一种基于深度学习和加密算法的安全人脸特征保护方法

冯勇，郭芷菡，刘紫雯，王显龙 *
蚌埠学院计算机与信息工程学院，安徽 蚌埠 233000
DOI: 10.61369/TACS.2025110039

摘　　要： 随着人脸识别技术的广泛应用，人脸数据的安全性和隐私保护成为研究的重点。本文提出了一种基于深度学习和加密算法的人脸特征保护方法。该方法首先对原始人脸图像进行可逆处理，利用 MTCNN 算法进行人脸检测和对齐。其次，通过深度学习模型提取人脸特征，生成高维特征向量。为确保数据的安全性和完整性，采用 SM2 非对称加密和 AES 对称加密算法对特征向量进行加密，并引入数字签名验证。
关 键 词： 人脸识别；深度学习；加密算法；SM2；AES；数字签名

A Secure Face Feature Protection Method Based on Deep Learning and Encryption Algorithms

Feng Yong, Guo Zhihan, Liu Ziwen, Wang Xianlong*
School of Computer and Information Engineering, Bengbu University, Bengbu, Anhui 233000

Abstract: With the widespread application of face recognition technology, the security and privacy protection of face data have become research focuses. This paper proposes a secure face feature protection method based on deep learning and encryption algorithms. Firstly, the method performs reversible processing on original face images, and uses the MTCNN algorithm for face detection and alignment. Secondly, it extracts face features through a deep learning model to generate high-dimensional feature vectors. To ensure data security and integrity, the SM2 asymmetric encryption and AES symmetric encryption algorithms are adopted to encrypt the feature vectors, and digital signature verification is introduced.
Keywords: face recognition; deep learning; encryption algorithms; SM2; AES; digital signature

引言

随着大数据技术的不断发展，每时每刻都会产生海量的数据，而对于这些数据的管理和保护变得尤为重要。在大数据技术的发展中，人脸识别技术更加成熟，这也使人们的生活更加便捷。但是随着时间的推进，数据隐私泄露愈加严重，一些不法分子通过窃取隐私数据来获利。基于这种现状，人们也在不断改进和研究新的人脸识别技术。目前深度学习已成为研究人脸识别领域的主流方向，经过多年的发展也逐渐成熟，其服务的身份认证功能被广泛应用与国家公共安全管理 [1]。因此可以利用深度学习模型进行人脸特征提取，这将更加有效。身份认证是通过一些技术来实现确认用户身份的过程，其经过多年的发展也逐渐成熟。身份认证是信息安全很重要的一部分，一般认为有以下几大特点 [2]：

（1）身份认证具有延迟性，其一般一系列加密算法来完成，这样会导致使用时出现延迟。

（2）身份认证在单机状态下几乎难以实现，所以使用者要在单机状态下进行一些超出安全范围的操作。

（3）用户的身份信息易遭窃取，入侵者或病毒可能会在用户的网络通信通道上进行窃取身份信息。

目前认为的身份认证分类一般有三种 [3]：

（1）用户所知认证：一般是将能够表明用户身份的一组信息告诉用户，类似与用户名和口令。通过检测用户数据库来匹配用户名和口令是一种较广泛的身份认证方法。

（2）用户所持标记认证：用户通过持有物品来进行身份认证，可以通过磁条卡、条码卡、光电卡等。

项目资助基金：蚌埠学院大学生创新创业训练计划项目（项目名称：“护你”——基于 MTCNN 和国密算法的图像加密人脸识别系统，项目编号：202311305050）。
作者简介：
第一作者：冯勇（2004—），男，安徽六安人，从事计算机应用技术研究。
通信作者：王显龙（1991—），男，安徽亳州人，硕士研究生，主要从事计算机视觉研究。

（3）用户生物特征性认证：通过利用人体所固有的生理特征或行为特征进行验证。如通过人脸、指纹、视网膜等进行验证。本文所介绍的方法就是基于用户生物特征性进行认证的。但是，随着生物特征识别技术的逐渐深入，安全性问题也逐渐显现。但对采集的生物特征用相同的方式进行特征提取生成特征信息时，这些特征信息在不同的系统数据库中时相似的，这就会产生一个问题，生物特征识别系统中存储的特征信息被未经授权的用户从数据库中盗取或破坏，数据的原主人将永远失去控制权，同时失去该身份信息[4]。

一、相关研究

近年来，国内相关领域的学者也对人脸识别技术进行了一定的探索和研究，为人脸识别技术领域作出了巨大的贡献。

随着科学技术的不断发展，人脸识别领域相关研究也愈加成熟。近些年，李丽平，徐营坤等人研究了一种基于 MTCNN 人脸检测方法，在 Windows 和 Android 平台的检测速度均提升了一倍，在工业界有重要的引用价值[5]。深度学习模型也更加频繁的被运用到人脸识别当中，郝林倩采用 CNN 算法，基于 python 深度学习库，构建 Mobilenetv1 网络模型，在此基础上通过 FaceNet 预测显示 Distance 值与事先设置的阀值对比情况，验证人脸图像，达到人脸识别的目的[6]。SM2 算法为我国基于椭圆曲线密码体系自主研制的一种非对称加密算法，陈有涛通过有限域上模运算基本算法为基础，通过硬件实现了 SM2 加密算法[7]。AES 是最常用的对称密码，它在硬件和软件上都具有高安全级别和高速实现，孙学刚提出的基于 AES 的统一图像加密系统在一定程度上解决了当下 AES 图像加密存在的一些问题[8]。加入数字签名验证可以确保数据的完整性和可靠性，陈楠通过解析数字签名与椭圆曲线离散对数问题，进一步研究了椭圆曲线无证书 SM2 数字签名方案相关算法以及正确性、安全性、效率[9-10]。

二、背景知识

（一）MTCNN 算法

深度学习在图像处理领域的应用越来越广，在人脸识别、目标检测等方面取得了显著的成果。MTCNN（Multi-Temporal Convolutional Network），与传统的卷积神经网络不同，MTCNN 利用两个 CNN 层来提取图像的特征信息，在处理一些复杂数据集时能够取得很好的效果。MTCNN 在人脸识别方面取得了巨大成功，已经成为目前人脸识别领域的研究热点。它在人脸检测、人脸表情和人脸属性识别等方面表现突出。

MTCNN 通过训练网络参数来用于人脸检测和对齐。它经由 P-Net、R-Net 和 O-Net 3个网络层次逐步精化的人脸检测。P-Net 首先通过多尺度滑动窗口快速遍历图像，产生大量可能包含人脸的初步候选区域，并判断其是否为人脸。接着，R-Net 对这些候选区域进行进一步筛选与调整，优化边界框位置，并初步估计面部关键点的大致方位。最后，O-Net 在前两阶段的基础上执行更精细的检测与校准，输出最终的人脸边界框以及精确的关键点坐标。MTCNN 能够在各种不同的情况下不受束缚地检测人脸和对人脸的对齐，和传统的算法相比，更有准确性。

MTCNN 算法，是一种基于像素的检测方法。它把一种多阶段的深度网络应用到了人脸检测上，形成了一种基于像素的检测方法。

（二）SM2 算法

SM2 是国家密码管理局发布的椭圆曲线公钥密码算法，属于非对称加密算法，非对称加密算法采用一对不同的密钥实现加解密操作，其中包含一个可公开的公钥和一个仅由持有者保密的私钥。这对密钥具有严格的对应关系：若使用公钥对信息进行加密，则必须通过对应的私钥才能解密；反过来，如果使用私钥加密，则需借助相应的公钥方可解密。因为具备这种独特的加解密特性，非对称加密算法不仅可实现数据的加密传输，还能对数据进行签名和验签。

1.SM2 加密算法

（1）用随机数发生器生成随机数 $k,0<k<n$ 。

其中 k 为随机数，用于生成加密算法中的临时私钥，n 为椭圆曲线的阶，表示椭圆曲线上的点的数量。

（2）计算椭圆曲线上的点 $C1=[k]G$

其中 G 为椭圆曲线上的基点，通常是一个事先固定的点。.C1：加密算法中计算得到的椭圆曲线上的点。.h：余因子，通常取值为 1。

（3）计算椭圆曲线点，若 S 为无穷远点则报错并退出，h 为余因子，这里取为 1。

（4）计算椭圆曲线上的点，利用公式 $[k]PB=(x2,y2)$ 。

将公钥 PB 与随机数 k 相乘，得到椭圆曲线上的另一点 (x2 y2)。其中 PB 为公钥点，用于加密和解密过程中的公钥。x2 y2 为椭圆曲线上的点的坐标。

使用 KDF 函数 $t=KDF(x2||y2,len)$ 计算。

将 (x2 y2) 作为输入，使用密钥派生函数 KDF 计算出 t。其中 t 为通过密钥派生函数计算得到的临时值，用于加密和解密过程中. KDF 为密钥派生函数用于生成临时值。若 t 全为 0 则返回 1。

（6）计算 $C2=M\oplus t$ ，将明文 M 与 t 进行异或操作，得到加密后的数据 C2。

其中 C2 为加密算法中计算得到的临时值，M 为要加密的消息。

（7）利用公式 $C=C1||C2||C3$ 将 C1 和 C2 拼在一起，得到最终的密文 C。

2.SM2 解密算法

（1）从密文中取出 C1，验证 C1 是否满足椭圆曲线方程若不满足则报错并退出。

（2）计算 $S=[h]C1$ ，将 C1 点乘以哈希函数 h 的值，确保 S

不是无穷点。其中 S 为解密算法中计算得到的临时值。若 S 为无穷远点则报错并退出。

（3）计算 [dB] C1=(x2 , y2) 。将私钥 d 与 C1 相乘，得到椭圆曲线上的另一点 (x2,y2)。其中 dB 为解密算法中的私钥。

（4）计算 t=KDF(x2||y2,len) 。将 (x2,y2) 作为输入，使用密钥派生函数 KDF 计算出 t。

（5）从 C 中取出 C2 计算 m=C2⊕t 。从密文中提取出 C2，将其与 t 进行异或操作，得到解密后的数据 m。其中 m 为解密算法中计算得到的明文。

（6）检查 u 与 C3 是否相等，若不相等则报错，并退出。

（7）输出明文 m。

三、方案设计

（一）总体过程

如图 1 所示，该方法首先对原始人脸图像进行可逆变换处理，并采用 MTCNN 算法进行人脸检测和对齐；然后，使用深度学习模型（如 FaceNet、ArcFace 等）进行人脸特征提取，产生高维的特征向量；接着，使用 SM2 非对称加密和 AES 对称加密算法对特征向量进行加密，并加入数字签名验证，确保数据完整性和可靠性。与传统加密算法相比，本方法的密钥长度更短且更安全，平均加密和解密的时间延迟更低。最后，使用解密后的特征向量与预存储的人脸特征向量进行比较，采用欧氏距离或余弦相似度等相似度度量方法进行特征匹配和人脸识别，取得了较好的识别效果。

图 1 基于深度学习和加密算法的安全人脸特征保护总体流程图

（二）加密过程

首先需要对目标图像进行图像转换，使用 Hash 函数计算公式 hi=SHA-256(mi)hi=SHA-256(mi)（其中，mimi 是原始图像的第 ii 个像素）对图像进行可逆转换处理，使用基于无损压缩的可逆信息隐藏。这类算法的思想是对原始图像进行无损压缩，产生冗余信息，使用冗余位置来隐藏数据。

利用多任务卷积神经网络 MTCNN 模型对所输入的图片进行人脸检测对图像，对人脸五个关键点进行检测，包括两眼、鼻子和两边嘴角的位置。在检测流程中，首先对输入图像进行多尺度变换，生成图像金字塔以适应不同大小的人脸。该金字塔图像随后被输入至 P-Net，该网络结构较为简单，通过卷积运算快速生成初步的人脸候选框。接着，这些候选框被送入 R-Net（Refine Network）进行精细化筛选；R-Net 在 P-Net 的基础上增加了全连接层，能够更准确地校准人脸区域。最后，O-Net 在前两级网络的基础上，使用更深的网络结构进行最终优化，实现人脸边界框的精确回归以及面部特征点位置的标定，从而提取人脸特征向量。

利用深度学习模型（如 FaceNet、ArcFace 等）对人脸区域进行特征提取，得到高维的人脸特征向量。将人脸特征向量转换为字节流表示。

四、安全分析

基于 SM2 椭圆曲线公钥密码算法构建。令用户 A 为加密方，用户 B 为解密方，双方预先约定相同的公共参数集 pp，其中包括大素数 p、定义在有限域 Fp 上的椭圆曲线 E、该曲线的一个 q 阶基点 G。设定明文空间 M 的比特长度 mlen 为 32 比特。符号说明如下：若 k 属于 Zq*，则 [k]G 表示基点 G 的 k 倍点；H 为一个输出域为 Zq 的密码杂凑函数；“x||y”表示比特串或字节串的拼接；“⊕”表示异或运算。

密钥生成阶段：用户 B 随机选取私钥 sk ∈ Zq-1*，并计算其对应的公钥 pk = [sk]G。

加密阶段：当用户 A 需要向用户 B 发送消息 m 时，执行以下步骤：

（1）计算椭圆曲线点 S = [h]pk（其中余因子 h 取 1），若 S 为无穷远点则终止流程。

（2）随机选取 k ∈ Zq-1*，计算点 c1 = [k]G = (x1, y1) 以及点 [k]pk = (x2, y2)。

（3）计算密文分量 c2 = [m]G + [k]pk。

（4）计算杂凑值 c3 = H(x2 || m || y2)。

（5）最终输出密文 c = (c1, c2, c3)。需要指出，标准 SM2 算法中 c2 通常由 m 与通过密钥派生函数 KDF 生成的 t 异或得到，但因本方案后续计算无需 t，故此处省略该计算。

解密阶段：用户 B 收到密文 c = (c1, c2, c3) 后，按如下流程解密：

（1）验证 c1 是否满足椭圆曲线方程，若不满足则报错退出。

（2）计算点 S = [h]c1（h=1），若 S 为无穷远点则报错退出。

（3）计算点 [sk]c1 = (x2, y2)，进而通过计算 c2- [sk]c1 得到点 [m]G。

（4）利用 BSGS 算法从点 [m]G 中恢复出明文 m。

（5）若处理的密文已通过同态运算，则直接输出 m 并退出。

方案性质：该方案满足解密正确性，因为对于诚实用户，有 c2 - [sk]c1 = [m]G。同时，方案支持加法同态运算：设明文 m1 和 m2 对应的密文分别为 (c1, c2, c3) 和 (c1‘, c2’, c3‘)，则密文分量满足 c1 + c1’ = [k1 + k2]G，c2 + c2‘ = [m1 + m2]G + [k1 + k2]pk。解密方可以从求和后的密文中得到点 [m1 + m2]G，并同样借助 BSGS 算法恢复出明文之和 m1 + m2。

方案特点与应用背景：该基于 SM2 的同态加密方案在提供加法同态性的同时，保留了密文校验能力。在典型的无第三方参与的两方纵向联邦学习场景（如逻辑回归）中，参与方需加密交互中间数据以协同训练模型。然而，进行同态计算的一方无法解密，而解密方获得的直接结果常为随机值，使得标准密文校验失效。本方案通过特定的设计，在限定明文空间（如 32 比特）以保障 BSGS 算法恢复效率的前提下，实现了对同态操作后密文有效性的验证。假设基于明文长度固定为 32 比特进行测算，且计算过

程采用标识密码算法，则不同方案密钥和密文对应的长度如下表1所示。

表1 不同方案密钥和密文对应的长度（单位：bits）

方案	公钥长度	私钥长度	密文长度
Exp-ElGamal	512	256	1024
Paillier	3072	3072	6144
Twisted-ElGamal	264	256	528
标准 SM2	512	256	800
基于 SM2 的加法同态加密	512	256	770

五、结束语

在人脸识别技术的不断发展和应用的背景下，我们提出了一种基于深度学习和加密算法的人脸特征保护方法。该方法通过对原始人脸图像的可逆处理和人脸检测与对齐，使用深度学习模型提取高维特征向量，并通过 SM2 非对称加密和 AES 对称加密算法对特征向量进行加密，同时加入数字签名验证以确保数据的完整性和可靠性。

实验结果表明，该方法比传统加密算法更好地保护人脸特征数据的安全和隐私，同时具有更高的安全性、可靠性和识别精度，且加密和解密速度更快，具有更高的实用性。

参考文献

[1] 张晶晶，李秋艳，刘硕等 . 基于深度学习的人脸识别在身份认证领域应用综述 [J]. 数据通信 ,2021.

[2] 张建晓，身份认证技术及其发展趋势 [J]. 信息通信 ,2015.

[3] 段正敏，身份认证技术研究与实现 [D]. 重庆大学 ,2004.

[4] 卢亚楠，应用于人脸身份特征的模板保护方法研究 [D]. 沈阳工业大学 ,2023.

[5] 李丽平，许营坤，王嘉航 . 基于锚框稀疏图像金字塔的 MTCNN 人脸检测方法 [J]. 浙江工业大学学报 2023.

[6] 郝林倩，基于 CNN 的 FaceNet 算法人脸图像识别研究 [J]. 智能计算机与应用 ,2022.

[7] 陈有涛 ,SM2 加密算法硬件设计与实现 [D]. 山东大学 ,2022.

[8] 孙学刚，基于 AES 的统一图像加密算法研究 [D]. 江西财经大学 ,2023.

[9] 陈楠，基于椭圆曲线的无证书 SM2 数字签名方案 .[J]. 现代计算机 ,2023.

[10] 许馨，郭家赫，乔宇等 . 一种基于遗忘机制与余弦相似度的智能推荐算法 [J]. 软件工程 ,2023.

