山西大学学报(自然科学版)47(5):964—972,2024
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2023101

基于轻量神经网络的指静脉密钥生成方法

周洋,王明文*
(西南交通大学 数学学院,四川 成都 611756)

摘 要:针对生物特征密钥生成中容易泄露模板信息、精度性能不高和过于复杂难以运用等问题,提出一种基于轻量神经网络的指静脉密钥生成方法。以反向残差瓶颈结构为核心提出轻量神经网络,结合标签平滑交叉熵对指静脉图像训练处理。在密钥生成模块中提出随机选择模块,快速生成新的密钥。最后采用纠错技术与安全散列算法,解决网络提取特征的不稳定性,增强密钥生成方法的安全性。该方法在三个公开数据库中得到了验证,提出的方法生成512位密钥的误识率为0.843%~1.469%、拒真率为0.651%~1.524%,并且密钥生成耗时不超过0.3 s,获得了比其他方法更优越的性能。安全分析表明,提出的模型可以有效抵御信息泄露、交叉匹配和其他攻击。理论分析和实验结果表明该方法具有泛化能力强,生成密钥精度高、生成时间短、安全性高等性质。

关键词:生物特征密钥;轻量神经网络;反向残差瓶颈结构;安全性分析
中图分类号:TP391 **文献标志码:**A **文章编号:**0253-2395(2024)05-0964-09

Finger Vein Key Generation Method Based on Lightweight Neural Network

ZHOU Yang, WANG Mingwen*
(*School of Mathematics, Southwest Jiaotong University, Chengdu* 611756*, China*)

Abstract: Aiming at the problems of easy disclosure of template information, low accuracy performance, complexity, and difficulties in generating biometric key, a finger vein key generation method based on lightweight neural network was proposed. Taking the inverted residual bottleneck structure as the core, a lightweight neural network was proposed, the finger vein image training processing was combined with label smoothing cross-entropy. In the key generation module, a random selection module was proposed to generate new keys quickly. Finally, error correction technology and security hash algorithm were used to solve the instability of network feature extraction and enhance the security of key generation method. This method has been verified in three public databases, and the false acceptance rate of the proposed method to generate a 512-bit key is 0.843%-1.469%, the false rejection rate is 0.651%-1.524%, and the key generation time does not exceed 0.3 s, which shows superior performance than other methods. Security analysis shows that the proposed model can effectively resist information leakage, cross-matching and other attacks. Theoretical analysis and experimental results show that the proposed method has the properties of strong generalization ability, high key generation accuracy, short generation time and high security.

Key words: biometric keys; lightweight neural networks; inverted residual bottleneck structure; security analysis

0 引言

密钥是现代密码系统中的核心要素,出于安全性考虑需要其具备足够的长度和随机性。密钥难以记忆,因此在密码应用系统中通常将其保存在智能卡中,然而一旦智能卡丢失或被

收稿日期:2023-03-15;**接受日期:**2023-05-26
基金项目:国家自然科学基金(62106206);四川省科技计划项目(2020YFG0045)
作者简介:周洋(2002-),女,四川南充人,硕士研究生,研究方向为智能信息处理。E-mail:918740591@qq.com
* **通信作者:**王明文(WANG Mingwen),E-mail:wangmw@swjtu.edu.cn
引文格式:周洋,王明文.基于轻量神经网络的指静脉密钥生成方法[J].山西大学学报(自然科学版),2024,47(5):964-972. DOI:10.13451/j.sxu.ns.2023101

盗,将导致系统不可用。鉴于人脸、指纹、指静脉等人体生物特征所具有的便携性、永久性、唯一性和高熵性特征,基于生物特征生成密钥无疑对克服传统密钥存在的问题具有十分重要的意义,在诸如身份认证、数字货币、数据加密、数字签名等信息安全场景中具有广阔的潜在应用。

由于光照、旋转、角度等原因,对同一个用户不同次的生物特征采样结果并不相同,而密钥必须是绝对精确的,为解决这种不确定性和确定性之间的矛盾,对生物特征自身的稳定性以及生物特征向量的提取方法都提出了较高的要求。2018年,王科俊等[1]使用改进的多尺度块中心对称局部二进制模式提取手指静脉特征信息生成密钥,同年Anees等[2]提出了均衡二进制模式提取人脸特征,再量化生成密钥。2021年Wang等[3]提取用户的指纹细节,然后计算两个细节的特征距离,使用特征距离构造唯一的区间生成密钥。上述方法对生物特征向量采取的都是手工设计的提取方式,对生物特征图像质量要求高,从而导致算法的泛化能力及鲁棒性较差。由于生物特征图像在提取过程中噪声较多,所以基于传统手工设计特征提取的生物特征密钥生成技术难以生成稳定一致的密钥,密钥精度性能不佳[4-5]。

随着深度学习技术在计算机视觉领域的迅速发展[6-7],采用深度学习网络进行自动特征提取相比传统手工设计特征提取体现出了显著的优越性,基于深度学习的生物特征密钥生成方法能捕获到图像更具有鉴别性的特征信息[8]。2018年Roh等[9]对人脸图像采用卷积神经网络(CNN)提取特征,然后将特征向量输入循环神经网络(RNN)中生成密钥。2020年Roy等[10]设计了三个CNN模型提取稳健的视网膜生物特征,再将所有参数连接在一起生成数字密钥。上述方法主要关注了密钥生成的准确性,但缺少对生物特征密钥安全性的分析。2021年,Peng等[11]提出一种基于反向传播神经网络(BPNN)和随机投影的生物特征密钥机制,通过将生物特征和随机矩阵投影为一个新的向量,然后训练BPNN将密钥和新的投影向量一一对应,在重构阶段即可以通过训练好的网络获得密钥。2022年Wu等[12]设计了一种适用于生成指纹生物特征密钥的多层卷积投影指纹生物特征密钥生成模型,通过特征选择和来自深度神经网络的逐层卷积投影特性有效消除指纹样本之间的不稳定性,进行编码解码获得密钥。上述基于深度神经网络生成密钥的方法虽然能够更好地提取可用于密钥生成的生物特征向量,但普遍模型复杂,对计算设备性能要求高,特征提取耗时长。

随着移动互联网、物联网、区块链等技术的迅猛发展,依托前端嵌入式智能设备的安全应用开始呈现爆发式增长,迫切需要一种基于轻量神经网络进行生物特征的自动提取,进而构建生物特征密钥的方法。2021年,Wang等[13]提出使用轻量神经网络提取人脸特征,然后利用二进制映射网络将特征向量映射到二进制码中生成密钥,获得了较好的时间性能,但仍存在网络训练复杂的问题。另一方面,因为采取的是人脸特征,一定程度上影响了整体方案的识别性能。在轻量级生物特征提取方案中,为达到好的性能对生物特征的稳定性和安全性提出了更高的要求。目前大多数研究所采用的指纹、人脸、掌纹等特征易采集、分辨率较高,但普遍存在易磨损、易留存、不稳定等安全问题。由于手指静脉隐藏在真皮层,具有高隐蔽性、唯一性、高稳定性和活体检测等优秀特性[4],所以本文选用手指静脉作为生物特征。

为了满足移动互联网等环境下生物特征密钥使用的需求,本文提出了一种基于轻量神经网络的手指静脉密钥生成方法。该方法由两部分组成:(1)轻量神经网络构建;(2)密钥生成方法设计。轻量神经网络提取生物图像特征信息,保证特征提取的准确性和速度。密钥生成环节量化特征信息,使用随机序列,在不重新训练网络的情况下对量化后的信息置换洗牌,以生成独特的生物特征密钥;采用纠错码技术和安全散列算法对密钥编码、生成辅助信息。在重构阶段,通过匹配辅助信息,判断生物特征密钥是否重构成功,增强稳定性和安全性。

1 轻量神经网络构建

1.1 预备知识

深度可分离卷积:深度可分离卷积将一个标准卷积(Conv)拆分成深度卷积(Dwise)和点卷积(Pwise),三种卷积如图1所示。标准卷积直接对所有通道进行处理,在深度维度产生一个输出通道。深度卷积则将输入图像和滤波器分离成M个不同的通道,将每个输入通道与相应的滤波器进行卷积,然后将卷积得到的通道堆叠。1×1的点卷积再对堆叠输出通道进行滤波,将堆叠的通道合并为一个通道。如此,深度可分离卷积产生与标准卷积相同的输出。而由图1可知,N个$D_k\times D_k\times M$的标准卷积、M个$D_k\times D_k\times 1$的深度卷积、N个点卷积$1\times1\times M$,设特征图尺寸$D_f\times D_f$,则深度可分离卷积与普通卷积的计算参数量下降倍数[14]如等式(1)所示。式中可见,深度可分离卷积极大提高运算效率[15],减少参数量。

$$\frac{D_k\cdot D_k\cdot D_f\cdot D_f\cdot M+M\cdot N\cdot D_f\cdot D_f}{D_k\cdot D_k\cdot M\cdot N\cdot D_f\cdot D_f}=\frac{1}{N}+\frac{1}{D_k^2}。\quad(1)$$

反向残差瓶颈结构:直接使用深度可分离卷积可能导致神经元梯度为0、权重无法再进行更新,网络无法学习,从而丢失信息。反向残差瓶颈结构[16]解决了这个问题,如图2所示。该结构主要由深度分离卷积构成,在深度卷积之前,加入点卷积升维,获得高维信息,再使用Relu6非线性激活函数,减少函数激活后的损耗;然后通过点卷积降维,将输入和输出相加,使得信息在各层之间流动得更容易。

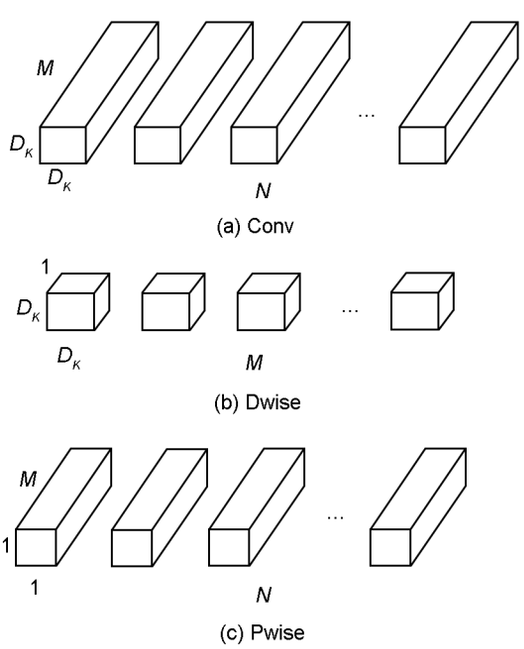


图1 不同卷积示意图

(a)标准卷积;(b)深度卷积;(c)点卷积

Fig. 1 Schematic diagram of different convolutions

(a) Conv (standard convolution); (b) Dwise (depthwise convolution); (c) Pwise (pointwise convolution)

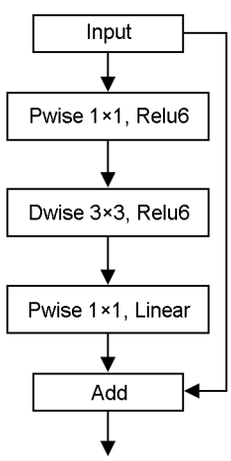


图2 反向残差瓶颈结构(InvBottleneck)

Fig. 2 Bottleneck structure of inverted residual (InvBottleneck)

1.2 提出的网络结构

传统的特征提取算法[17-18]对图像要求较高,泛化能力较差;普通的卷积神经网络太过复杂、参数量和计算量大[19],在实际的特征提取中耗费时间多,难以满足实际应用的需要。为了解决以上问题,减少计算能力和内存存储量,采用深度可分离卷积层代替标准卷积设计一个轻量特征提取网络。所提出的网络是为了准确提取丰富的手指静脉特征信息,所以主体结构采用反向残差瓶颈结构(InvBottleneck),以获得有效且稳健的生物特征向量,如图3所示。由图可知网络设计7层反向残差瓶颈结构和两个卷积层构成特征提取层,并设置分类层来训练网络。在训练网络模型并获得最佳结果后,从特征提取的最后一层中提取指静脉特征,并在后续阶段依赖于这些特征。

1.3 分类用户ID

为了令重构阶段能顺利获取对应用户的存储信息,设置每个用户的真实标签值作为用户ID,利用各自的用户ID查找对应的存储信息,其中$M=\{1,\cdots,C\}$为标签空间,C是类别数。

神经网络的线性层通过检验因变量的预测值进行分类。对任何特征信息 V,将分配给预测响应的最高分量对应的类,具体操作如下:

$$y=f(V,\theta), \tag{2}$$

$$c=j, y_j=\max(y_1,y_2,\cdots,y_C), \tag{3}$$

其中 $f(V,\theta)$ 代表线性层对应函数关系,θ 代表其中的权重。通过注册阶段训练后确定对应函数关系,在重构阶段即对特征信息进行分类,利用分类获得的标签值作为对应用户 ID。

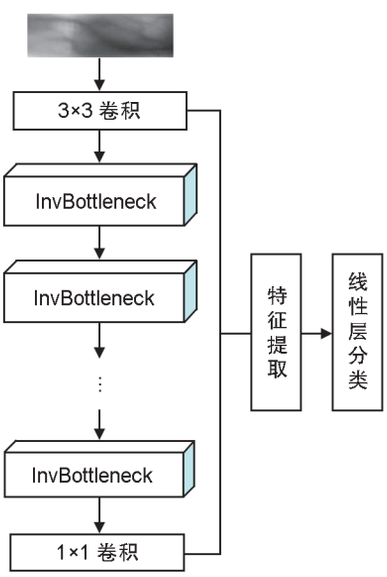


图 3 轻量神经网络模型

Fig. 3 Lightweight network model

1.4 网络训练

指静脉特征相似,将导致模型在训练时过于自信预测标签,使模型的泛化能力差,提取的特征在不同类别间的差距较小。为了增强模型的泛化能力,提高不同类特征信息差距,提出带有标签平滑的交叉熵损失函数来实现端到端的网络训练。

标签平滑是一种正则化策略,通过加入噪声,减少了真实样本标签的类别在计算损失函数时的权重,抑制过拟合,增加类间距离,减少类内距离[20]。增加标签平滑后真实的概率分布发生改变:

$$y_i=\begin{cases}1, i=\text{target}\\0, i\neq\text{target}\end{cases}\Rightarrow\hat{y}_i=\begin{cases}1-\varepsilon, i=\text{target}\\\varepsilon/C, i\neq\text{target}\end{cases}, \tag{4}$$

$$\hat{y}_i=y_i(1-\varepsilon)+\varepsilon/C。 \tag{5}$$

y_i 表示真实的概率值,ε 表示一个噪音系数,一般是一个很小的值。对传统的交叉熵损失函数进行更新替换,可以得到:

$$L=-\sum\hat{y}_i\ln P_i=-(1-\varepsilon)\sum y_i\ln P_i-\varepsilon/C\sum\ln P_i。 \tag{6}$$

网络训练过程采用等式(6)计算损失函数值,使用 Adam 梯度下降算法来更新参数。在训练过程中,完成 20% 的迭代轮次,学习率下降 10%,动态的学习率衰减有助于保持梯度稳定地向下移动,降低网络训练的误差。

2 密钥生成方法设计

2.1 总体框架

基于轻量神经网络的指静脉密钥生成机制总体框架如图 4 所示,包括注册和重构阶段。

注册阶段:针对用户指静脉图像,训练网络、提取指静脉特征和用户 ID。在密钥生成阶段,将特征量化为二进制编码,随机选择生成密钥。最后通过摘要信息生成模块获得哈希摘要,隐藏密钥值,并在注册阶段保存摘要信息和随机序列。

重构阶段:用户使用相同手指采集的指静脉图像,通过网络提取特征信息并分类获得用户 ID,得到二进制编码。再根据用户 ID 获取注册阶段存储的随机序列重构密钥,并对重构的密钥 BCH(Bose Chaudhuri Hocquenghem)纠错解码,然后生成对应摘要信息。最后利用数据库存储的摘要进行匹配,判断解码后的密钥是否与注册阶段生成的密钥一致,确认密钥是否重构成功。

2.2 随机选择模块

随机选择模块将特征信息通过动态阈值分割,转为二进制编码。设特征向量 $\boldsymbol{V}$,$\boldsymbol{V}\in R^l$,l 为向量的维数,令 $\boldsymbol{V}$ 均值 $\bar{V}=\frac{1}{l}\sum_{i=1}^{l}V_i$ 为阈值,二进制量化函数定义为:

$$g(V_i)=\begin{cases}1, & V_i>\overline{V}\\0, & \text{其他}\end{cases}, 1\leqslant i\leqslant l \tag{7}$$

其中 V_i 是 $\boldsymbol{V}$ 中的第 i 个特征分量,二进制编码为 $BK=[g(V_1),g(V_2),g(V_3),\cdots,g(V_l)]$。然后在二进制编码中设计生物特征密钥。对每位用户设置不同的随机种子,采用随机生成器(Random Number Generator,RNG),生成一个 l 维的序列[13]:

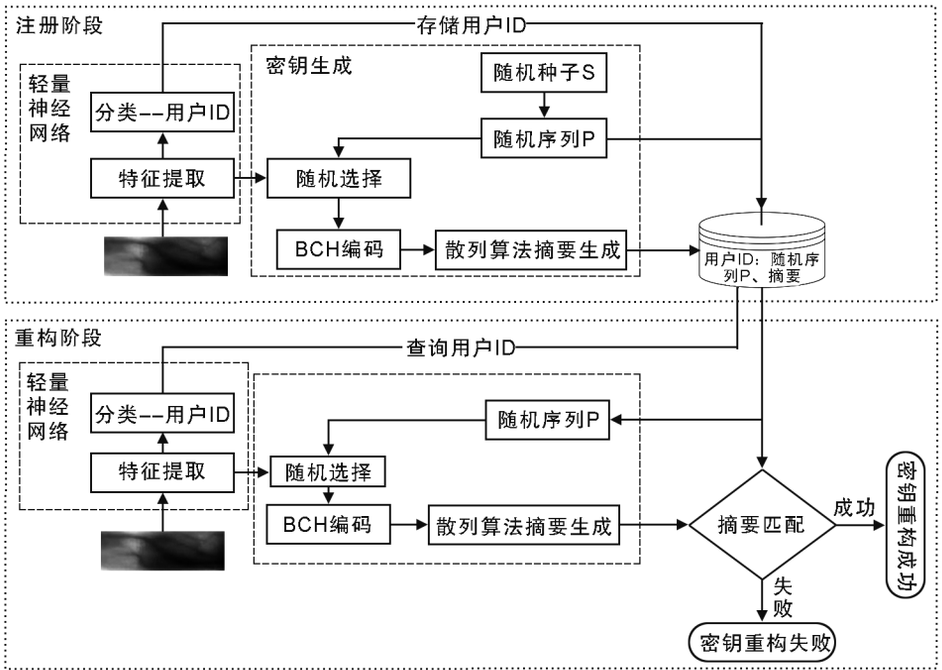
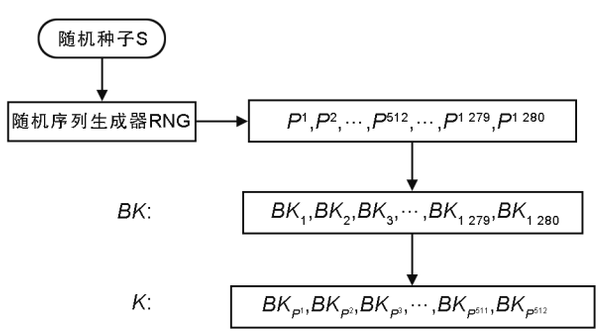


图 4 指静脉密钥生成总示意图(用户ID:用户序列号,BCH:纠正多个随机错误的循环码)

Fig. 4 General diagram of finger vein key generation (User ID: User number, BCH: Cyclic code to correct multiple random errors)

$P=\{P^1,P^2,P^3,\cdots,P^r,\cdots,P^{l-1},P^l\}$, $\forall t\in\{1,\cdots,l\}$, $\exists t=P^r$。在序列 P 中选择前 z 位,二进制编码按照前 z 位序列随机选择,使原来的二进制编码 BK 置换后成为该用户的生物特征密钥:$K=[BK_{P^1},BK_{P^2},BK_{P^3},\cdots,BK_{P^z}]$。以 $l=1\,280,z=512$ 为例,随机选择如图5所示。最后将 z 位随机序列存储在数据库中,重构阶段利用随机序列直接作用生物特征生成密钥。通过随机选择模块,(1)保护生物特征信息,防止泄露;(2)得到不同的二进制编码,满足密钥的可撤销;(3)随时对密钥进行修改,不需要通过网络运算,大大减少计算量,提高密钥生成的速度。



BK:二进制编码序列,*K*:生物特征密钥。

BK: binary encoding sequence, *K*: biometric key.

图 5 随机选择密钥生成示例

Fig. 5 Example of randomly selecting key generation

2.3 摘要信息生成

考虑生物特征密钥的稳定性和安全性,提出摘要信息生成模块。因为生物特征的模糊性,重构阶段的密钥与注册阶段的密钥存在距离误差,提出BCH纠错码校正重构的密钥,以获得稳定唯一的生物特征密钥。当用户验证输入的指静脉图像获得生物特征密钥与正确的密钥编码的距离误差 $|d|$ 小于BCH的容错阈值 τ 时,可以正确恢复生物特征密钥[13];相反,无法正确重构生物特征密钥。为了验证密钥是否成功重构和保证密钥的安全,提出进行安全散列算法生成摘要,通过SHA256散列算法以不可逆的变换化为一段摘要信息。在注册阶段只保存摘要信息,在重构阶段进行对比,判断密钥是否成功重构。该阶段不会泄露密钥,密钥生成安全性得到有效保证。

3 实验设计与分析

3.1 实验准备

实验中,为了确保实验的客观和充分性,采用三个公开可用的指静脉数据库:马来西亚理工大学指静脉数据集(FV_USM)[21]、香港理工大学指静脉数据集(HKPU)[22]、天津指静脉数据集(TJDB)。

FV_USM数据集包含492类样本,每类12张样本图像,总共5 904张图像;HKPU数据集包含312类样本,其中210类有12张样本图像,102类有6张样本图像,总共3 132张图像;TJDB数据集包含64类样本,每类包含15张样本图像,总共960张图像。为了获得最佳的目标结果,对指静脉图像进行感兴趣区域(Region of Interest,ROI)处理,并随机旋转20%的图像,保证特征提取模块的鲁棒性和泛化性。为了保证网络特征提取的有效性,将数据集划分为训练集和测试集,具体样本数如表1所示。训练步骤和测试步骤是在NVIDIA GTX 1080Ti GPU上运行,11 GB显存,内存32 GB,采用Pytorch1.7的深度学习框架,编码环境为Jupyter-Notebook和PyCharm。

表1 数据集训练样本和测试样本数

Table 1 Number of training and testing samples in datasets

数据集	训练样本数/张	测试样本数/张
FV_USM	4 723	1 181
HKPU	2 505	627
TJDB	768	192

3.2 轻量神经网络分析

轻量神经网络保证特征提取的准确性和速度。稳定的特征提取不仅对后续密钥生成有着重要作用,在分类获得用户ID的环节也至关重要,特征信息越好,图像分类结果越准确;特征提取耗时越小,密钥生成用时越短。为了评估网络性能,基于上述数据集进行实验分析。

3.2.1 轻量性

通过程序统计得出特征提取阶段在三个数据集的模型大小和耗时,如表2所示。实验数据表明轻量神经网络在三个数据集上模型的参数量不超过3 M,特征提取的时间没有超过0.3 s,表现了所提网络在嵌入式系统应用中的实用性。

3.2.2 识别精度

为了评估指静脉图像识别精度的性能,将本文提出的方法的识别与几种经典的模型进行比较。表3显示了三个数据集在不同模型上的识别准确率。其中'—'表示相关文献中无实验数据和结果。结果表明,本文提出的方法在三个数据集上都取得了令人满意的精度。在三个公开数据集的识别准确率都不低于0.99,与其他四种模型相比,都有增长。而且FV_USM、HKPU数据集复杂、类别多,TJDB数据集的类别少、样本多,数据样本类型不同,但所提出的网络在三个数据集上的识别精度都较好。进一步表明,特征提取模块的提取性能高、分类效果好、模型更具有泛化性。

表2 轻量神经网络参数量和特征提取时间

Table 2 Parameter of lightweight network and time of feature extraction

	FV_USM	HKPU	TJDB
模型参数量/M	2.85	2.62	2.31
特征提取时间/ms	232.37	235.36	204.4

表3 不同模型在三个数据集的识别准确率

Table 3 Recognition accuracy of different models in three datasets

数据集	Liu *et al*. 2018[23]	Das *et al*. 2019[24]	Ren *et al*. 2021[25]	Zhang *et al*. 2022[26]	本文方法
FV_USM	—	0.985 8	0.991 9	0.988	0.999
HKPU	—	0.965 5	0.984 0	0.984	0.993
TJDB	0.969	—	—	—	0.999

3.3 密钥生成性能分析

接下来,基于上述三个数据集分别生成128、256、512 bits密钥,从密钥生成耗时、密钥精度、密钥安全性等方面进行讨论。

3.3.1 密钥生成耗时

密钥生成模块,由表4可知,三个数据集生成128 bits密钥,耗费时间不超过3 ms;生成256 bits密钥耗费时间不超过4 ms;512 bits密钥消耗时间不超过8 ms。

表4 不同长度密钥生成耗时(ms)

Table 4 The elapsed time in ms for key generation of different lengths

	FV_USM	HKPU	TJDB
128 bits	1.99	2.01	0.96
256 bits	3.99	2.98	2.95
512 bits	7.98	6.98	5.95

3.3.2 密钥精度

表5统计了上述三个公开数据集的不同位的生物特征密钥的拒真率FRR和误识率FAR。据表5可知,随着密钥长度的增大,误识率更小,表现了密钥生成模块在长密钥方面的高安全性。

表 5 三个数据集上不同位密钥的精度表现(FRR:拒真率,FAR:误识率)

Table 5 Precision representation of different bit keys on three datasets (FRR: false rejection rate, FAR: false acceptance rate)

密钥长度/bits	FV_USM		HKPU		TJDB	
	FRR	FAR	FRR	FAR	FRR	FAR
128	3.895%	3.992%	5.628%	3.84%	2.734%	2.876%
256	1.566%	3.506%	4.191%	3.525%	1.17%	1.289%
512	1.524%	1.469%	1.79%	1.72%	0.651%	0.843%

3.3.3 与其他密钥生成方法比较

本节主要从密钥精度性能和密钥生成时间消耗两个角度比较我们的方法与其他生物密钥生成方法。如表6所示,前三种方法主要通过传统的特征提取方式,所以在密钥生成时间方面较短,但是获得的密钥性能更低,后面两种方法,采用神经网络的方式提取特征,所花时间较长,但密钥性能较好。本文所提出的方法即是采用轻量神经网络的方法提取特征,相较于MB-CSLBP(Multiscale Block-Center-Symmetric Local Binary Pattern)[1]手指静脉密钥生成方法,密钥性能更加稳定;与Wu等[12]提出的指纹密钥生成方法相比,时间消耗降低了0.4 s。表明了本文提出的方法在生物密钥精度和时间性能间得到了更好的权衡,表现了轻量神经网络特征提取的有效性。同时需要指出的是,以上比较实验对象和环境有所差异,所以比较结果仅具有一定意义。

3.3.4 密钥安全性分析

密钥系统的安全性主要包括生物特征模板信息和生成的生物特征密钥的安全性。本文提出获取用户生物特征,对生物特征随机选择,然后直接生成密钥。在注册阶段没有直接保存生物特征模板和生物特征密钥,而是存储对特征分类后获得的用户ID,然后对应存储随机选择过程的随机序列和最后对生物密钥生成的摘要信息。通过保存摘要信息,判断重构阶段的密钥是否重构成功。所以,攻击者只能通过用户ID获得随机序列和摘要信息。但随机序列和摘要信息都是一串随机的、相互独立的值,与生物密钥并没有联系,想通过这两种数值获得生物密钥是难以实现的。接下来,从暴力攻击和交叉匹配攻击进行讨论。

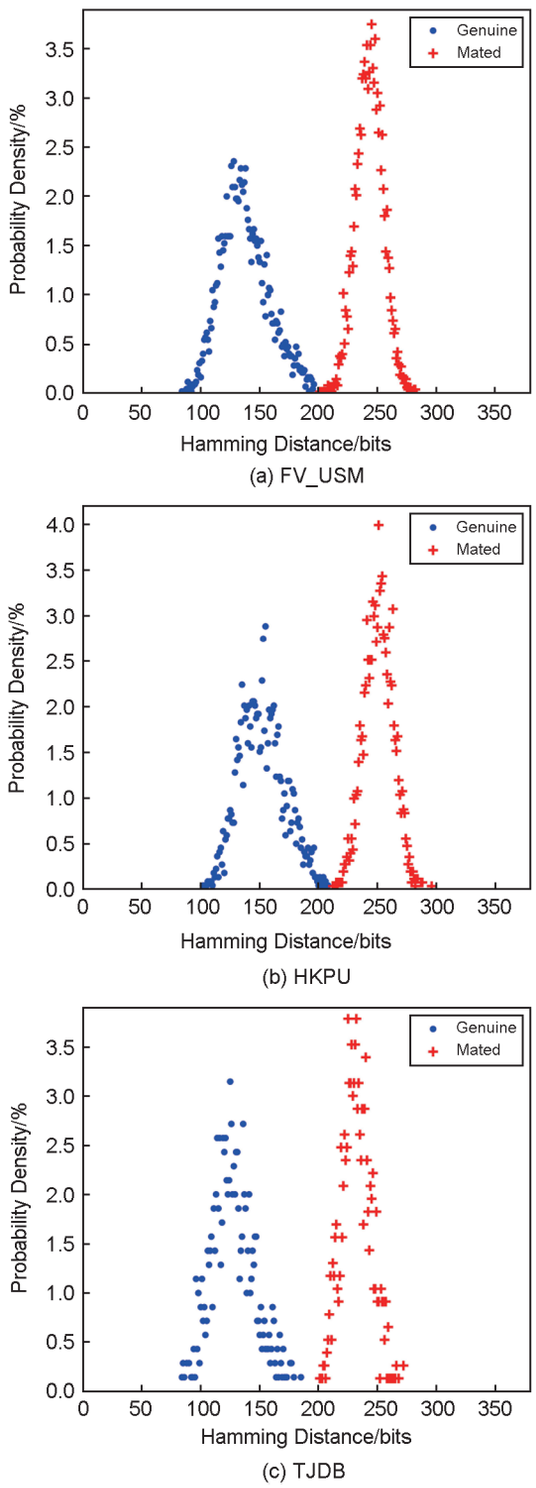
暴力攻击:在这种攻击场景中,攻击者可以尝试猜测生物特征密钥。如果攻击者知道生物特征密钥的长度z,那么攻击者需要进行2^z次实验才能获得正确的结果。例如当$z=512$时,攻击者进行2^{512}次尝试,在这种情况下,攻击者很难猜出生物特征密钥。

交叉匹配攻击:在该场景中,假设攻击者可以获取用户的生物密钥,利用该密钥可以在多个生物特征数据库中进行交叉匹配.但在本文提出的密钥生成方法中,通过生成不同的随机序列,可以再生成新的生物密钥。进一步为了证明密钥的可再生性,在三个数据集进行实验。首先计算相同用户、不同随机种子生成的新密钥和旧密钥之间的汉明距离,记为匹配的汉明距离(Mated)。然后再计算同一个随机种子的用户内部的密钥之间的汉明距离,记为真实的汉明距离(Genuine)。如果匹配的汉明距离都接近$\frac{L}{2}$,L表示密钥的长度,则表示新的生物特征密钥与旧的生物特征密钥完全不同[13]。

表 6 本文方法与其他生物密钥生成方法比较(FRR:拒真率,FAR:误识率)

Table 6 Comparison between our method and other biological key generation methods (FRR: false rejection rate, FAR: false acceptance rate)

方法	生物特征	数据集	密钥长度/bits	密钥精度结果/%	耗时/s
MB-CSLBP 2018[1]	手指静脉	哈尔滨工程大学指静脉数据库	400	FAR=0.47,FRR=22.47	—
Anees *et al*. 2018[2]	人脸	the AT&T face	256	FAR=0.06, FRR=10.02	0.023 1
Wang *et al*. 2021[3]	指纹	FVC2004 DB3、HD-FP2015 DBv1	120~168	FAR=2.58, FRR=7.08	0.051
Wu *et al*. 2022[12]	指纹	Hdu_sec01	512	FAR=3.0, 准确率99.1	0.72
本文的方法	手指静脉	FV_USM、TJDB	512	FAR=0.843~1.469 FRR=0.651~1.524	小于0.3



Genuine:同一个随机种子,用户内部生成的密钥的汉明距离;Mated:相同用户、不同随机种子的新旧密钥的汉明距离。

Genuine: Hamming distance between intra-user keys generated by the same random seed; Mated: Hamming distance between new keys and old keys generated by different random seed in intra-users.

图 6 密钥的匹配和真实汉明距离

Fig. 6 Key mated and Genuine Hamming distance

以 $L=512$ 示例,计算三个数据集匹配和真实的汉明距离作为横坐标,统计该距离的概率密度为纵坐标,如图 6。结果表明,三个数据集的匹配的和真实的汉明距离的分布可区分,匹配的汉明距离主要分布在密钥长度的一半左右。也就是说,来自同一用户的新生物特征密钥和旧生物特征密钥之间完全独立,彼此不同,确保生物密钥对用户的可更新性。所以,本文提出的方法可以有效地抵抗交叉匹配攻击。

综合以上分析,表明本文提出的密钥生成系统具有较好的安全性。

4 结论

本文提出了一种基于轻量神经网络的指静脉密钥生成方法,以解决现有生物特征密钥生成方法安全性低、精度性能差、模型参数多等问题。实验结果表明,所提出神经网络模型参数量不超过 3 M,却在指静脉数据集上有较高的识别精度,表明该网络具有较好的特征提取效果;密钥生成的对比实验中表明,本文提出的密钥生成方法有更好的精度性能。对该方法进行的安全分析结果表明密钥生成系统有较好的安全性。未来的研究将进一步提升所提出的指静脉密钥生成方法性能及扩展到其他生物特征进行测试。

参考文献:

[1] 王科俊, 曹逸, 邢向磊. 基于MB-CSLBP的手指静脉加密算法研究[J]. 智能系统学报, 2018, **13**(4): 543−549. DOI: 10.11992/tis.201704034
WANG K J, CAO Y, XING X L. Finger-vein Encryption Algorithm Based on MB-CSLBP[J]. *CAAI Trans Intell Syst*, 2018, **13**(4): 543−549. DOI: 10.11992/tis.201704034

[2] ANEES A, CHEN Y P P. Discriminative Binary Feature Learning and Quantization in Biometric Key Generation [J]. *Pattern Recognit*, 2018, **77**: 289−305. DOI: 10.1016/j.patcog.2017.11.018.

[3] WANG P Y, YOU L, HU G R, *et al*. Biometric Key Generation Based on Generated Intervals and Two-layer Error Correcting Technique[J]. *Pattern Recognit*, 2021, **111**: 107733. DOI: 10.1016/j.patcog.2020.107733.

[4] HAO F, ANDERSON R, DAUGMAN J. Combining Crypto with Biometrics Effectively[J]. *IEEE Trans Comput*, 2006, **55**(9): 1081−1088. DOI: 10.1109/TC.2006.138.

[5] WU L F, LIU X S, YUAN S L, *et al*. A Novel Key

Generation Cryptosystem Based on Face Features[C]// IEEE 10th International Conference on Signal Processing Proceedings. New York: IEEE, 2010: 1675−1678. DOI: 10.1109/ICOSP.2010.5656719.

[6] ZHAO D D, MA H, YANG Z D, *et al*. Finger Vein Recognition Based on Lightweight CNN Combining Center Loss and Dynamic Regularization[J]. *Infrared Phys Technol*, 2020, **105**: 103221. DOI: 10.1016/j. infrared.2020.103221.

[7] XU X Z, DU M, GUO H X, *et al*. Lightweight FaceNet Based on MobileNet[J]. *Int J Intell Sci*, 2021, **11**(1): 1−16. DOI: 10.4236/ijis.2021.111001.

[8] DAAS S, YAHI A, BAKIR T, *et al*. Multimodal Biometric Recognition Systems Using Deep Learning Based on the Finger Vein and Finger Knuckle Print Fusion[J]. *IET Image Process*, 2020, **14**(15): 3859−3868. DOI: 10.1049/iet-ipr.2020.0491.

[9] ROH J H, CHO S, JIN S H. Learning Based Biometric Key Generation Method Using CNN and RNN[C]//2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE). New York: IEEE, 2018: 136−139. DOI: 10.1109/ICITEED.2018.8534873.

[10] ROY N D, BISWAS A. Fast and Robust Retinal Biometric Key Generation Using Deep Neural Nets[J]. *Multimed Tools Appl*, 2020, **79**(9/10): 6823−6843. DOI: 10.1007/s11042-019-08507-y.

[11] PENG J L, YANG B, GUPTA B B, *et al*. A Biometric Cryptosystem Scheme Based on Random Projection and Neural Network[J]. *Soft Comput*, 2021, **25**(11): 7657−7670. DOI: 10.1007/s00500-021-05732-2.

[12] WU Z D, LV Z Y, KANG J, *et al*. Fingerprint Bio-key Generation Based on a Deep Neural Network[J]. *Int J Intell Syst*, 2022, **37**(7): 4329−4358. DOI: 10.1002/int.22782.

[13] WANG Y Z, LI B, ZHANG Y, *et al*. A Secure Biometric Key Generation Mechanism *via* Deep Learning and Its Application[J]. *Appl Sci*, 2021, **11**(18): 8497. DOI: 10.3390/app11188497.

[14] HOWARD A G , ZHU M, CHEN B, *et al*. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications[EB/OL]. arXiv Preprint: 1704.04861, 2017. https://arxiv.org/abs/1704.04861.

[15] INDRASWARI R, ROKHANA R, HERULAMBANG W. Melanoma Image Classification Based on MobileNetV2 Network[J]. *Procedia Comput Sci*, 2022, **197**: 198−207. DOI: 10.1016/j.procs.2021.12.132.

[16] SANDLER M, HOWARD A, ZHU M L, *et al*. MobileNetV2: Inverted Residuals and Linear Bottlenecks[C]// 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. New York: IEEE, 2018: 4510−4520. DOI: 10.1109/CVPR.2018.00474.

[17] 梁雪慧, 赵菲, 程云泽, 等. 手指静脉特征提取分析与对比[J]. 化工自动化及仪表, 2020, **47**(3): 256−259. DOI: 10.3969/j.issn.1000-3932.2020.03.013.
LIANG X H, ZHAO F, CHENG Y Z, *et al*. Study on Finger Vein Feature Extraction[J]. *Control Instrum Chem Ind*, 2020, **47**(3): 256−259. DOI: 10.3969/j.issn.1000-3932.2020.03.013.

[18] KHUSNULIAWATI H, FATICHAH C, SOELAIMAN R. Multi-feature Fusion Using SIFT and LEBP for Finger Vein Recognition[J]. *TELKOMNIKA Telecommun Comput Electron Control*, 2017, **15**(1): 478. DOI: 10.12928/telkomnika.v15i1.4443.

[19] 张东, 高丙朋. 基于改进MobileNet网络的人脸识别方法[J]. 山西大学学报(自然科学版), 2023, **46**(1): 147−153. DOI: 10.13451/j.sxu.ns.2022036.
ZHANG D, GAO B P. Face Recognition Method Based on Improved MobileNet Network[J]. *J Shanxi Univ Nat Sci Ed*, 2023, **46**(1): 147−153. DOI: 10.13451/j. sxu.ns.2022036.

[20] MÜLLER R, KORNBLITH S, HINTON G. When does Label Smoothing Help?[EB/OL]. arXiv Preprint: 1906.02629, 2019. https://arxiv.org/abs/1906.02629.

[21] MOHD ASAARI M S, SUANDI S A, ROSDI B A. Fusion of Band Limited Phase only Correlation and Width Centroid Contour Distance for Finger Based Biometrics [J]. *Expert Syst Appl*, 2014, **41**(7): 3367−3382. DOI: 10.1016/j.eswa.2013.11.033.

[22] KUMAR A, ZHOU Y B. Human Identification Using Finger Images[J]. *IEEE Trans Image Process*, 2012, **21**(4): 2228−2244. DOI: 10.1109/TIP.2011.2171697.

[23] LIU Y, LING J, LIU Z S, *et al*. Finger Vein Secure Biometric Template Generation Based on Deep Learning [J]. *Soft Comput*, 2018, **22**(7): 2257−2265. DOI: 10.1007/s00500-017-2487-9.

[24] DAS R, PICIUCCO E, MAIORANA E, *et al*. Convolutional Neural Network for Finger-vein-based Biometric Identification[J]. *IEEE Trans Inf Forensics Secur*, 2019, **14**(2): 360−373. DOI: 10.1109/TIFS.2018.2850320.

[25] REN H Y, SUN L J, GUO J, *et al*. Finger Vein Recognition System with Template Protection Based on Convolutional Neural Network[J]. *Knowl Based Syst*, 2021, **227**: 107159. DOI: 10.1016/j.knosys.2021.107159.

[26] ZHANG Z X, WANG M W. A Simple and Efficient Method for Finger Vein Recognition[J]. *Sensors*, 2022, **22**(6): 2234. DOI: 10.3390/s22062234.