全性和隐私性的关键技术—模板保护技术进行了阐述,重点介绍了模板保护技术的分类与代表性技术方案.最后,指出了构建安全的 BA 系统的 3 个困难和可能的解决思路.

参 考 文 献

[1] Technical Committee of China Academy of Electronic Technology Standardization. White Paper on Biometric Recognition (2017 Edition)[EB/OL]. (2017-07-24)[2019-07-31]. http://www.cesi.cn/images/editor/20170724/20170724083637734.pdf (in Chinese)
(全国信息技术标准化技术委员会生物特征识别分技术委员会. 生物特征识别白皮书(2017 版)[EB/OL]. (2017-07-24)[2019-07-31]. http://www.cesi.cn/images/editor/20170724/20170724083637734.pdf)

[2] Cross J F, Cross J, Daly J. Sex, race, age, and beauty as factors in recognition of faces [J]. Perception & Psychophysics, 1971, 10(6): 393-396

[3] Schuckers S A C. Spoofing and anti-spoofing measures [J]. Information Security Technical Report, 2002, 7(4): 56-62

[4] Gregory B, San Francisco could be first to ban facial recognition tech [EB/OL]. (2019-02-01) [2019-04-01]. https://www. wired. com/story/san-francisco-could-be-first-ban-facial-recognition-tech/

[5] Pagnin E, Mitrokotsa A. Privacy-preserving biometric authentication: Challenges and directions [J]. Security & Communication Networks, 2017: Article ID 7129505

[6] Ross A A, Nandakumar K, Jain A K. Handbook of Multibiometrics: International Series on Biometrics [M]. Berlin: Springer, 2006

[7] Campisi P. Security and Privacy in Biometrics [M]. Berlin: Springer, 2013: 2-6

[8] Goodin D. Get your german interior minister's finger-print here [EB/OL]. (2008-03-30) [2019-04-01]. http://www. theregister. co. uk/2008/03/30/german _ interior _ minister _ fingerprint_appropriated/

[9] Ratha N K. Connell J H, Bolle R M. Enhancing security and privacy in biometrics-based authentication systems [J]. IBM Systems Journal, 2001, 40(3): 614-634

[10] Tuyls P P. Skoric B B, Kevenaar T T. Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-counterfeiting [M]. Berlin: Springer, 2007

[11] Kumar S, Singh S K, Singh A K, et al. Privacy preserving security using biometrics in cloud computing [J]. Multimedia Tools and Applications, 2018, 77(9): 11017-11039

[12] Wehde A, Beffel J N, Finger-Prints Can be Forged [M]. Chicago: Tremonia Publishing Company, 1924

[13] Chingovska I, Mohammadi A, Anjos A, et al. Evaluation methodologies for biometric presentation attack detection [M] //Handbook of Biometric Anti-Spoofing. Berlin: Springer, 2019: 457-480

[14] Krausová A, Hazan H, Matejka J. Biometric data vulnerabilities: Privacy implications [J]. The Lawyer Quarterly, 2018, 8(3): 295-306

[15] Galbally J, McCool C, Fierrez J, et al. On the vulnerability of face verification systems to hill-climbing attacks [J]. Pattern Recognition, 2010, 43(3): 1027-1038

[16] Gomez-Barrero M, Rathgeb C, Scherhag U, et al. Predicting the vulnerability of biometric systems to attacks based on morphed biometric information [J]. IET Biometrics, 2018, 7(4): 333-341

[17] Bhilare S, Kanhangad V, Chaudhari N. A study on vulnerability and presentation attack detection in palmprint verification system [J]. Pattern Analysis and Applications, 2018, 21(3): 769-782

[18] Blanton M, Gasti P. Secure and efficient protocols for iris and fingerprint identification [C] //Proc of the European Symp on Research in Computer Security. Berlin: Springer, 2011: 190-209

[19] Akhtar Z, Micheloni C, Foresti G L. Biometric liveness detection: Challenges and research opportunities [J]. IEEE Security & Privacy, 2015, 13(5): 63-72

[20] Singh M, Singh R, Ross A. A comprehensive overview of biometric fusion [OL]. (2019-02-11) [2019-04-01]. https://www.researchgate.net/publication/331008840_A_Comprehensive_Overview_of_Biometric_Fusion

[21] Salem M, Taheri S, Yuan J S. Utilizing transfer learning and homomorphic encryption in a privacy preserving and secure biometric recognition system [J]. Computers, 2019, 8(1): Article ID 3

[22] Marcel S, Nixon M S, Fierrez J, et al. Handbook of biometric anti-spoofing [M]. Berlin: Springer, 2014

[23] Nixon K A, Aimale V, Rowe R K. Spoof detection schemes [G] //Handbook of Biometrics. Berlin: Springer, 2008: 403-423

[24] Pang Liaojun, Zhao Weiqiang, Li Yan, et al. Basis to Biometric Cyptography [M]. Beijing: Electronic Industry Press, 2016 (in Chinese)
(庞辽军, 赵伟强, 李岩, 等. 生物特征加密基础[M]. 北京: 电子工业出版社, 2016)

[25] Gavrilova M L, Monwar M. Multimodal Biometrics and Intelligent Image Processing for Security Systems [M]. Hershey: IGI Global, 2013

[26] Centro C N. Characterizing attacks to fingerprint verification mechanisms, 2009-30-INF-515 [R]. Madrid, Spain: Ministerio Defensa Espana, 2010

[27] Busch C. Handbook of Biometric Anti-Spoofing [M]. Berlin: Springer, 2019: 503-514

[28] BTAS 2018 Council. Announcements for the 9th IEEE Int Conf on Biometrics: Theory, Applications, and Systems [EB/OL]. [2019-04-01]. https://www. isi. edu/events/btas2018/announcements

[29] International Association for Pattern Recognition. Welcome message from the General Chairs of the 12th IAPR Int Conf on Biometrics (ICB 2019) [EB/OL]. [2019-04-01]. http://www.icb2019.org/Misc/Welcome_message_from_the_General_Chairs.pdf

[30] Ghiani L, Yambay D, Mura V, et al. Livdet 2013 fingerprint liveness detection competition [C] //Proc of the 2013 Int Conf on Biometrics. Piscataway, NJ: IEEE, 2013: 1-6

[31] Yambay D, Becker B, Kohli N, et al. LivDet iris 2017—Iris liveness detection competition [C] //Proc of the 2017 IEEE Int Joint Conf on Biometrics. Piscataway, NJ: IEEE, 2017: 733-741

[32] Biometrics Institute. What Is Biometrics? [EB/OL]. [2019-04-01]. https://www.biometricsinstitute.org/what-is-biometrics/

[33] Center for Biological Recognition and Safety Technology, State Key Laboratory of Pattern Recognition (CBSR). Introduction for CBSR [EB/OL]. [2019-04-01]. http://www.cbsr.ia.ac.cn/china/index%20CH.asp (in Chinese)

(模式识别国家重点实验室生物识别与安全技术研究中心(CBSR). CBSR 中心简介[EB/OL]. [2019-04-01]. http://www.cbsr.ia.ac.cn/china/index%20CH.asp)

[34] Jain A K, Flynn P, Ross A A. Handbook of Biometrics [M]. Berlin: Springer, 2007

[35] Smith M, Mann M, Urbas G. Biometrics, Crime and Security [M]. New York: Routledge, 2018

[36] International Organization for Standardization. ISO/IEC WD 24745 Information technology-security techniques-biometric information protection [OL]. [2019-04-01]. https://www.iso.org/standard/75302.html

[37] Jain A K, Nandakumar K, Nagar A. Biometric template security [J]. EURASIP Journal on Advances in Signal Processing, 2008 (1): Article No.13

[38] Pagnin E, Dimitrakakis C, Abidin A, et al. On the leakage of information in biometric authentication [G] //LNCS 8885: Proc of the Int Conf in Cryptology in India. Berlin: Springer, 2014: 265-280

[39] Menaria L, Jain K. A survey on biometric template protection [J]. International Journal of Scientific Research in Computer Science, 2017, 2(2): 995-999

[40] Wu Lifang, Ma Yukun, Zhou Peng, et al. A review of biometric template protection [J]. Journal of Instruments and Instruments, 2016, 37(11): 2407-2420 (in Chinese)
(毋立芳, 马玉琨, 周鹏, 等. 生物特征模板保护综述[J]. 仪器仪表学报, 2016, 37 (11): 2407-2420)

[41] Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics [J]. EURASIP Journal on Information Security, 2011, 2011 (1): Article No.3

[42] Jin A, Teoh 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

[43] Lumini A, Nanni L. An improved biohashing for human authentication [J]. Pattern Recognition, 2007, 40(3): 1057-1065

[44] Ratha N K, Chikkerur S, Connell J H, et al. Generating cancelable fingerprint templates [J]. IEEE Transactions on pattern analysis and machine intelligence, 2007, 29(4): 561-572

[45] Feng Quan, Su Fei, Anni C, et al. Cracking cancelable fingerprint template of Ratha [C] //Proc of the 2008 Int Symp on Computer Science and Computational Technology, Vol 2. Piscataway, NJ: IEEE, 2008: 572-575

[46] Chikkerur S, Ratha N K, Connell J H, et al. Generating registration-free cancelable fingerprint templates [C] //Proc of the 2nd IEEE Int Conf on Biometrics: Theory, Applications and Systems. Piscataway, NJ: IEEE, 2008: 1-6

[47] Maiorana E, Martinez-Diaz M, Campisi P, et al. Template protection for HMM-based on-line signature authentication [C] //Proc of the 2008 IEEE Computer Society Conf on Computer Vision and Pattern Recognition Workshops. Los Alamitos, CA: IEEE Computer Society, 2008: 1-6

[48] Maiorana E, Campisi P, Fierrez J, et al. Cancelable templates for sequence-based biometrics with application to on-line signature recognition [J]. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2010, 40(3): 525-538

[49] Bloom B H. Space/time trade-offs in hash coding with allowable errors [J]. Communications of the ACM, 1970, 13 (7): 422-426

[50] Rathgeb C, Breitinger F, Busch C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters [C] // Proc of the 2013 Int Conf on Biometrics (ICB). Piscataway, NJ: IEEE, 2013: 1-8

[51] Rathgeb C, Breitinger F, Busch C, et al. On application of bloom filters to iris biometrics [J]. IET Biometrics, 2014, 3 (4): 207-218

[52] Hermans J, Mennink B, Peeters R. When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system [C] //Proc of the 2014 Int Conf of the Biometrics Special Interest Group (BIOSIG). Piscataway, NJ: IEEE, 2014: 1-6

[53] Bringer J, Morel C, Rathgeb C. Security analysis of bloom filter-based iris biometric template protection [C] //Proc of the 2015 Int Conf on Biometrics (ICB). Piscataway, NJ: IEEE, 2015: 527-534

[54] Gomez-Barrero M, Rathgeb C, Galbally J, et al. Unlinkable and irreversible biometric template protection based on bloom filters [J]. Information Sciences, 2016, 2016(370): 18-32

[55] Yang Bian, Martiri E. Using honey templates to augment hash based biometric template protection [C] //Proc of the 39th IEEE Annual Computer Software and Applications Conf. Piscataway, NJ: IEEE, 2015: 312-316

[56] Martiri E, Yang Bian, Busch C. Protected honey face templates [C] //Proc of the 2015 Int Conf of the Biometrics Special Interest Group (BIOSIG). Piscataway, NJ: IEEE, 2015: 1-7

[57] Martiri E, Gomez-Barrero M, Yang B, et al. Biometric template protection based on Bloom filters and honey templates [J]. IET Biometrics, 2017, 6(1): 19-26

[58] Academia. The multiscenario multienvironment biosecure multimodal database (BMDB) [EB/OL]. [2019-04-01]. https://www.academia.edu/23641196/The_Multiscenario_ultienvironment_BioSecure_Multimodal_Database_BMDB_

[59] Tomko G J, Soutar C, Schmidt G J. Fingerprint Controlled Public Key Cryptographic System: US, 5541994[P]. 1996-07-30

[60] Li Peng, Tian Jie, Yang Xin, et al. Biometric template protection [J]. Journal of Software, 2009, 20(6): 1553-1573 (in Chinese)
(李鹏, 田捷, 杨鑫, 等. 生物特征模板保护[J]. 软件学报, 2009, 20(6): 1553-1573)

[61] Ballard L, Kamara S, Reiter M K. The practical subtleties of biometric key generation [C] //Proc of the USENIX Security Symp. Berkeley, CA: USENIX, 2008: 61-74

[62] Monrose F, Reiter M K, Wetzel S. Password hardening based on keystroke dynamics [J]. International Journal of Information Security, 2002, 1(2): 69-83

[63] Monrose F, Reiter M K, Li Qi, et al. Cryptographic key generation from voice [C] //Proc of the 2001 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2001: 202-213

[64] Harada A, Yamazaki Y, Ohki T. Biometric bit string generation for smart-phones using voice data [C] //Proc of the 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conf (APSIPA ASC). Piscataway, NJ: IEEE, 2018: 12-16

[65] Goh A, Ngo D C L. Computation of cryptographic keys from face biometrics [G] //LNCS 2828: Proc of the IFIP Int Conf on Communications and Multimedia Security. Berlin: Springer, 2003: 1-13

[66] Roh J, Cho S, Jin S H. Learning based biometric key generation method using CNN and RNN [C] //Proc of the 10th Int Conf on Information Technology and Electrical Engineering (ICITEE 2018). Piscataway, NJ: IEEE, 2018: 136-139

[67] Vielhauer C, Steinmetz R, Mayerhofer A. Biometric hash based on statistical features of online signatures [C] //Proc of the Object Recognition Supported by User Interaction for Service Robots. Piscataway, NJ: IEEE, 2002: 123-126

[68] Vielhauer C, Steinmetz R. Handwriting: Feature correlation analysis for biometric hashes [J]. EURASIP Journal on Advances in Signal Processing, 2004, 2004(4): 542-558

[69] Feng Hao, Chan C W. Private key generation from on-line handwritten signatures [J]. Information Management & Computer Security, 2002, 10(4): 159-164

[70] Kuan Y W, Goh A, Ngo C L D, et al. Cryptographic keys from dynamic hand-signatures with biometric secrecy preservation and replaceability [C] //Proc of the 4th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05). Piscataway, NJ: IEEE, 2005: 27-32

[71] Rathgeb C, Uhl A. Privacy preserving key generation for iris biometrics [C] //Proc of the IFIP Int Conf on Communications and Multimedia Security. Berlin: Springer, 2010: 191-200

[72] Akdogan D, Altop D K, Levi A. Secure key agreement based on ordered biometric features [OL]. [2019-04-01]. https://doi.org/10.1016/j.comnet.2019.106885

[73] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data [C] //Proc of the Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 523-540

[74] Teoh A B J, Toh K A, Yip W K. 2^N discretisation of biophasor in cancellable biometrics [C] //Proc of the 2007 Int Conf on Biometrics. Berlin: Springer, 2007: 435-444

[75] Juels A, Sudan M. A fuzzy vault scheme [J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257

[76] Soutar C, Roberge D, Stoianov A, et al. ICSA Guide to Cryptography [M]. New York: McGraw-Hill, 1998

[77] Soutar C, Roberge D, Stoianov A, et al. Biometric encryption using image processing [G] //SPIE 3314: Proc of the Optical Security and Counterfeit Deterrence Techniques II. Bellingham, WA: SPIE, 1998: 178-188

[78] Soutar C, Roberge D, Stoianov A, et al. Biometric encryption: Enrollment and verification procedures [G] //SPIE 3386: Proc of the Optical Pattern Recognition IX. Bellingham, WA: SPIE, 1998: 24-36

[79] Juels A, Wattenberg M. A fuzzy commitment scheme [C] //Proc of the 6th ACM Conf on Computer and Communications Security. New York: ACM, 1999: 28-36

[80] Naor M. Bit commitment using pseudorandomness [J]. Journal of Cryptology, 1991, 4(2): 151-158

[81] Hao Feng, Anderson R, Daugman J. Combining crypto with biometrics effectively [J]. IEEE Transactions on Computers, 2006, 55(9): 1081-1088

[82] Van D V, Kevenaar T, Schrijen G J, et al. Face biometrics with renewable templates [G] //SPIE 6072: Proc of the Security, Steganography, and Watermarking of Multimedia Contents VIII. Bellingham, WA: SPIE, 2006: 2-12

[83] Teoh A B J, Kim J. Secure biometric template protection in fuzzy commitment scheme [J]. IEICE Electronics Express, 2007, 4(23): 724-730

[84] Shi Sha, Cui Jia, Liu Yang, et al. Fingerprint recognition strategies based on a fuzzy commitment for cloud-Assisted IoT: A minutiae-based sector coding approach [J]. IEEE Access, 2019, 7: 44803-44812

[85] Maiorana E, Campisi P, Neri A. User adaptive fuzzy commitment for signature template protection and renewability [J]. Journal of Electronic Imaging, 2008, 17(1): 011011

[86] Maiorana E, Campisi P. Fuzzy commitment for function based signature template protection [J]. IEEE Signal Processing Letters, 2009, 17(3): 249-252

[87] Choi D, Seo S H, Oh Y S, et al. Two-factor fuzzy commitment for unmanned IoT devices security [J]. IEEE Internet of Things Journal, 2019, 6(1): 335-348

[88] Bentahar A, Meraoumia A, Bendjenna H, et al. IoT securing system using fuzzy commitment for DCT-based fingerprint recognition [C] //Proc of the 3rd Int Conf on Pattern Analysis and Intelligent Systems. Piscataway, NJ: IEEE, 2018: 1-5

[89] Clancy T C, Kiyavash N, Lin D J. Secure smartcardbased fingerprint authentication [C] //Proc of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications. New York: ACM, 2003: 45-52

[90] Yang Shenglin, Verbauwhede I M. A secure fingerprint matching technique [C] //Proc of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications. New York: ACM, 2003: 89-94

[91] Yang Shenglin, Verbauwhede I. Automatic secure fingerprint verification system based on fuzzy vault scheme [C] //Proc of the IEEE Int Conf on Acoustics, Speech, and Signal Processing. Piscataway, NJ: IEEE, 2005: 609-612

[92] Uludag U, Pankanti S, Jain A K. Fuzzy vault for fingerprints [C] //Proc of the Int Conf on Audio-and Video-Based Biometric Person Authentication. Berlin: Springer, 2005: 310-319

[93] Uludag U, Jain A. Securing fingerprint template: Fuzzy vault with helper data [C] //Proc of the 2006 Conf on Computer Vision and Pattern Recognition Workshop. Piscataway, NJ: IEEE, 2006: 163-163

[94] Nandakumar K, Jain A K, Pankanti S. Fingerprint-based fuzzy vault: Implementation and performance [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(4): 744-757

[95] Chung Y, Moon D, Lee S, et al. Automatic alignment of fingerprint features for fuzzy fingerprint vault [C] //Proc of the 2006 Int Conf on Information Security and Cryptology. Berlin: Springer, 2005: 358-369

[96] Li Peng, Yang Xin, Cao Kai, et al. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme [J]. Journal of Network and Computer Applications, 2010, 33 (3): 207-220

[97] Nguyen M T, Truong Q H, Dang T K. Enhance fuzzy vault security using nonrandom chaff point generator [J]. Information Processing Letters, 2016, 116(1): 53-64

[98] Nguyen T H, Wang Yi, Ha Yajun, et al. Improved chaff point generation for vault scheme in bio-cryptosystems [J]. IET Biometrics, 2013, 2(2): 48-55

[99] Wu Lifang, Xiao Peng, Yuan Songlong, et al. A fuzzy vault scheme for ordered biometrics [J]. Journal of Communications, 2011, 6(9): 682-690

[100] Moon D, Choi W Y, Moon K, et al. Fuzzy fingerprint vault using multiple polynomials [C] //Proc of the 13th IEEE Int Symp on Consumer Electronics. Piscataway, NJ: IEEE, 2009: 290-293

[101] Wu Yongdong, Qiu Bo. Transforming a pattern identifier into biometric key generators [C] //Proc of the 2010 IEEE Int Conf on Multimedia and Exposition. Piscataway, NJ: IEEE, 2010: 78-82

[102] Lee Y J, Bae K, Lee S J, et al. Biometric key binding: Fuzzy vault based on iris images [C] //Proc of the Int Conf on Biometrics. Berlin: Springer, 2007: 800-808

[103] Wu Xiangqian, Qi Ning, Wang Kunquan, et al. An iris cryptosystem for information security [C] //Proc of the 2008 Int Conf on Intelligent Information Hiding and Multimedia Signal Processing. Piscataway, NJ: IEEE, 2008: 1533-1536

[104] Wu Xiangqian, Wang Kunquan, Zhang D. A cryptosystem based on palmprint feature [C] //Proc of the 19th Int Conf on Pattern Recognition. Piscataway, NJ: IEEE, 2008: 1-4

[105] Kumar A, Kumar A. Development of a new cryptographic construct using palmprint-based fuzzy vault [J]. EURASIP Journal on Advances in Signal Processing, 2009, 2009(1): Article ID 967046

[106] Kholmatov A, Yanikoglu B. Biometric cryptosystem using online signatures [C] //Proc of the Int Symp on Computer and Information Sciences. Berlin: Springer, 2006: 981-990

[107] Yao A C C. Protocols for secure computations [C] //Proc of the 23rd FOCS. Piscataway, NJ: IEEE, 1982: 160-164

[108] Blanton M, Aliasgari M. Secure computation of biometric matching, 2009-03 [R]. South Bend, USA: Department of Computer Science and Engineering, University of Notre Dame, 2009

[109] Evans D, Huang Yan, Katz J, et al. Efficient privacy-preserving biometric identification [C] //Proc of the 17th Conf Network and Distributed System Security Symp. Reston, VA: The Internet Society, 2011: 2652-2660

[110] Bringer J, Chabanne H, Patey A. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends [J]. IEEE Signal Processing Magazine, 2013, 30(2): 42-52

[111] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms [J]. Foundations of Secure Computation, 1978, 4(11): 169-180

[112] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of the STOC 2009. New York: ACM, 2009: 169-178

[113] Chou T, Orlandi C. The simplest protocol for oblivious transfer [C] //Proc of the Int Conf on Cryptology and Information Security in Latin America. Berlin: Springer, 2015: 40-58

[114] Yao A C C. How to generate and exchange secrets [C] //Proc of the 27th Annual Symp on Foundations of Computer Science. Piscataway, NJ, 1986: 162-167

[115] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [C] //Proc of the Annual Cryptology Conf. Berlin: Springer, 2010: 465-482

[116] Van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C] //Proc of the EUROCRYPT 2010. Berlin: Springer, 2010: 24-43

[117] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [J]. ACM Transactions on Computation Theory, 2014, 6(3): No.13

[118] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler asymptotically-faster attribute-based [C] //Proc of the CRYPTO 2013. Berlin: Springer, 2013: 75-92

[119] Nuida K, Kurosawa K. (Batch) fully homomorphic encryption over integers for non-binary message spaces [C] //Proc of the EUROCRYPT 2015. Berlin: Springer, 2015: 537-555

[120] Yasuda M, Shimoyama T, Kogure J, et al. Packed homomorphic encryption based on ideal lattices and its application to biometrics [C] //Proc of the Int Conf on Availability, Reliability, and Security. Berlin: Springer, 2013: 55-74

[121] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472

[122] Pascal P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes [C] //Proc of the EUROCRYPT 1999. Berlin: Springer, 1999: 223-238

[123] Naccache D, Stern J. A new public key cryptosystem based on higher residues [C] //Proc of the ACM Conf on Computer and Communications Security. New York: ACM, 1998: 59-66

[124] Barni M, Bianchi T, Catalano D, et al. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates [C] //Proc of the 4th IEEE Int Conf on Theory, Applications and Systems. Piscataway, NJ: IEEE, 2010: 1-7

[125] Montano R B. Biometric validation method and biometric terminal: US, 9537654 [P]. 2017-01-03

[126] Yasuda M. Secure Hamming distance computation for biometrics using ideal-lattice and ring-LWE homomorphic encryption [J]. Information Security Journal: A Global Perspective, 2017, 26(2): 85-103

[127] Wong K S, Kim M H. A privacy-preserving biometric matching protocol for iris codes verification [C] //Proc of the 3rd FTRA Int Conf on Mobile Ubiquitous and Intelligent Computing. Piscataway, NJ: IEEE, 2012: 120-125

[128] Bringer J, Chabanne H, Patey A. Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends [J]. IEEE Signal Processing Magazine, 2013, 30(2): 42-52

[129] Rachapalli D R, Kalluri H K. A survey on biometrie template protection using cancelable biometric scheme [C] //Proc of the 2nd Int Conf on Electrical, Computer and Communication Technologies (ICECCT 2017). Piscataway, NJ: IEEE, 2017: 1-4

[130] Lopez, Nicole A D, Richard B L, et al. Securing health information system with CryptDB [G] //Theory and Practice of Computation: Proc of Workshop on Computation: Theory and Practice 2015. Singapore: World Scientific, 2017: 136-158

[131] Dhande M, Bamania A, Mehta U, et al. Secure client-server authentication system using grid based and zero knowledge protocol with RSA cryptography [J]. Imperial Journal of Interdisciplinary Research, 2017, 3(4): 403-405

[132] Ali R, Pal A K. A secure and robust three-factor based authentication scheme using RSA cryptosystem [J]. Int Journal of Business Data Communications and Networking (IJBDCN), 2017, 13(1): 74-84

[133] Gomez B M, Maiorana E, Galbally J, et al. Multi-biometric template protection based on homomorphic encryption [J]. Pattern Recognition, 2017, 67: 149-163

[134] Yildiz M, Yanikoğlu B, Kholmatov A, et al. Biometric layering with fingerprints: template security and privacy through multi-biometric template fusion [J]. The Computer Journal, 2017, 60(4): 573-587

[135] Im J H, Choi J C, Nyang D H, et al. Privacy-preserving palm print authentication using homomorphic encryption [G] //Autonomic and Secure Computing: Proc of the 14th Intl Conf on Pervasive Intelligence and Computing. Piscataway, NJ: IEEE, 2016: 878-881

[136] Bingham E, Mannila H. Random projection in dimensionality reduction: applications to image and text data [C] //Proc of the 7th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. New York: ACM, 2001: 245-250

[137] Wang Huiyong, Ding Yong, Tang Shijie, et al. An efficient privacy-preserving palmprint authentication scheme based on homomorphic encryption [C] //Proc of the 2017 Int Symp on Cyberspace Safety and Security. Berlin: Springer, 2017: 503-512

[138] Gao Zhiqiang, Ding Yong, Wang Huiyong, et al. A new way for extracting region of interest from palmprint by detecting key points [C] //Proc of the 2017 Int Symp on Cyberspace Safety and Security. Berlin: Springer, 2017: 442-451

[139] Zhang Lu, Wang Jinhai, Cui Jun, et al. Research on parameters optimization for fuzzy vault algorithm of template alignment [J]. Journal of Frontiers of Computer Science and Technology, 2017, 11(9): 1451-1460 (in Chinese)
(张璐, 王金海, 崔军, 等. 模糊保险箱算法的模板校准参数优化研究[J]. 计算机科学与探索, 2017, 11(9): 1451-1460)

[140] Zhang Lu, Wang Huabin, Taoliang, et al. Adaptive multi-biometric feature fusion based on classification distance score [J]. Journal of Computer Research and Development, 2018, 55(1): 151-162 (in Chinese)
(张露, 王华彬, 陶亮, 等. 基于分类距离分数的自适应多模态生物特征融合[J]. 计算机研究与发展, 2018, 55(1): 151-162)

[141] Dwork C. Differential privacy [G] //Encyclopedia of Cryptography and Security. Berlin: Springer, 2011: 338-340

Wang Huiyong, born in 1977. PhD. Associate professor. His main research interests include privacy-preserving technologies, biometric authentication and machine learning.

Tang Shijie, born in 1980. PhD candidate, lecturer. Her main research interests include data fusion, homomorphic encryption and privacy-preserving technologies.

Ding Yong, born in 1975. PhD, professor, PhD supervisor. Senior member of Chinese Association for Cryptologic Research. His main research interests include public key cryptography, homomorphic encryption, cryptographic protocols, block chain and its applications.

Wang Yujue, born in 1981. PhD, associate professor. Member of Chinese Association for Cryptologic Research. His main research interests include application cryptography, cloud computing security and data privacy protection.

Li Jiahui, born in 1996. Master candidate. Her main research interests include biometric authentication and privacy-preserving technologies.

2020 年《计算机研究与发展》专题(正刊)征文通知
——人机混合增强智能的典型应用

当前,以大数据驱动的机器学习为核心的人工智能在不确定性、脆弱性和开放性实际应用环境中面临重大挑战.随着知识引导的兴起,一种新的学习范式——“知识引导+数据驱动”的人机混合增强智能应运而生.其基本思路是将人的高级认知、推理和随机决策能力引入到机器高效的计算过程中,实现人在回路的混合增强智能.人机混合的增强智能还面临一系列难题,例如,如何将人的认知、决策行为与机器的知识表征、因果推理过程有效融合;如何构建面向不同计算应用任务的人机混合智能增强智能方法;如何表征和评估人与机器形成的混合增强智能系统的性能等.

《计算机研究与发展》拟于 2020 年 12 月出版应用技术专题——人机混合增强智能的典型应用.本专题希望围绕上述难题讨论人机混合增强智能的关键技术与发展趋势,报导相关技术在行业中的实践案例,交流思想和成果,进而促进相关技术的研究与发展.

征文内容 本专题包括(但不限于)下列主题:

1) 人机混合的知识表征与融合;
2) 人机混合的知识理解与因果推理;
3) 人机混合增强智能在教育领域的典型应用;
4) 人机混合增强智能在舆情分析领域的典型应用;
5) 人机混合增强智能在智慧税务领域的典型应用;
6) 人机混合增强智能在智慧医疗领域的典型应用.

投稿要求

1) 论文应属于作者的科研成果,数据真实可靠,具有重要的学术价值与推广应用价值,未在国内外公开发行的刊物或会议上发表或宣读过,不存在一稿多投问题.作者在投稿时,需向编辑部提交版权转让与投稿声明.
2) 论文一律用 Word 排版,格式体例请参考《计算机研究与发展》近期文章.
3) 论文请通过期刊网站 (http://crad.ict.ac.cn)进行投稿,并在作者留言中注明“人机混合增强智能 2020 专题”(否则按自由来稿处理).

重要日期

征文截止日期:2020 年 9 月 15 日
录用通知日期:2020 年 10 月 15 日
修改稿提交日期:2020 年 10 月 20 日
出版日期:2020 年 12 月

特邀编委

郑庆华 教授 西安交通大学 qhzheng@mail.xjtu.edu.cn

联系方式

编 辑 部:crad@ict.ac.cn, 010-62620696, 010-62600350
通信地址:北京 2704 信箱《计算机研究与发展》编辑部
邮 编:100190