基于SM4算法的隐私保护轻量化人脸认证方案

张旭诚[1]，熊玲[2]，刘志才[1]
（1. 西华大学计算机与软件工程学院，四川 成都 610039；2. 北京语言大学信息科学学院，北京 100083）

摘　要：为解决大数据时代下人脸识别技术中的隐私保护问题，基于SM4算法提出一种具有隐私保护的轻量化人脸认证方案。利用FaceNet模型提取人脸特征向量，并用SM4算法对其加密，提升图像加密效率。通过局部感知哈希函数快速匹配人脸特征的密文值。在此基础上，设计一个新的轻量化人脸认证协议。安全性分析表明，该协议可提供防重放攻击、数据泄露和用户身份的匿名认证。实验结果表明，与同态加密相比，该方案在计算和通信效率上有显著提升。

关键词：人脸识别；感知哈希函数；隐私保护；对称加密
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025233

Lightweight facial authentication scheme based on the SM4 algorithm for privacy protection

ZHANG Xucheng[1], XIONG Ling[2], LIU Zhicai[1]
1. School of Computer and Software Engineering, Xihua University, Chengdu 610039, China
2. School of Information Science, Beijing Language and Culture University, Beijing 100083, China

Abstract: In order to address the issue of data privacy protection in facial recognition technology in the era of big data, a lightweight facial authentication scheme based on the SM4 algorithm for privacy protection was proposed. It utilized the FaceNet model to extract facial feature vectors and encrypted them using the SM4 algorithm, enhancing image encryption efficiency. The p-stable LSH function was employed to quickly match the ciphertext values of facial features. Based on this, a new lightweight facial authentication protocol was designed. The security analysis indicats that the protocol can provide protection against replay attacks, data leakage, and anonymous authentication of user identities. Experimental results show that the scheme achieves a significant improvement in computational and communication efficiency compared to homomorphic encryption.

Keywords: facial recognition, perceptual hash function, privacy protection, symmetric encryption

0　引言

在信息技术迅猛发展的今天，人脸识别技术因其便捷性和准确性，在生物特征认证、视频监控、智能安防、移动支付等多个领域得到了广泛应用。人脸识别技术的核心在于，通过分析个人面部特征实现个体的快速识别与验证。然而，随着大数据技术的不断发展，个人隐私泄露和数据安全问题日益成为公众关注的焦点。尤其是在人脸识别领域，个人面部信息的敏感性和独特性使隐私保护问题尤其突出。

传统的生物认证技术在提取用户隐私数据以及对隐私数据进行处理的过程中均以明文形式进行，这显然不能满足当下对用户隐私性的保护要求[1]。此外，随着人工智能技术的发展，深度学习特别是卷积神经网络（CNN, convolutional neural network）在图像识别领域取得了革命性的进

收稿日期：2025–08–31；修回日期：2025–10–15
通信作者：熊玲，lingdonghua qq@163.com

展，这为人脸识别技术的发展提供了新的机遇。然而，如何在利用这些先进技术提高识别效率和准确性的同时确保个人隐私不被侵犯，成为一个亟待解决的问题。

针对上述问题，本文提出了一种基于SM4算法的隐私保护轻量化人脸认证方法。SM4算法是中国国家密码管理局发布的商用分组密码算法[2]，具有高安全性和高效率的特点。通过将SM4算法应用于人脸认证过程中，本文方法旨在实现对人脸数据的加密处理，确保数据在传输和存储过程中的安全性。同时，结合感知哈希函数和深度学习模型FaceNet，本文方法能够在保护用户隐私的同时，实现高效的人脸识别和认证。

本文贡献如下。

1) 本文使用安全加密算法SM4对数据进行加密处理，确保数据在传输过程中得到保护，不被篡改或泄露，从而维护数据的完整性和隐私性。在认证阶段，通过感知哈希函数匹配加密数据，确保人脸数据和相似度未被篡改和泄露，从而保证数据在处理过程中的完整性。

2) 本文介绍了一种近似的高维相似性搜索方案，该方案对数据大小具有可证明的亚线性依赖性。它没有使用树状空间分区，而是依赖于一种被称为敏感散列的新方法。关键思想是使用多个散列函数对查询点进行散列，以确保每个函数中彼此靠近的对象的碰撞概率比相距遥远的对象高得多。然后，通过对查询点进行哈希运算并检索存储在包含该点的桶中的元素来确定近邻。

3) 用户匿名指用户将自己的人脸特征信息加密上传后，数据库服务器不能够窃取用户的人脸特征明文信息。

4) 在加密通信中，时间戳可以用来防止重放攻击，即攻击者拦截并重新发送之前的通信内容。通过检查时间戳，系统可以拒绝过期的请求。

5) 通过设置使用期限，即使密钥被未授权的人员获取，也只有在有限的时间窗口才可以使用这个密钥。这增加了系统的安全性，因为它限制了未授权访问可能造成的损害。

1 相关工作

1.1 SM4算法

SM4是一种使用Feistel结构的对称密钥分组密码算法[3]，其分组长度和密钥长度均为128 bit。其中加密算法、解密算法以及密钥扩张算法都采用了32轮非线性迭代结构[4]，并且每一轮都需要有一个轮密钥参与运算，这与高级加密标准（AES）和数据加密标准（DES）算法类似。SM4算法的加密和解密算法都采用相同的结构，但在轮密钥的使用顺序上有所区别。加密时按照顺序使用轮密钥，而解密时需要按照相反的顺序使用轮密钥。

SM4会对一段明文进行分组加密，对一个分组进行加密，输出一个分组的密文。分组长度为128 bit，把一组128 bit的明文分成4个部分，每部分为1字，1字等于32 bit。由此，一组128 bit的明文变成了4字明文。加密的流程分为两个部分，分别是32轮迭代与1次反序变换。其中32轮迭代需要用到轮函数F和32个1字的轮密钥。由于非线性变换的混淆效应，SM4密码的安全性大大提高[5]。轮函数表示为：$\boldsymbol{X}$代表明文中的一个字，rk代表轮密钥。

1.2 感知哈希函数

p-stable LSH函数[6-8]：一类特殊的哈希函数，它们在保持数据局部性的同时，能够将数据点高效地映射到哈希码空间。在机器学习和数据挖掘中，LSH是一种重要的技术，用于大规模数据集中的近似最近邻搜索。p-stable LSH是基于p稳定分布的LSH函数，其中p稳定分布是一种概率分布，其线性组合也服从同样的分布。最常见的p稳定分布是高斯分布（p=2），也就是正态分布。p-stable LSH函数通常用于处理欧几里得空间中的数据，具体实现通常涉及随机投影，其中数据点通过随机生成的向量进行投影，并使用投影结果来确定哈希码。

LSH背后的基本思想是对数据和查询点进行哈希处理，使距离较近的点之间发生碰撞的概率远远高于距离较远的点之间发生碰撞的概率，即两点之间的距离越小，碰撞的概率越高。如果任意两点$q,p \in S$和$h(q),h(p) \in U$满足式(1)和式(2)所示条件，则称哈希函数族$H=(h:S \to U)$为(r_1,r_2,p_1,p_2)敏感函数。

$$d(q,p) \leqslant r_1 \text{ then } \Pr_H\left[h(q)=h(p)\right] \geqslant p_1 \tag{1}$$

$$d(q,p) \geqslant r_2 \text{ then } \Pr_H\left[h(q)=h(p)\right] \leqslant p_2 \tag{2}$$

其中，S为点q和p的定义域，d为定义域内定义的

距离度量，U为映射后的集合，Pr[ ]为概率函数。为了使位置敏感族有用，必须满足不等式$p_1 > p_2$和$r_1 < r_2$。

在原始的LSH方法中，计算之前需要将原始空间嵌入汉明（Hamming）空间中。然而，基于p-stable LSH的算法不需要嵌入，可以直接在欧几里得空间或曼哈顿空间进行LSH计算。

假设$\boldsymbol{a}$为d维向量，由服从p稳定分布的随机函数生成，首先，将特征向量$\boldsymbol{v}$投影到向量$\boldsymbol{a}$上，并将b的修正偏差值加到投影结果中；然后，以w为区间进行量化；最后，使用散列函数将彼此接近的点映射到相似的区间。基于p-stable LSH函数族H中的每个哈希函数可表示为$f_{a,b}(v)=\left\lfloor \dfrac{\boldsymbol{a}\cdot\boldsymbol{v}+b}{w} \right\rfloor$，其中，$\lfloor\cdot\rfloor$为舍入函数，$b$为从$\lfloor 0,w \rfloor$中均匀选取的实数，$w$的最优值在不同的数据集上可能会有所不同。哈希族中的函数根据向量$\boldsymbol{a}$和b之间的差异进行索引。

1.3　FaceNet人脸识别模型

FaceNet[9-11]是一种基于谷歌开发的深度卷积神经网络（DCNN, deep convolutional neural network）的架构模型，旨在将面部检测和面部识别集成到一个框架中。FaceNet使用欧几里得空间直接训练面部，其中距离由面部模型之间的相似性组成。当获得人脸模型之间相似性的结果时，使用附着在FaceNet上的特征向量进行人脸识别和分类将变得容易。

在训练过程中，FaceNet通过使用在线新颖的三元组挖掘方法进行面对面匹配来应用三元组。这个三元组由一组锚点图像组成，其中每个图像由正图像和负图像组成。深度架构是DCNN，然后是L2归一化，这是人脸嵌入的结果。

FaceNet在训练过程中也受到三重丢失的影响，三重损失训练方法有3个主要要素，即锚定、积极和消极。这种三重损失通过正向最小化锚之间的距离和负向最大化锚之间的距离来起作用。其中，积极因素与锚具有相同的身份，消极因素与锚的身份不同。

FaceNet通过应用基于LMNN的三重损失方法将其输出直接训练为简洁的128维嵌入[12]。它由两个比较面部的缩略图和不匹配的缩略图组成，损失旨在使用一个范围的限制来区分正对和负对。缩略图在面部区域被紧紧地剪切，除了实现比例和平移外，不需要进行2D或3D调整。

2　方案设计

本文构建了一种基于SM4算法的隐私保护轻量化人脸认证方法，避免数据在传输过程中被篡改或泄露，从而保护了用户的隐私信息。方案分为初始化、用户注册和认证3个部分。在初始化阶段中，服务器选择FaceNet模型和p-stable LSH函数，客户端生成长期私钥MK，融合时间戳、使用期限等信息存储，设定人脸识别阈值。在用户注册阶段中，用户上传人脸图像至客户端，客户端经FaceNet模型提取特征向量，通过p-stable LSH函数计算哈希值，SM4算法加密特征向量，将加密向量与哈希值发至给服务器。在认证阶段中，用户上传人脸图像后，客户端提取特征向量并计算哈希值发送至服务器；服务器根据哈希值匹配对应的密文并反馈至客户端，客户端使用密钥解密密文后，完成人脸特征的相似度计算。本文使用安全加密算法SM4对数据进行加密处理，确保数据在传输过程中得到保护，不被篡改或泄露，从而维护数据的完整性和隐私性。

2.1　初始化过程

在初始化阶段，客户端生成长期私钥MK与时间戳、使用期限等信息的合并$K = H(\mathrm{MK}||T||\mathrm{PT})$，其中，$T$为当前时间戳，PT为使用期限，设定人脸识别阈值。

2.2　注册过程

图1为基于SM4加密的人脸识别隐私保护方法的注册过程，具体步骤如下。

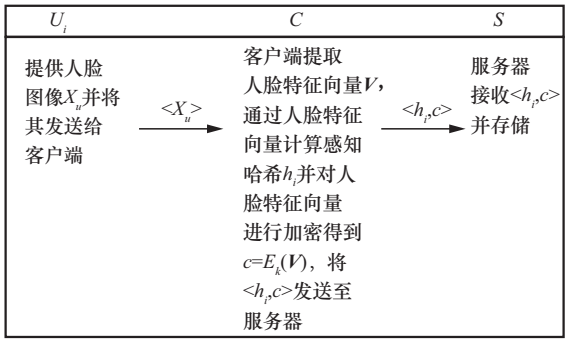


图1　基于SM4加密的人脸识别隐私保护方法的注册过程

1) 用户U_i通过一个专用通道，即客户端的摄像设备，将自己的面部图像和注册请求发送给客户

端。客户端从U_i接收到人脸图像X_u后，通过训练的FaceNet模型提取人脸特征向量$\boldsymbol{V}$；使用p-stable SLH函数计算得到感知哈希值h_i=PHash($\boldsymbol{V}$)；加密人脸特征向量得到$c=E_k(\boldsymbol{V})$，最后将h_i和c发送给服务器。

2) 服务器接收到（h_i,c）后，服务器存储（h_i,c）。

2.3　认证过程

图2为基于SM4加密的人脸识别隐私保护方法的整体流程。

1) 用户向客户端发起认证请求，客户端收到并响应请求；客户端通过摄像设备采集用户U_i的人脸图像X_u，载入预训练的FaceNet模型，通过FaceNet对X_u提取人脸特征向量$\boldsymbol{V}'$，通过p-stable LSH函数得到h_i=PHash($\boldsymbol{V}'$)，并将h_i发送至服务器。

2) 服务器收到h_i后，快速匹配到人脸特征向量密文c，并将密文c发送给客户端。

3) 客户端从服务器接收到密文c，对密文c进行解密，得到$X=D_k(V)$，通过欧氏距离公式$d(V,V')=\sqrt{\sum_{i=1}^{D}(v-v')^2}$，计算得到相似度值。判断该值是否在规定阈值内，如果不在规定阈值内，则用户U_i认证失败；反之，则用户U_i认证通过。

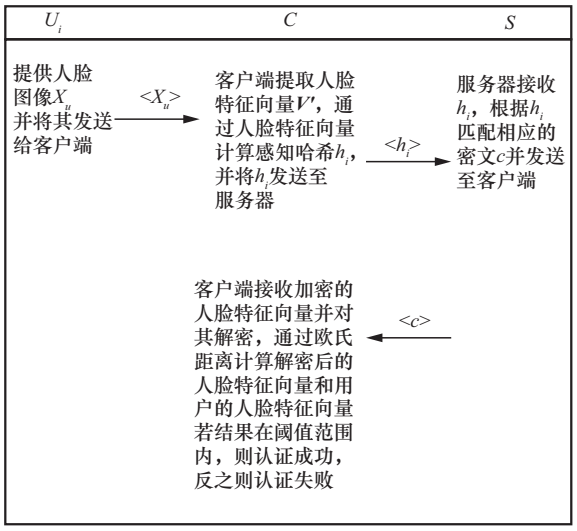


图2　基于SM4加密的人脸识别隐私保护方法的整体流程

3　实验

本节首先介绍了本次实验中使用的数据集，然后分析了FaceNet的识别性能，给出了该方案的密文平均计算时间以及明文和密文条件下识别准确率，最后将SM4加密算法的人脸识别在不同阈值下的识别准确率与其他方法进行了比较。

3.1　数据集

本文使用的数据集是LFW。该数据集包含来自互联网的13 233张人脸图像，涉及5 749个不同的人物。图像在自然环境下采集姿态、表情、光照等变化。

3.2　实验结果及分析

3.2.1　密文平均计算时间

在LFW中随机挑选一张人脸图像进行FaceNet人脸识别，测量得到明文状态下进行一次FaceNet人脸识别的平均时间约为0.286 ms。然后在密文状态下进行FaceNet人脸识别并计算其平均识别时间。采用对比方法，李雅硕等[13]使用CKKS加密[14-16]算法对开源人脸数据集中的人脸信息[17-18]进行加密，并使用FaceNet模型进行人脸识别计算。表1为本文SM4加密算法与李雅硕等使用CKKS加密算法进行密文人脸识别的平均计算时间对比。

表1　密文人脸识别的平均计算时间

加密方法	时间/ms
CKKS	3.982
SM4	2.793

从表1可以看出，使用SM4加密算法进行FaceNet人脸识别的密文平均计算时间约为2.793 ms，效率远高于李雅硕等[13]使用的CKKS加密算法。

3.2.2　识别准确率

为了验证SM4加密算法在人脸识别中的准确率，本节将实验分为4组，每组分别在数据集中随机选择500、1 000、2 000、5 000张人脸图像。每组实验中，对所有选取出来的人脸图像使用FaceNet模型进行特征提取，将提取出的特征向量进行SM4加密，然后进行认证，输出认证准确率，即算法能够识别且正确匹配用户信息的数量与进行人脸识别的总次数之比。本文对提取出的4组人脸信息特征向量分别用明文和密文形式进行完整的FaceNet人脸识别，计算时间和识别准确率如表2所示。

表2　明文和密文的计算时间和识别准确率

人脸图像数量/张	形式	时间/ms	准确率
500	明文	205.45	98.8%
	密文	1 989.56	98.6%
1 000	明文	396.24	98.7%
	密文	4 085.92	98.4%
2 000	明文	832.17	98.5%
	密文	8 273.96	98.2%
5 000	明文	1 985.63	98.3%
	密文	20 372.86	97.6%

3.2.3　实验对比

为了有一个直观的认识，现将本文方案与李雅硕等[13]基于FaceNet算法结合CKKS加密算法提出的人脸识别加密方案和FDAE轻量级隐私保护框架[19]进行对比，3种方案同样在LFW数据集下进行训练，在不同阈值下的识别准确率如图3所示。本文方案识别准确率最高大约为98.8%，CKKS方案识别准确率最高大约为94.7%，FDAE方案识别准确率最高大约为96.1%，这表明本文方案在识别准确率上有更大的优势。

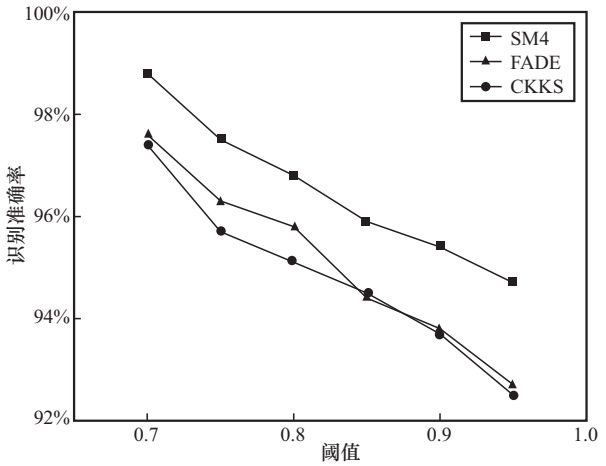


图3　在不同阈值下的识别准确率

4　协议证明

4.1　初始假设

客户端和服务器都相信 SM4 算法的安全性，即$C|\equiv$SM4安全，$S|\equiv$SM4安全。

客户端相信自己生成的长期私钥MK、时间戳T和使用期限PT的保密性，即$C|\equiv(\mathrm{MK},T,\mathrm{PT})$。

服务器相信数据库中存储的感知哈希值和密文的完整性，即$S|\equiv$完整感知哈希值密文。

4.2　注册过程证明

客户端将人脸特征$\boldsymbol{V}$用SM4算法加密为$c=E_k(\boldsymbol{V})$，并计算哈希值。此时，客户端发送消息$<h_i,c>$给服务器。根据BAN逻辑的接收规则，服务器收到消息后，有$S\lessdot\!\lessdot h_i,c>$。

由于客户端和服务器都相信SM4算法的安全性，根据加密消息的推理规则，若$S\lhd c$且$S|\equiv$SM4安全，则$S|\equiv C|\sim V$，即服务器相信客户端发送过原始的人脸特征向量。

4.3　认证过程证明

客户端采集人脸图像提取特征向量$\boldsymbol{V}'$，加密为$c=E_k(\boldsymbol{V}')$并计算哈希值h_i，发送消息$<h_i,c>$和身份验证请求给服务器。服务器收到消息后，有$S\lessdot\!\lessdot h_i,c>$。

服务器遍历数据库匹配感知哈希值和对应的密文，将密文发送至客户端并对其解密，解密后的人脸特征向量与客户端的人脸特征向量进行欧氏距离计算。若得到的结果在规定阈值内，则认证通过。

对于抵抗重放攻击，假设攻击者重放之前的认证消息，由于消息中包含时间戳T，服务器在收到消息后，根据时间戳验证规则，若消息中的时间戳T不在有效范围内，则$S|\equiv$无效$<h_i,c>$，拒绝该请求，证明了方案对重放攻击的抵抗性。

5　安全性分析

在大数据时代，越来越多的企业选择将数据外包，以获得企业不具备的计算能力。本文提出的基于SM4加密的人脸识别隐私保护方法可以较好地满足人脸特征数据的私密性要求。该方法具备以下基本安全特性。

5.1　不可逆性

使用SM4对称加密算法对人脸特征数据进行加密，确保数据在传输和存储过程中不被篡改或泄露。SM4是一种分组密码算法，具有较高的安全性，能够有效保护数据的机密性和完整性。

5.2　用户匿名性

用户的人脸特征信息在上传时经过加密处理，服务器无法获取用户的明文人脸特征信息。即使在认证阶段，服务器中存放的也是加密人脸特征向

量，不会泄露人脸特征，进一步保护了用户的隐私。

5.3 抵抗多种攻击

客户端生成的长期私钥MK与时间戳T和使用期限PT合并，生成密钥K。时间戳的使用可以有效防止重放攻击，即攻击者无法通过拦截并重新发送之前的通信内容来绕过系统。系统会检查时间戳，拒绝过期的请求，这增强了系统的安全性。

5.4 增强密钥安全性

为了防止密钥被长时间使用而增加泄露的风险，系统通过设置使用期限来实现密钥轮换策略。即使密钥被未授权人员获取，但也只能在有限的时间窗口内使用，减少了密钥泄露带来的潜在损害。

5.5 不可链接性与高效检索

使用p-stable LSH函数对人脸特征向量计算感知哈希值，LSH函数能够在保持数据局部性的同时将数据点高效地映射到哈希码空间，确保在大规模数据集中的近似最近邻搜索效率。

在认证阶段，服务器通过感知哈希值快速匹配密文，减少了计算复杂度。

6 结束语

本文提出了一种基于SM4加密算法和感知哈希函数分类查询的人脸隐私保护方案，该方案可以对人脸特征加密并在加密情况下对人脸识别，解决隐私泄露的风险。所提方案使用户只需注册一次，就可以使用相同的身份来完成身份验证和人脸识别。安全分析表明，该方案可以实现相互认证、用户匿名、保密等功能。最后，将所提方案与之前的相关方案进行比较。比较结果表明，该方案不仅提供了有用的安全特性，而且具有较高的计算和通信效率。

本文提出的方案的局限性在于感知哈希碰撞会产生误差，这是一个非常有趣和具有挑战性的问题。在未来的工作中，笔者将重点研究如何有效地解决这个问题。

参考文献：

[1] 邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(5): 51-63.
XING H Q. Legal regulation of face recognition[J]. Journal of Comparative Law, 2020(5): 51-63.

[2] ZHOU Y K, WU N S, HU B D, et al. Implementation and performance of face recognition payment system securely encrypted by SM4 algorithm[J]. Information, 2022, 13(7): 316.

[3] DIFFIE W, LEDIN G. SMS4 encryption algorithm for wireless networks[J]. IACR Cryptology ePrint Archive, 2008(2008): 329.

[4] LI Y Q, WU X J, BAI G Q. Implementation of SM4 algorithm based on asynchronous dual-rail low-power design[C]//Proceedings of the 2018 14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT). Piscataway: IEEE Press, 2018: 1-3.

[5] ABED S, JAFFAL R, MOHD B J, et al. Performance evaluation of the SM4 cipher based on field-programmable gate array implementation[J]. IET Circuits, Devices & Systems, 2021, 15(2): 121-135.

[6] JAFARI O, MAURYA P, NAGARKAR P, et al. A survey on locality sensitive hashing algorithms and their applications[J]. arXiv Preprint, arXiv: 2102.08942, 2021.

[7] DATAR M, IMMORLICA N, INDYK P, et al. Locality-sensitive hashing scheme based on p-stable distributions[C]//Proceedings of the Twentieth Annual Symposium on Computational Geometry-SCG’04. New York: ACM Press, 2004: 253-262.

[8] BAI X, YANG H C, ZHOU J, et al. Data-dependent hashing based on p-stable distribution[J]. IEEE Transactions on Image Processing, 2014, 23 (12): 5033-5046.

[9] WU C M, ZHANG Y. MTCNN and FACENET based access control system for face detection and recognition[J]. Automatic Control and Computer Sciences, 2021, 55(1): 102-112.

[10] CAHYONO F, WIRAWAN W, FUAD RACHMADI R. Face recognition system using facenet algorithm for employee presence[C]//Proceedings of the 2020 4th International Conference on Vocational Education and Training (ICOVET). Piscataway: IEEE Press, 2020: 57-62.

[11] SRINIVAS S, SELVAN M P. E-CNN-FFE: an enhanced convolutional neural network for facial feature extraction and its comparative analysis with FaceNet, DeepID, and LBPH methods[C]//Data Management, Analytics and Innovation. Berlin: Springer, 2024: 339-354.

[12] WILLIAM I, SETIADI D R I M, RACHMAWANTO E H, et al. Face recognition using FaceNet (survey, performance test, and comparison) [C]//Proceedings of the 2019 Fourth International Conference on Informatics and Computing (ICIC). Piscataway: IEEE Press, 2019: 1-6.

[13] 李雅硕, 龙春, 魏金侠, 等. 基于同态加密的人脸识别隐私保护方法[J]. 信息安全研究, 2023, 9(9): 843-850.
LI Y S, LONG C, WEI J X, et al. Face recognition privacy protection method based on homomorphic encryption[J]. Journal of Information Security Research, 2023, 9(9): 843-850.

[14] YALAVARTHI B, KAUSHIK A R, ROSS A, et al. Enhancing privacy in face analytics using fully homomorphic encryption[C]//Proceedings of the 2024 IEEE 18th International Conference on Automatic Face and Gesture Recognition (FG). Piscataway: IEEE Press, 2024: 1-9.

[15] ZHAO S, ZHANG L F, XIONG P. PriFace: a privacy-preserving face recognition framework under untrusted server[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(3): 2967-2979.

[16] ZHANG S C, MA J F, ZHANG M X, et al. Privacy-preserving face recognition for access control systems[C]//Proceedings of the 2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS). Piscataway: IEEE Press, 2024: 348-356.

[17] NASER N M, NAIF J R. A systematic review of ultra-lightweight encryption algorithms[J]. International Journal of Nonlinear Analysis and Applications, 2022, 13(1): 3825-3851.

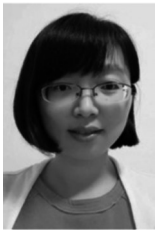
[18] SONG Z G, WANG G, YANG W Q, et al. Privacy-preserving method

for face recognition based on homomorphic encryption[J]. PLoS One, 2025, 20(2): e0314656.

[19] OSORIO-ROIG D, RATHGEB C, DROZDOWSKI P, et al. Stable hash generation for efficient privacy-preserving face identification[J]. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021, 4(3): 333-348.

[作者简介]

张旭诚（2000– ），男，四川乐山人，西华大学硕士生，主要研究方向为人脸识别。



熊玲（1983– ），女，安徽合肥人，博士，北京语言大学副教授、硕士生导师，主要研究方向为身份认证、访问控制、隐私计算、人工智能安全、区块链技术。

刘志才（1978– ），男，四川泸州人，博士，西华大学教授、硕士生导师，主要研究方向为膜计算、机器学习、模式识别、图像处理和计算机视觉。