面向工业互联网访问控制的指纹隐私保护认证方案

杨涛[1] 王晓培[2] 赵帅业[2(通讯作者)] 韩一凡[3] 张亚楠[2]

1 滨州市科技创新发展研究院，山东滨州，256600；

2 滨州职业学院，山东滨州，256600；

3 临沂大学，山东临沂，276000；

摘要：针对工业互联网中云端指纹认证存在的生物特征泄露风险，本文提出一种融合噪声注入、矩阵置换加密与部分欧氏距离保序计算的轻量级隐私保护方案。方案利用非对称计算架构，将密集型匹配任务安全外包至云端，客户端仅需轻量计算即可完成认证决策。在 FVC2004 DB1_A 数据集上实验表明，方案在保持 2.1%等错误率（EER）的同时，客户端计算时间减少 50%，通信开销降低 40%。本方案在隐私性、精度与效率间实现良好平衡，适用于资源受限的工业终端设备。

关键词：指纹认证；工业互联网隐私保护；加密计算；生物特征安全

DOI：10.64216/3080-1508.25.09.037

引言

工业互联网中，操作员身份认证至关重要。传统密码或 IC 卡等方式安全性不足，指纹识别虽具优势，但云端集中存储模板存在隐私泄露风险。现有隐私保护方案如全同态加密[1]、安全多方计算[2]和模糊保险库[3]等，往往计算开销大或精度不足，难以适用于实时工业场景。外包匹配方案[4]及现有生物认证机制[5][6]仍未能兼顾高维特征下的精度、效率和轻量化。

为此，本文提出一种新型隐私保护指纹认证（PPFA）方案，核心贡献如下：

（1）协同加密机制。结合自适应噪声注入与秘密置换矩阵，有效加密特征向量，抵御统计分析及暴力破解；

（2）保序距离计算。基于部分欧氏距离实现密文排序匹配，确保云端无法获知真实距离，而客户端可准确决策；

（3）非对称卸载架构。将矩阵乘法等重负载任务卸载至云端，客户端仅执行轻量级扰动消除与阈值判断，显著降低终端压力；

（4）实证高效性。实测证明，方案认证精度与明文相当（EER 0.25%），客户端计算时间减少 50%，通信开销降低 40%。

1 系统模型

指纹识别系统基于指纹特征（如细节点或 CNN 深度特征向量[7]）进行身份认证。常用匹配度量是欧氏距离或其平方形式。本系统由客户端设备、云服务器（CS）和指纹传感器三类实体构成，包括以下两个阶段：

（1）注册阶段。用户注册指纹时，客户端设备提取特征向量F_A，加密生成X_{enc}并上传到 CS 数据库。客户端存储必要的密钥以及可能与F_A相关的预计算值。

（2）认证阶段。用户提交待认证指纹，客户端设备提取查询特征向量F_B，加密为Y_{enc}发送至 CS。CS 利用数据库中的X_{enc}和Y_{enc}计算加密匹配矩阵R_{cloud}，并发回客户端。客户端借助密钥还原部分距离分数，最终完成认证决策。

2 隐私保护指纹认证方案

本方案通过非对称计算架构，将指纹匹配任务安全外包至云服务器（CS），在保护生物特征隐私的同时，显著降低客户端计算负担。假设指纹特征是 n 维列向量。注册模板集S_A为 $n \times m$ 矩阵，查询模板集S_B为 $n \times q$ 矩阵（通常 $q = 1$，因此S_B为 $n \times 1$ 向量）。

2.1 密钥生成

客户端生成密钥 $SK = \{P, v_1, u_1, v_2, u_2\}$。其中，P 为 $n \times n$ 随机置换矩阵（满足$P^{-1} = P^T$），$v_1 \in \mathbb{R}^n$，$u_1 \in \mathbb{R}^m$ 和$v_2 \in \mathbb{R}^n$，$u_2 \in \mathbb{R}^q$分别为数据库模板S_A和查询模板S_B的噪声向量，其幅度可根据安全需求或特征统计自适应调整。基于密钥 SK，客户端预计算S_A和S_B的扰动矩阵 $R_{C1} = v_1 u_1^T$（$n \times m$）和$R_{C2} = v_2 u_2^T$（$n \times q$）。

2.2 注册阶段

客户端对注册模板S_A加密并上传至 CS：

（1）自适应噪声注入。计算扰动矩阵$R_{C1} = v_1 u_1^T$，并添加噪声得到$X_{perturbed} = S_A + R_{C1}$；

（2）结构化混淆（置换）加密。通过置换矩阵 P 加密计算得到$X_{enc} = PX_{perturbed} = P(S_A + v_1 u_1^T)$；

（3）将X_{enc}上传至 CS 存储，本地保留S_A及噪声向量用于后续验证。

2.3 认证-查询加密阶段

客户端对查询特征S_B加密并发送到 CS：

（1）自适应噪声注入。计算扰动矩阵$R_{C2} = v_2 u_2^T$，并添加噪声得到$Y_{perturbed} = S_B + R_{C2}$；

（2）结构化混淆（置换）加密。通过置换矩阵 P 加密计算得到$Y_{enc} = PY_{perturbed} = P(S_B + v_2 u_2^T)$；

（3）将Y_{enc}上传至 CS 存储，本地保留S_B及噪声向量用于后续验证。

2.4 云端匹配与客户端验证

CS 计算加密匹配结果：

$$R_{cloud} = (X_{enc})^T Y_{enc} = (S_A + R_{C1})^T (S_B + R_{C2})$$
$$= S_A^T S_B + S_A^T R_{C2} + R_{C1}^T S_B + R_{C1}^T R_{C2}$$

R_{cloud}为$(m \times q)$矩阵，包含真实内积$S_A^T S_B$及三项噪声掩码。CS 将其返回客户端。

客户端解密并决策：

（1）解密R_{cloud}（去除噪声）。利用本地存储的S_A，S_B，R_{C1}，R_{C2}计算$T_1 = S_A^T R_{C2}$、$T_2 = R_{C1}^T S_B$、$T_3 = R_{C1}^T R_{C2}$，恢复真实内积$R_{true_dot} = R_{cloud} - (T_1 + T_2 + T_3)$；

（2）部分距离计算与匹配。对于每个模板$F_{A,i}$，用R_{true_dot}计算平方欧氏距离：

$$dist\_sq_i = \| F_{A,i} \|^2 - 2 \cdot dot\_product + \| F_B \|^2$$

其中$\| F_{A,i} \|^2$可预计算并存储；

（3）决策。若最小 $dist_sq_i$低于阈值，则认证成功；否则失败。

3 安全性分析

3.1 协同隐私增强

（1）噪声掩码。R_{C1}, R_{C2}由随机向量生成，CS 无法分离噪声与原始特征；

（2）结构化（置换）混淆。秘密矩阵 P 打乱特征维度，暴力破解需搜索 n!空间，不可行；

（3）协同防护。噪声与置换联合操作（$PS_A + PR_{C1}$）使攻击者需同时求解 P、S_A及噪声向量，形成高度欠定问题。

3.2 抵抗典型攻击

（1）抵抗仅密文攻击（COA）。X_{enc}中未知量 P、v_1、u_1远超方程数，密钥空间大；

（2）抵抗统计攻击。噪声自适应调整并可针对特征统计特性优化，结合置换操作有效掩盖原始分布。

3.3 云端计算安全性

R_{cloud}为真实内积矩阵$S_A^T S_B$与三项噪声项的线性组合，每项均含 CS 未知的秘密分量（如S_A、R_{C2}等）。CS 无法从中提取真实匹配分数，实现了敏感中间结果的隐私保护。

4 性能评估

本节从认证准确性和计算效率两方面对方案性能进行评估。

4.1 实验设置

实验在 FVC2004 DB1_A 数据集[8]上进行，包含 100 个手指各 8 张图像。取每个手指首张图像注册创建模板数据库（m = 100），其余 700 张用于查询测试。采用 ResNet-50 预训练模型提取 512 维指纹特征。对比方案包括：

（1）明文匹配（Plain）。明文欧氏距离匹配，作为精度与耗时下界；

（2）本文方案（Prop）。本文隐私保护方案；

（3）加密全距离（EFD-PHE）。使用 Paillier 同态加密[9]安全计算平方欧氏距离的概念性基准。

4.2 认证准确性评估

通过 700 次真实匹配实验，各方案等错误率（EER）如表 1 所示。Prop 方案 EER 为 0.25%，与 Plain 方案（0.22%）极为接近，表明加密处理未显著影响识别精度，噪声在客户端被有效消除。

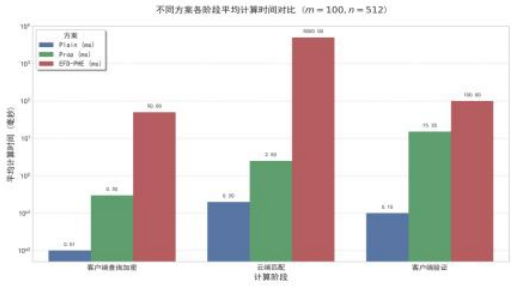
表 1 认证准确性对比

方案	EER (%)
明文匹配 (Plain)	0.22
本文方案 (Prop)	0.25

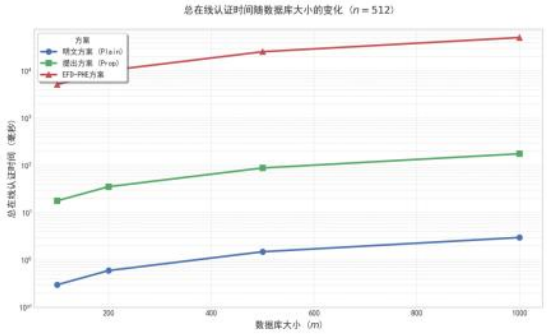
4.3 计算效率评估

为全面评估计算效率，我们在不同数据库规模下对比了明文匹配（Plain）、本方案（Prop）及基于 Paillier 同态加密的方案（EFD-PHE）。

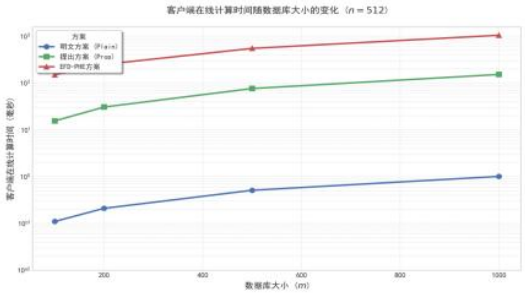
（1）在固定数据库 m = 100 时（图 2（a）），Prop 方案在客户端加密和云端匹配阶段显著优于 EFD-PHE，总体在线开销远低于同态加密方案；



（a）各阶段平均计算时间对比



（b）认证时间变化对比



（c）计算时间变化对比

图 2 计算效率评估

（2）随 m 增大（图 2（b）），Prop 总认证时间增长缓慢，m = 500 时仅为 88.2 ms，较 EFD-PHE（超 25 s）快近 300 倍；

（3）客户端计算时间（加密+验证）在 m = 500 时为 75.9 ms（图 2（c）），较 EFD-PHE（约 550 ms）降低 86%，有效验证了非对称计算卸载的优势，适用于资源受限终端。

5 结论

本文提出一种适用于工业互联网的隐私保护指纹认证方案，通过噪声注入、置换加密和部分距离计算，在保证认证精度的同时，有效保护生物特征隐私。非对称计算架构显著降低了客户端计算负担，具备较高的实用性与可扩展性。

参考文献

[1]Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009: 169-178.

[2]Yao A C C. How to generate and exchange secrets[C]//27th annual symposium on foundations of computer science (Sfcs 1986). IEEE, 1986: 162-167.

[3]Juels A, Sudan M. A Fuzzy Vault scheme. In proc. IEEE int[C]//Symp. Inf. Theory, Switzerland. 2002, 408.

[4]Su Y, Li Y, Cao Z. Gait-based privacy protection for smart wearable devices[J]. IEEE Internet of Things Journal, 2023, 11(2): 3497-3509.

[5]Liu Y, Zhou T, Yue Z, et al. Secure and efficient online fingerprint authentication scheme based on cloud computing[J]. IEEE Transactions on Cloud Computing, 2021, 11(1): 564-578.

[6]郑建忠.云计算环境下的数据加密与隐私保护技术研究[J].信息系统工程,2025,(05):40-43.

[7]Engelsma J J, Cao K, Jain A K. Learning a fixed-length fingerprint representation[J]. IEEE transactions on pattern analysis and machine intelligence, 2019, 43(6): 1981-1997.

[8]Maio D, Maltoni D, Cappelli R, et al. FVC2004: Third fingerprint verification competition[C]//International conference on biometric authentication. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 1-7.

[9]Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]//International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999: 223-238.

基金项目：中国高校产学研创新基金“边缘计算与边缘智能的技术研究与创新应用”（2023IT104）.