

信息技术 生物特征识别模板保护方案 的性能测试

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 符合性	3
6 生物特征模板保护方法	3
6.1 概述	3
6.2 生物特征模板保护系统的通用架构	4
6.3 数据分离	7
6.4 模板保护系统典型架构示例	7
7 生物特征模板保护方案性能评估概述	9
7.1 攻击生物特征模板保护系统的方法	9
7.2 有别于传统识别性能度量项的必要性	9
7.3 技术评估	9
7.4 理论评估与实验评估	9
7.5 威胁模型	9
8 生物特征模板保护系统的性能度量项	11
8.1 总则	11
8.2 多重生物特征访问控制系统案例	11
8.3 注册和验证性能的度量项	11
8.4 安全和隐私保护性能度量项	13
附录 A（资料性）性能评估中使用算法或证明的出版物	17
参考文献	18

引 言

GB/T XXXXX—XXXX《信息技术 生物特征识别模板保护方案的性能测试》主要目的是描述生物特征模板保护领域中的保护方法和保护方案性能评估,并规定了生物特征模板保护方案准确性、保密性和隐私性的评估方法,旨在科学、客观地评估生物特征模板保护方案。

生物特征模板是从个体的生物学特性和行为特性中获得的一组参考生物特征项,并存储在注册数据库中。一般系统允许有限次数地撤销和更新已被侵犯的生物特征注册信息。但是,个体可以提取的独特的生物特征的数量是有限的,因此生物特征注册信息不可能像信用卡号或密码一样无限次地被撤销和更新。存储在注册数据库中的生物特征注册记录被侵犯是一个严重的问题。在传统的生物特征识别控制系统中,攻击者入侵注册数据库可获得注册个体的生物特征数据。如果生物特征识别系统容易受到呈现攻击或重放攻击,那么攻击者就能通过所入侵的注册数据库的个体生物特征数据伪装成个体对系统进行访问,而这是我们不能接受的。更进一步,如果生物特征注册数据库中包含未受保护的模板,并且在多个应用程序中采用相同的生物特征识别模态,则攻击者可以将这些应用程序中的个体帐户关联起来(交叉匹配)。因此,我们需要采取各种方法和程序来降低被侵犯的风险,保护注册数据库中个体生物特征模板的保密性。

目前,生物特征模板保护技术已经实现无需将个体的生物特征项直接存储在访问控制设备中来进行生物特征验证。该方法的基本原理是,访问控制系统不是直接存储生物特征项,而是从生物特征项中衍生一些数据并将这些提取的衍生数据存储在设备上。在生物特征验证阶段,系统从需要访问的个体采集生物特征样本,而后和衍生数据进行比对,产生生物特征验证的结果。衍生数据具有几乎或完全不揭示在注册阶段采集到的生物特征特性信息的关键特性。即使访问控制设备被攻击者侵犯,只有衍生数据落入攻击者的手中,但这些数据并不能使攻击者能够恢复在注册数据库中的个体的生物特征特性,从而保护了注册数据库中的个体隐私信息。此外,如果攻击者试图通过伪造的生物特征样本来访问系统,那么一个设计良好的生物特征识别系统可以通过衍生数据比对来辨识出伪造的生物特征样本,从而导致生物特征验证失败。因此,该技术不但保护了注册数据库中个体的保密性,而且实现了安全的生物特征验证。

新度量项的原理

有多种方法可以实现生物特征模板保护。无论采用何种方法来构建衍生数据,在评估生物特征模板保护系统时都必须考虑以下问题:

- a) 系统拒绝真实个体和接受冒名顶替者的概率是多少?这是任何生物特征验证系统都必然要考虑的一个问题。FNMR和FMR这两个度量项用来衡量传统的生物识别系统的这个性能(GB/T 29268.1),生物特征模板保护系统也继续采用这些度量项。
- b) 对已注册个体数据库有所了解的攻击者被成功验证为已注册个人之一的概率有多大?
- c) 攻击者通过攻击访问控制设备并窃取到存储在设备上的衍生注册信息后所能获得的信息是多少。在传统生物特征识别系统中,攻击者可以获得的重要信息,包括存储在设备上的生物特征模板或者特征项。生物特征模板保护系统的目标就是确保这些存储在设备上的衍生数据不会泄漏注册个体的太多信息。
- d) 攻击者成功侵犯一个或多个访问控制设备并窃取存储在设备上的数据后,利用所获得的信息在访问控制设备上成功验证的概率是多少?

这些问题构成了评估生物特征模板保护系统的准确性、保密性和隐私性的基础,并成功引入了一组与之前评估传统生物特征识别系统不同的新度量项。

标准化的必要性

基于生物特征模板保护的系统有多种架构，例如，基于模糊保险箱的系统、基于安全概略的系统、可撤销的生物特征系统、基于安全多方计算的系统等。因此有必要定义适用于各种基于生物特征模板保护架构的关键度量项，并回答以上问题，从而为基于不同架构的系统进行比对提供了一个共同的基础。本文件的目标是确定这些新的度量项，以用于评估基于模板保护的生物特征验证和辨识系统。第8章中为每个度量项提供了基于理论和实验的定义。

信息技术 生物特征识别模板保护方案的性能测试

1 范围

本文件支持生物特征模板保护方案的准确性、保密性和隐私性的评价。确立了用于说明生物特征模板保护方案性能的定义、术语和度量项。本文件特别规定了以下各项的测试和报告的要求：

- 生物特征模板保护方案的理论和实验的准确性；
- 成功攻击生物特征模板保护方案（单个或多个）的理论和实验的概率；
- 当一个或多个生物特征模板保护方案被侵犯时，泄漏的关于原始生物特征的信息。

本文件适用于评估生物特征模板保护方案的准确性、保密性和隐私性。

本文件不适用于：

- 建立模板保护方案；
- 针对传统加密方案的测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

ISO/IEC 2382-37 信息技术 词汇 第 37 部分：生物特征识别 (Information technology — Vocabulary — Part 37: Biometrics)

注：GB/T 5271.37-2021 信息技术 词汇 第37部分：生物特征识别（ISO/IEC 2382—37：2017，MOD）。

ISO/IEC 19795-1 信息技术 生物特征识别性能测试和报告 第1部分：原则与框架 (Information technology — Biometric performance testing and reporting — Part 1: Principles and framework)

注：GB/T 29268.1—2012 信息技术 生物特征识别性能测试和报告 第1部分：原则与框架（ISO/IEC 19795-1：2006，IDT）

ISO/IEC 19795-2 信息技术 生物特征识别性能测试和报告 第2部分：技术与场景评价的测试方法 (Information technology Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation)

注：GB/T 29268.2-2012 信息技术 生物特征识别性能测试和报告 第2部分：技术与场景评价的测试方法（ISO/IEC 19795-2：2007，IDT）

ISO/IEC 24745:2022 信息技术 数字安全和隐私保护 生物特征信息保护 (Information security, cybersecurity and privacy protection— Biometric information protection)

注：ISO/IEC 24745:2022 被引用的内容与 ISO/IEC 24745:2011 被引用的内容没有技术上的差异。

3 术语和定义

ISO/IEC 2382-37和ISO/IEC 24745界定的以及下列术语和定义适用于本文件。

3.1

精度下降 accuracy degradation

对于同一生物特征识别系统，在有无模板保护方案的情况下进行测试，所得FNMR/FMR（或FAR/FRR）之间的差异。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/796010040053010234>