

基于改进生物特征保险箱的 Multi-Factor Authentication Method Based on Improved Biometric Vault

多因素认证方法

贵圣兰¹, 刁力力² (1. 南京钢铁股份有限公司, 江苏 南京 210000; 2. 南京特殊教育师范学院, 江苏 南京 210000)
Ben Shenglan¹, Diao Lili² (1. Nanjing Iron and Steel United Co. Ltd., Nanjing 210000, China; 2. Nanjing Normal University of Special Education, Nanjing 210000, China)

摘要:

随着移动互联网及识别技术的发展,生物特征识别技术被广泛用于用户身份认证。与密码、智能卡等传统认证技术相比,生物特征的隐私保护问题尤为重要。如何在降低识别准确率的前提下对生物特征进行有效的保护也成为研究者关注的热点问题。针对该问题,提出一个基于改进模糊保险箱技术的生物特征模板保护算法,并基于该算法提出一个增强的三因素认证方案用于远程身份认证。安全分析表明,提出的认证方案可以在不降低生物特征识别率的同时保证认证的安全性,避免生物特征的泄漏。

关键词:

身份认证;生物特征模板保护;多因素认证;模糊保险箱

doi:10.12045/j.issn.1007-3043.2026.09.002

文章编号:1007-3043(2026)09-0007-06

中图分类号:TP309.7

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

With the development of mobile Internet and recognition technologies, biometric recognition has been widely deployed for user identity authentication. Compared with traditional authentication mechanisms such as passwords and smart cards, the privacy protection of biometric data has become an extremely critical concern. Effectively protecting biometric templates without degrading recognition accuracy has also become a prominent research hotspot in academia. To address this issue, a biometric template protection algorithm based on the improved fuzzy vault technique is proposed, and based on this algorithm, an enhanced three-factor authentication scheme for remote identity authentication is constructed. Security analysis demonstrates that the proposed authentication scheme can guarantee the authentication security while maintaining the original biometric recognition accuracy, and effectively prevent the leakage of sensitive biometric data.

Keywords:

Authentication; Biometric template protection; Multi-factor authentication; Fuzzy vault

引用格式: 贵圣兰, 刁力力. 基于改进生物特征保险箱的多因素认证方法[J]. 邮电设计技术, 2026(9): 7-12.

0 引言

生物特征识别被广泛应用于互联网及移动支付认证。研究者常将生物特征与密码等传统因素结合,形成多因素认证方案^[1]。然而,生物特征包含大量用户隐私信息,具有不可撤销和修改的特性,一旦泄露将导致严重隐私风险和身份冒用问题。现有方案多采用哈希变换加密生物特征^[2-3],但由于哈希函数不具备距离保持特性,难以应对生物特征的内类变化,在

实际应用中存在较大局限性。

针对上述问题,研究者提出多种生物特征模板保护技术^[4-5],通过对生物特征数据进行加密或变换,生成生物特征模板保存在数据库中,用于后续比对,从而可以降低生物特征数据泄漏的风险,保障生物特征的隐私性和安全性。常见的生物特征模板保护技术可分为基于特征变换的方法和基于加密的方法2类。

基于特征变换的方法将原始生物特征数据经过函数变换后作为生物特征模板存储在数据库中。例如 BioHashing 算法^[6],使用一个正交随机变换矩阵对生物特征进行变换,通过改变变换矩阵,可以生成不

收稿日期:2026-07-06

同的生物特征模板,实现生物特征的可撤销性。文献[7]使用单向变换函数将指纹的特征点投影到另一个空间,如果生物特征模板泄漏,可以通过修改变换函数的参数进行更新。对于这类方法,生物特征模板的安全性取决于通过逆变换获取原始特征的难度,相应的改进也主要集中在提升变换函数的不可逆性上^[8-9]。

基于加密的方法使用生物特征来保护密码的密钥系统。根据密钥产生方式的不同,又可以分为密钥生成算法和密钥绑定算法。密钥生成算法注册时从生物特征中直接生成密钥保存在数据库中,在认证时由查询生物特征再次生成密钥并进行比对。代表性的密钥生成算法包括模糊提取器算法和安全概略算法^[10]。为生成一致性强的密钥,这类算法要求注册和查询的生物特征尽可能接近,因此生物特征的类内多变性会影响识别的性能。密钥绑定的方法将生物特征和密钥以某种特定算法结合在一起生成生物特征模板和辅助数据存储在数据库中。在认证时,首先查询生物特征和辅助数据从生物特征模板中恢复密钥,然后比对密钥完成认证。通过绑定不同的密钥,密钥绑定算法可以生成不同的生物特征模板,实现可撤销性和不可链接性的要求。典型的密钥绑定算法包括模糊承诺算法^[11-12]和模糊保险箱算法^[13-14]。

上述生物特征模板保护算法一般都需要将生物特征转换为二值或整型,而在目前主要的生物特征识别算法中,生物特征一般表示为浮点数的有序向量,量化过程会损害特征精度,降低识别率。在距离选择上,上述算法大都只适用于特定的距离度量,普适性较低,也较难适用于识别准确率更高的新算法。因此,如何在保证生物特征安全性的同时,尽可能少的降低识别准确性一直是生物特征模板保护的研究难点。

针对上述问题,本文提出一个基于改进模糊保险箱的生物特征模板保护方案,在保证生物特征安全性的同时,可以容忍生物特征的类内变化,不降低生物特征识别的准确率。该方案还可以适应多种不同的生物特征识别匹配算法,普适性更好。基于改进的生物特征模板保护方案,本文进一步提出三因素的远程身份认证方案,从而可以实现安全、准确、可撤销的远程生物特征认证。

1 生物特征模板保护策略

传统模糊保险箱方法存在2个根本性局限性:一

是其要求将生物特征数据以无序集合方式存储,导致关键位置信息丢失;二是需要将浮点型数据量化为整数或二进制格式,并依赖精确匹配,这与生物特征固有的类内变化相矛盾。针对这2个问题,虽然研究者已采用有序特征插入^[15]、配准技术^[16]等方法加以改进,但这些方法仅能在一定程度上降低部分信息损失,无法彻底解决上述问题。

考虑到远程身份认证中,用户同时持有生物特征和密钥,本文对模糊保险箱进行改进,使用密钥来保护生物特征,设计了一个可以保存和恢复有序浮点数生物特征的方案,从而可以在保护生物特征安全性的同时,不降低生物特征的识别率。对应的生物特征编码和解码过程如下。

1.1 生物特征编码算法

本文提出的编码方案可以直接基于浮点数的生物特征数据进行编码,其具体操作步骤如下。

a) 将密码PW转换为二进制序列 s ,将 s 分割为 $l+1$ 个不重叠的子序列,每个子序列转换成一个参数,得到 $a_0, a_1, a_2, \dots, a_l$ 。 a_0 作为特征的平移参数, $a_1, a_2, \dots, a_l$ 用于生成多项式 $f(x) = a_1x_1 + a_2x_2 + \dots + a_lx_l, x = [x_1, x_2, \dots, x_l]$ 。

b) 将生物特征序列分成 m 个长度为 l 的不重叠子序列 $\{b_j = [b_{j1}, b_{j2}, \dots, b_{jl}]\}_{j=1, \dots, m}$,对各子序列 b_j ,首先计算其在函数 $f(x)$ 上的映射 $f(b_j)$,记 $G = \{(b_j + a_0f(b_j))\}_{j=1, \dots, m}$ 为真实点集。

c) 随机选择 $C = \{(x_i, y_i)\}_{i=1, \dots, n-k}$ 作为杂凑点,其中 x_i 为 l 维的随机向量, $y_i \neq f(x_i - a_0)$ 。

d) 存储 $V = G \cup C$ 作为模糊保险箱。

1.2 生物特征解码算法

在解码步骤中,用户输入查询生物特征 B' 和密码PW',希望从保险箱 V 中恢复注册的生物特征模板。

与编码步骤类似,首先从密码PW'产生平移参数 a'_0 及多项式 $f'(\cdot)$,并将生物特征 B' 分割成 m 个 l 维的子序列 $\{b'_j\}_{j=1, \dots, m}$ 。

而后,算法通过如下方法识别真实点集。对于每个子序列 b'_j ,计算 $b'_j + a'_0$ 到保险箱中各点的 x 分量的距离,选择距离小于阈值 τ 的点作为 b'_j 对应的注册特征子向量的候选集 $T_j = \{(x, y) \mid \text{dist}(b'_j + a'_0, x) \leq \tau\}$ 。

这里距离 $\text{dist}(\cdot, \cdot)$ 可以选择任意合适的距离测度。对于 T_j 中的候选点, 比较 $f'(x)$ 和 y , 将 $b'_j = \arg \min_{x|(x,y) \in T} \left\{ \left\| f'(x - a'_0) - y \right\| \right\}$ 识别为子向量 b'_j 在注册模板中对应的子向量。

从上述过程看出, 要从保险箱中正确复原注册的生物特征模板, 用户必须同时具备有效生物特征和正确密码, 因此, 可以有效保障生物特征模版的安全性。此外, 可以根据生物特征类型和识别算法的要求, 选择不同的子向量长度 l 和距离 $\text{dist}(\cdot, \cdot)$, 从而使生物特征比对的准确性尽可能地接近原识别算法。

2 基于改进模糊保险箱的远程三因素认证方案

基于上述改进的生物特征保险箱, 本文提出一个用于远程身份认证的三因素认证方案。本方案假设注册中心 R 为一个可信的第三方, 注册中心选择主密钥 X_s , 通过可信的信道发到服务器 S 。方案包括用户注册步骤、登录步骤、认证步骤以及密码修改4个部分。所使用的符号如表1所示。

2.1 用户注册步骤

在注册阶段, 用户 C_i 执行下述步骤完成注册。

a) C_i 通过终端设备扫描生物特征 B_i , 设置密码 PW_i , 将 $\{ID_i, B_i, PW_i\}$ 通过安全信道发送给注册中心 R 。

b) 收到信息后, 注册中心 R 产生主密钥 X_s , 计算 $r_i = h(ID_i \| X_s)$, $f_i = h(PW_i \| B_i)$, $e_i = r_i \oplus h(PW_i \oplus B_i)$, 将 $\{ID_i, e_i, f_i, h(\cdot)\}$ 通过安全信道发送给用户 C_i 。将 $\{ID_i, X_s\}$ 通过安全信道发送给服务器存储。

c) 用户 C_i 使用生物特征编码算法 (BioEAlgo) 将生物特征 B_i 编码到模糊保险箱 V_i , 将 $\{ID_i, e_i, f_i, h(\cdot), V_i\}$ 存入用户所持的终端设备。

2.2 登录步骤

用户 C_i 执行如下步骤, 生成有效的登录请求信

息, 发送给服务器 S_i 。

a) 用户 C_i 输入 ID'_i, PW'_i , 扫描生物特征 B'_i 。

b) 用户所持有的终端设备使用生物特征解密算法 (BioDAlgo) 从模糊保险箱 V_i 中恢复注册的生物特征模板 B_i^* 。

c) 用户所持有的终端设备计算 $f'_i = h(PW'_i \| B_i^*)$, 并将其与 f_i 进行比较, 如果 $f'_i = f_i$, 表明用户持有合法的生物特征和密码, 进入步骤 d); 否则, 用户输入的密码 PW'_i 或生物特征 B'_i 至少有一项是无效的, 终止登录过程。

d) 用户 C_i 计算 $M_1 = h(PW'_i \oplus B_i^*)$, $M_2 = e_i \oplus M_1$, $M_3 = h(M_2 \| t_c)$, $M_4 = M_3 \oplus R_c$ 和 $M_5 = h(M_3 \| R_c)$, 其中 t_c 为 C_i 的当前时间戳。

e) C_i 将信息 $\{ID'_i, M_4, M_5, t_c\}$ 发送给远程服务器 S_i 。

2.3 认证步骤

在收到登录请求信息后, 远程服务器 S_i 和用户 C_i 需要执行如下步骤, 对彼此身份进行认证, 并达成一个共享的会话密钥, 用于后续通信。

a) S_i 验证 ID'_i 的有效性。

b) 若 ID'_i 有效, S_i 计算 $M_6 = h(ID'_i \| X_s)$, $M_7 = h(M_6 \| t_c)$, $M_8 = M_4 \oplus M_7$, $M_9 = h(M_7 \| M_8)$, 验证 $M_9 = M_5$ 是否成立。如果不成立, S_i 拒绝登录请求, 并终止会话。否则, S_i 完成对 C_i 的身份认证, 将 $\{ID'_i, t_c\}$ 存入数据库。当再次收到 C_i 的登录请求时, S_i 通过验证 $t'_c \geq t_c$ 是否成立以判断本次登录请求是否是重放攻击。

c) S_i 产生一个随机数 R_s , 计算 $M_{10} = M_6 \oplus R_s$, $M_{11} = h(M_6 \| M_8 \| R_s)$, 返回信息 $\{M_{10}, M_{11}\}$ 给 C_i 。

d) C_i 计算 $M_{12} = M_{10} \oplus M_2$, $M_{13} = h(M_2 \| R_c \| M_{12})$, 并验证 $M_{13} = M_{11}$ 是否成立。如果成立, C_i 完成对 S_i 的身份认证; 否则, C_i 终止会话。

e) 按上述步骤完成相互认证后, C_i 和 S_i 分别计算 $h(R_c \| M_3 \| M_1)$ 和 $h(M_8 \| M_7 \| R_s)$ 作为共享密钥, 用于后续会话。

2.4 更新密码

在更新密码时, 用户 C_i 首先输入 ID'_i , 旧密码 PW'_i , 扫描生物特征 B'_i 。终端设备使用生物特征解密算法恢复注册的生物特征模板 B_i^* , 计算 $f'_i =$

表1 本文所使用的符号

符号	注释	符号	注释
R	可信的注册中心	X_s	服务器主密钥
S_i	认证服务器	R_c	C_i 选择的随机数
C_i	用户	R_s	S_i 选择的随机数
ID_i	用户 C_i 的身份信息	$A \ B$	将数据 A 与数据 B 串联
PW_i	用户 C_i 的密码	$A \oplus B$	对 A 和 B 进行异或
B_i	用户 C_i 的生物特征数据	$\text{dist}(A, B)$	向量 A 与 B 的距离
$h(\cdot)$	单向 hash 函数	-	-

$h(PW'_i \| B_i^*)$, 并比较 $f'_i = f_i$ 以验证用户输入的密码 PW'_i 和生物特征 B'_i 的有效性。

如果 $f'_i = f_i$ 成立, C_i 输入新密码 PW_i^{new} , 终端设备使用 BioEAlgo 计算新的模糊保险箱 V''_i , 并计算 $M'_1 = h(PW' \oplus B_i^*)$, $M_2 = e_i \oplus M'_1$, $e''_i = M'_2 \oplus h(PW_i^{\text{new}} \oplus B_i^*)$, $f'_i = h(PW_i^{\text{new}} \| B_i^*)$ 。最后, 将终端设备中的 V_i, e_i 和 f_i 分别替换为 V''_i, e''_i 和 f'_i , 完成密码更新。

3 安全性及性能分析

3.1 生物特征模板安全性及识别性能分析

有效、安全的生物特征模板通常需要满足如下要求。

a) 不可逆性。攻击者不能从保护的生物特征模板中恢复出原始生物特征数据。

b) 多样性。用户对应的生物特征模板在不同数据库之间不能进行交叉匹配, 否则一个数据库发生泄漏, 会造成其他系统的生物特征认证安全性也受到威胁。

c) 不可链接性。要求不同的身份认证系统中, 用户生物特征模板的关联性尽可能小, 攻击者即使获得用户保存在多个不同系统的生物特征模板, 也不能从这些模板中恢复出原始的生物特征数据。

d) 可撤销性。类似于修改密码功能, 用户可以生成新模板以替换原有生物特征模板, 并且新模板与原有模板间不能相互认证。

e) 识别性能。对生物特征进行的相关保护技术, 不能影响生物特征的识别性能。该项要求关系到生物特征模板保护算法的实际可用性。

除上述要求, 如何提高生物特征模板保护算法对不同生物特征和识别方法的普适性也至关重要。本文方法适用于多种数据类型的生物特征, 并且可以根据识别算法的要求选择合适的距离度量 $\text{dist}(\cdot, \cdot)$, 因此可以适用于多种生物特征识别算法。

本方案使用用户生物特征模板与密钥进行绑定, 加上杂凑点后保存在模糊保险箱中, 生物特征的安全性依赖于杂凑点的数量。假设模糊保险箱中包含 m 对真实点, $n - m$ 对杂凑点, 攻击者需要尝试 $P_n^m = \frac{n!}{(n-m)!}$ 次才有可能找到注册的生物特征点对。即使攻击者选择出了注册的生物特征点对集合, 因为生物特征的认证过程是与用户密码绑定的, 没有用户密

码, 攻击者无法验证所获得的生物特征集合是否正确。因此本方案满足不可逆性的要求。

传统的 Fuzzy Vault 算法中, 用户生物特征数据中的各元素作为 x 分量保存在保险箱中, 如果攻击者获取了该用户在多个不同系统中注册的保险箱, 有可能通过对 x 值聚类找出用户的生物特征数据。本方案中, 用户生物特征数据被分割成多维子向量, 经过平移变换后保存在保险箱中。由于各系统使用的平移参数不同, 攻击者即使获取了用户在多个系统中的生物特征保险箱, 也很难通过聚类找出真实的生物特征数据。因此本方案满足不可链接性的要求。

方案中, 用户可以通过修改密码重新生成生物特征保险箱, 满足可撤销性要求。用户在不同系统中注册的生物特征保险箱, 也可以通过使用不同的密码以满足多样性要求。

与以往的 Fuzzy Vault 算法将生物特征转换为整型的数据集合或向量不同, 本文的生物特征加密算法通过比较 $f'_i = h(PW'_i \| B_i^*)$ 与 f_i 来完成对用户的生物特征认证。其中验证的准确性依赖于注册生物特征模板恢复的准确性, 即 B_i^* 与 B_i 是否一致。该解码方式在生物特征比对时, 使用的是 $\text{dist}(B'_i, B_i) \leq \tau$, 与目前大部分认证算法的比对方式一致, 并且可以根据生物特征识别算法要求选择合适的距离度量, 因此对于识别准确率的影响非常小, 当子特征长度等于原始生物特征时, 识别准确率等价于对应识别算法的明文生物特征识别率。

表2将本文方案与其他生物特征模板保护算法进行比较, Fuzzy Commitment 算法^[12]采用双因子认证思想, 结合令牌和虹膜特征进行认证, 使得生物特征模板具有可撤销性, 但是该方法要求生物特征是固定长度的二进制序列, 对于实值生物特征, 需要首先进行二值化操作, 从而导致识别率降低。文献[14]的 Fuzzy Vault 算法可以用于融合特征的加密, 该方案需要将特征序列转换为十进制, 对于算法的识别率和普适性都有一定影响。与传统 Fuzzy Vault 算法类似, 该算法也不满足不可链接性的要求。文献[9]提出非线性谱哈希方法 (Bonlinear Spectral Hashing, NSH) 对掌静脉数据进行保护, 该方案需要将特征序列转换为二进制, 不适用于人脸等有较高精度要求的生物特征, 对算法普适性都有一定影响。通过表2的比较可以看出, 本文方法能够比较好地兼顾生物特征安全性和识

表2 生物特征模板保护算法比较

比较项	Hao's FC ^[12]	Lin's FV ^[14]	NSH ^[9]	本文方法
不可逆性	是	是	是	是
多样性	是	是	是	是
非链接性	是	否	是	是
可撤销性	是	是	是	是
普适性	否	否	否	是
识别率影响	高	高	中	低

别准确性要求,对于识别算法也具有更好的普适性。

3.2 认证方案的性能及安全性分析

本节分析所提多因素认证方案面临主要类型攻击时的安全性以及认证的性能。本节的安全性分析假设智能终端及通信信道都存在泄漏风险,在这种情况下,攻击者可以同时获取智能终端中存储的信息以及用户与服务器的所有会话信息。

3.2.1 安全性分析

a) 密码猜测攻击。攻击者可以在登录过程中通过验证 $f_i = h(PW_i \| B_i)$ 实现对用户密码的暴力破解。然而,为实现上述目的,攻击者必须先获得用户生物特征模板 B_i ,攻击者完成对密码暴力破解的难度非常大。

b) 伪装攻击。攻击者需要获取 $h(ID_i \| X_s)$ 以伪造登录请求信息。该信息通过 $e_i = h(ID_i \| X_s) \oplus h(PW_i \oplus B_i)$ 形式存储在用户持有的终端设备中。攻击者需要首先破解密码和生物特征,获得 $h(PW_i \oplus B_i)$ 才能从 e_i 中解码出 $h(ID_i \| X_s)$ 。因此,攻击者无法伪造有效的登录信息,完成伪装攻击。

c) 伪装服务器攻击。攻击者需要获取 $h(ID_i \| X_s)$ 、 R_c 和 R_s 以伪造服务器响应信息对用户的登录请求进行响应。然而,如前文分析,攻击者很难通过截取的信息获取上述有效信息。

d) 重放攻击。本文的认证方案使用时间戳 t_c 以抵御重放攻击。假设攻击者A获取了用户之前会话的登录请求信息 (ID_i, M_4, M_5, t_c) ,并将它再次发送给服务器进行登录。收到该信息后,服务器将 t_c 与数据库中存储的时间戳 t'_c 进行比对,由于 $t_c \leq t'_c$,服务器判定该登录请求无效,终止会话。

e) 中间人攻击。攻击者需要在登录和认证阶段将合法的会话信息替换成攻击者伪造的信息。在本

文的认证方案中,由于攻击者无法获取密钥 X_s 和随机数 R_c, R_s ,因此无法在 S_i 和 C_i 通信中伪造有效的信息,骗过交叉验证,实现中间人攻击。

3.2.2 计算性能分析

本文中,生物特征的编码和解码操作通过多项式投影和距离比对完成,只需要多项式时间,计算代价较小,因此本节主要统计散列运算需要的时间。记 T_h 为一次单向散列运算 $h(\cdot)$ 所需的时间,本方案在注册及登录认证阶段分别需要 $3T_h$ 和 $9T_h$ 的计算量,该计算量高于文献[2]的方案而低于其他对比方案。

3.2.3 比对分析

本节以文献[2]、文献[3]、文献[17]、文献[18]这4个支持生物特征验证的远程认证方案为参照,从生物特征安全性和识别性能、认证的安全性和计算性能等角度进行比对分析,相关比较如表3和表4所示。

文献[2]和文献[3]的方案都使用哈希函数对生物特征进行加密,虽然能保证生物特征数据的安全性,但是这种方法对生物特征的类内变化敏感,容易导致合法的用户不能通过生物特征认证。此外,这2类方法在认证安全性上也存在一些缺陷,容易受到网络攻击的影响。文献[17]的方案从生物特征提取密钥 B_i 并通过比较 $h(ID_i \| PW_i \| B_i)$ 完成生物特征和密码认证。该方案仅保存经过单向散列运算的密钥 B_i ,可以保证生物特征数据的安全性。但如前面分析,现有

表3 三因素认证方案计算性能比较

比较项	文献[2]	文献[3]	文献[17]	文献[18]	本文方法
注册步骤	$3T_h$	$4T_h$	$7T_h$	$7T_h + 4T_m + 1T_{gen}$	$3T_h$
登录及认证步骤	$7T_h$	$10T_h$	$31T_h$	$41 + 8T_m$	$9T_h$
总计	$10T_h$	$14T_h$	$38T_h$	$48T_h + 12T_m + 1T_{gen}$	$12T_h$

表4 认证安全性比较

比较项	文献[2]	文献[3]	文献[17]	文献[18]	本文方法
生物特征安全性	高	高	中	高	高
生物特征认证性能	低	低	中	中	高
密码及生物特征模板更新	否	是	是	是	是
抵御密码猜测攻击	否	是	否	是	是
抵御伪装用户攻击	否	是	是	是	是
抵御伪装服务器攻击	否	是	是	是	是
抵御重放攻击	是	否	是	是	是
抵御中间人攻击	否	是	是	是	是

的生物特征密钥生成算法只能适用于特定的生物特征类型,在密钥生成中需要量化,这也会损失有效信息,降低认证准确性。此外,该方案在智能卡中同时保存了随机数 k_i 和 $j_i = (ID_i \parallel PW_i) \oplus k_i$,如果智能卡丢失,攻击者可以恢复出 $ID_i \parallel PW_i$,降低了密码猜测的难度。文献[18]的方案使用了Fuzzy commitment进行密钥生成,需要对生物特征进行二值化处理,会导致识别率降低。此外,方案涉及椭圆曲线密码运算,计算成本显著增加。综合比较计算量、认证安全性、生物特征隐私性和认证准确性,可以看出本文方案更好地兼顾各方面需求。

4 总结

本文针对生物特征模板保护中生物特征数据安全性和生物特征识别的准确性难以兼顾的问题,对模糊保险箱算法进行改进,使用密码对生物特征子向量进行投影,加入杂凑点保证生物特征的安全性。在进行生物特征认证时,首先基于查询特征子向量与保险箱 x 分量的比对以确定生物特征候选集,而后通过用户密码对应的曲线投影,从候选集中找出注册的生物特征子向量。该方案适用于多种数据类型的生物特征,可以根据识别算法选择合适的比对距离,对生物特征识别算法准确性的影响非常小。基于改进的生物特征模糊保险箱,本文进一步提出一个三因素远程身份认证方案。分析表明,该方案可以有效抵御远程认证中的各类攻击,保证认证过程的有效性和安全性。与其他基于生物特征的远程认证方案相比,本方案可以更好地兼顾远程认证的安全性、隐私性、准确性和计算效率等多方面需求。

参考文献:

- [1] Ometov A, Bezzateev S, Makitalo N, et al. Multi-factor authentication: A survey[J]. Cryptography, 2018, 2(1). (2018-01-05)[2026-02-14]. <https://doi.org/10.3390/cryptography2010001>.
- [2] Li C T, Hwang M S. An efficient biometrics-based remote user authentication scheme using smart cards[J]. Journal of Network and Computer Applications, 2010, 33(1): 1-5.
- [3] Khan M K, Kumari S. An improved biometrics-based remote user authentication scheme with user anonymity[J]. BioMed Research International, 2013: Article ID 491289.
- [4] Menaria L, Jain K. A survey on biometric template protection[J]. International Journal of Scientific Research in Computer Science, 2017, 2(2): 995-999.
- [5] 王会勇,唐士杰,丁勇,等.生物特征识别模板保护综述[J].计算机研究与发展,2020,57(5):1003-1021.
- [6] Lumini A, Nanni L. An improved biohashing for human authentication[J]. Pattern Recognition, 2007, 40(3): 1057-1065.
- [7] Ratha N K, Chikkerur S, Connell J H, et al. Generating cancelable fingerprint templates[J]. IEEE Trans on Pattern Analysis and Machine Intelligence, 2007, 29(4): 561-572.
- [8] Chee K Y, Jin Z, Cai D W, et al. Cancellable speech template via random binary orthogonal matrices projection hashing[J]. Pattern Recognition, 2018, 76: 273-287.
- [9] Yunpeng Li, Wei Wu, Yuan Zhang, et al. Palm vein template protection scheme for resisting similarity attack[J]. Computers & Security, 2025, 150: 104227.
- [10] Dodis Y, Reyzin L, Smith A. Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data[C]// Proc of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 523-540.
- [11] Juels A, Wattenberg M. A fuzzy commitment scheme[C]// Proc of the 6th ACM Conference on Computer and Communications Security. New York: ACM, 1999: 28-36.
- [12] Hao Feng, Anderson R, Daugman J. Combining crypto with biometrics effectively[J]. IEEE Trans on Computers, 2008, 55(9): 1081-1088.
- [13] Juels A, Sudan M. A fuzzy vault scheme[J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257.
- [14] You Lin, Wang Ting. A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion[J]. Soft Computing, 2019, 23: 3843-3851.
- [15] Wu Lifang, Xiao Peng, Yuan Songlong, et al. A Fuzzy Vault Scheme for Ordered Biometrics. Journal of Communications, 2011, 6(9): 682-690.
- [16] Chung Y, Moon D, Lee S, et al. Automatic alignment of fingerprint features for fuzzy fingerprint vault[C]// Proc of the 2006 International Conference on Information Security and Cryptology. Berlin: Springer, 2005: 358-369.
- [17] 徐钦桂,黄培灿,杨桃栏.增强的基于生物特征密钥智能卡远程身份认证方案[J].计算机研究与发展,2015,52(11):2645-2655.
- [18] Huang W. ECC-based three-factor authentication and key agreement scheme for wireless sensor networks[J]. Scientific Reports, 2024, 14(1).

作者简介:

贵圣兰,高级工程师,博士,主要从事智能制造及信息安全相关工作;刁力力,正高级工程师,博士,主要从事信息安全及数据挖掘相关算法研究工作。

