BinaryFace: 基于深层卷积神经网络的人脸模板保护模型

赵铖辉, 李　勇, 张振江

北京交通大学电子信息工程学院 北京 中国 100044

摘要　随着生物识别技术的广泛应用, 人们越来越担心生物模板信息的安全性和隐私性。为此人们提出很多生物模板信息的保护算法, 但其一般需要牺牲可识别性来换取高安全性。为了在保证高安全性的同时尽可能提高可识别性, 本文提出一种新的由特征转换和生物加密组成的二阶段人脸模板保护方案。在特征转换阶段, 基于 VGGFace 提出一种新的基于卷积神经网络的 BinaryFace 网络, 通过设计新的随机正交映射矩阵、量化损失函数和最大熵损失函数实现人脸模板的二进制转换。同时为了减少网络参数, 设计新的深度可分离瓶颈卷积层, BinaryFace 相比 VGGFace 在参数和浮点数(Flops)上分别减少约 75%和约 35%。在生物加密阶段, 将人脸二进制模板转换中随机正交映射生成的纠错码输入模糊承诺方案, 生成加密的人脸模板并存储到数据库中。在验证阶段, 通过相同的流程恢复出纠错码, 并与原始纠错码进行哈希校验得到最终的匹配结果。在评测阶段, 本文提出的方法在 CMU-PIE、FEI、Color FERET 等 3 个数据集上, 相比之前的工作在 GAR 上有约 6.5%的提升, 同时将 EER 降低了约 4 倍。

关键词　模板保护; BinaryFace; 随机正交映射; 模糊承诺
中图法分类号　TP391.41　DOI 号 10.19363/J.cnki.cn10-1380/tn.2020.09.04

BinaryFace: the Model of Face Template Protection based on CNN

ZHAO Chenghui, LI Yong, ZHANG Zhenjiang

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Abstract　With the widespread use of biometrics, there is growing concern about the security and privacy of biometric template information. So many protection algorithms based on biological template information have been proposed, but they generally need to sacrifice recognizability in exchange for high security. In order to ensure high security while maximizing recognizability, this paper proposes a new two-stage face template protection scheme consisting of feature conversion and bio-encryption. In the feature conversion stage, a new BinaryFace network based on convolutional neural networks was proposed based on VGGFace. Binary conversion of face templates was achieved by designing a new random orthogonal mapping matrix, quantization loss function, and maximum entropy loss function. At the same time, in order to reduce the network parameters, a new deep separable bottleneck convolution layer was designed. Compared with VGGFace, BinaryFace reduced parameters and floating point numbers (Flops) by about 75% and 35%, respectively. In the bio-encryption phase, the key generated by the random orthogonal mapping in the binary binary template conversion is input into the fuzzy commitment scheme, and the encrypted face template is generated and stored in the database. In the verification phase, the key is recovered through the same process and compared with the original key to obtain the final matching score. At the evaluation stage, the method proposed in this paper has about 6.5% improvement in GAR on the three datasets of CMU-PIE, FEI, Color FERET, etc., while reducing EER by about 4 times.

Key words　template protection; BinaryFace; random orthogonal mapping; fuzzy commitment

1　引言

生物识别是一种基于个人独一无二的行为以及生物学特征的自动识别技术。典型的生物识别系统通过传感器获取用户的生物特征(如指纹、虹膜、人脸、声音、步态等)[1-2], 之后通过算法提取生物特征

通讯作者: 李勇, 博士, 副教授, Email: liyong@bjtu.edu.cn。
本课题得到国家自然科学基金面上项目(No.61472032)资助。
收稿日期: 2019-10-22; 修改日期: 2020-01-07; 定稿日期: 2020-08-21

的主要信息。在注册阶段, 会将提取到的特征向量作为模板 T_x 存储在数据库中。在验证阶段, 匹配器将两个生物模板 T_x (存储的模板)和 T_y (查询的模板)作为输入并输出一个匹配分数来表明两个模板之间的相似性。如果匹配分数超过设定的阈值则表明用户验证成功, 反之表明用户验证失败。

但是一个安全的生物识别系统仅是准确地鉴别用户(减少对合法用户的误判, 即让合法用户丧失系统权限)和拒绝系统服务(减少对非法用户的误判, 即让非法用户拥有系统权限), 也应该保障生物模板的安全性。不像信用卡或密码在泄露后都可以重新分发, 生物特征因为是和用户永久绑定的, 所以无法被替换, 其一旦暴露就将永远丢失。而且丢失的生物模板也将威胁其他数据库(存储同样的生物模板)的安全。因此在设计一个安全的生物识别系统时要优先解决生物模板保护的问题。

一个理想的生物模板保护方案需要满足以下四个要求[2-6]:

1) 多样性: 同一个用户的生物信息可以为了不同的应用需求生成不同的被保护的生物模板;

2) 可取消性: 若用户的生物模板丢失, 则生物识别系统应能轻易地基于相同的生物信息生成新的被保护的生物模板, 替换丢失的生物模板;

3) 安全性: 从被保护的生物模板中恢复出用户原始的生物信息需要难以承受的计算力, 这样能够保证攻击者无法从偷窃得到的生物模板中恢复出原始的生物信息;

4) 可识别性: 在保证生物模板高安全性的同时也要尽可能不影响生物识别系统的正确接收率(Genuine Accept Rate, GAR), 错误拒绝率(False Reject Rate, FRR), 错误接受率(False Accept Rate, FAR)等可识别性能指标[1], 要做到相同用户的生物模板之间的距离尽可能小, 不同用户的生物模板之间的距离尽可能大。

生物模板保护方案为了满足上述四个要求面临的第一个难题是如何解决用户极大的类内差距和极小的类间差距问题。极大的类内差距(由于姿态、光照、表情的不同导致)会导致很高的 FRR, 而极小的类间差距会导致很高的 FAR。为了同时实现模板的高度安全性和可识别性, 生物识别系统的首要目标是尝试减小用户的类内差距和增大用户的类间差距。其次在生物模板保护方案中往往会引入生物加密算法, 这一类算法要求输入必须是二进制向量, 这就引入了量化损失(连续值向量和离散值向量之间的差值)。生物加密算法虽然提高了安全性, 但是却降低了可识别性, 如何尽可能地减小量化损失对于可识别性是极其关键的。

传统的人脸模板保护方案主要分为三类: 生物加密、特征转换、混合策略。

生物加密在人脸模板保护方案中引入了加密系统, 因此能得到极高的安全性。经典的生物加密方案如模糊金库[7](Fuzzy Vault)和模糊承诺[8](Fuzzy Commitment)都会输出一个加密的生物模板来提高安全性。两个方案都使用了纠错码(Error Correcting Code, ECC)来解决类内差距大的问题, 但当类内差距过大时仍旧会导致可识别性能的下降。同时加密方案要求输入必须为二进制向量, 由于传统的卷积神经网络输出的都是实值化向量, 因此在转换的过程中会带来量化损失。

特征转换会将原始的生物模板转换到另一个新的空间域, 其通常通过不可逆变换(Non-invertible Transform)和加盐法(Salting)实现。但是这些方法都需要在可识别性和安全性之间做出选择, 无法做到两者兼容。Ratha 等人[9]为了生成可取消的人脸和指纹模板提出了三种不可逆变换, 分别是笛卡尔坐标变换、极坐标变换、函数变换。但这些变换在实现了高安全性的同时降低了可识别性。Teoh 等人[10]针对人脸模板保护提出了基于加盐转换法的随机多空间量化(RMQ, Random Multispace Quantization)。但在加盐法中使用的变换函数的安全性取决于密钥, 若密钥丢失则将引发严重的安全问题。

混合策略结合了生物加密和特征转换两种方案的优点。Feng 等人[11]为生成人脸保护模板第一次提出了混合策略。这种方法采用特征向量提取器从人脸模板中提取特征信息, 同时令随机映射将提取后的人脸模板映射到一个新的子空间, 从而生成可取消的模板。然后引入能保留识别性能的转换方法来加强可取消模板的可识别性, 并且将实值化模板转换为二进制模板。最后采用模糊承诺方案来保障二进制模板的安全性。

深度卷积神经网络(Deep Convolutional Nerual Network)已经在人脸识别领域取得了巨大的进展, 如 Facenet[12]和 VGGFace[13]等算法的表现已经超越了大多数传统算法。因此, 越来越多的工作聚焦于如何将深度卷积神经网络引入人脸模板保护方案来提高可识别性。Feng 等人[14]第一次将卷积神经网络(CNN)中的感知机(Perceptron)引入了特征转换模块, 实现二进制模板转化的同时提高了人脸模板的可识别性。但感知机(单个神经元)是单层线性映射函数, 无法拟合比较复杂的人脸图像。Erin Liong 等人[15]

通过结合 GIST(Generalized Search Trees)特征和 3 个全连接层(Fully Connected Layer)来拟合原始人脸图像到二进制模板的多层非线性变换, 进一步提升了神经网络的学习能力。Pandey 和 Govindraju[16]利用梯度直方图(Histogram of Gradients, HoG)和局部二进制模式(Local Binary Pattern, LBP)从选中的人脸局部区域中提取特征。利用哈希函数(SHA3-512)对每一个局部区域中提取到的特征进行处理。最后将一系列处理后的局部特征作为人脸模板进行存储。这种方法的匹配准确率较低并且哈希后的特征空间不是均匀分布的。为了解决上述算法的缺陷, Pandey 等人[17]提出新的人脸模板保护算法, 其在注册阶段会给每一个用户分配一个独一无二并具有最大熵的二进制代码(按位随机生成), 并用浅层卷积神经网络(由两个卷积层和两个全连接层组成)学习人脸图像到二进制代码的紧凑映射。分配给用户的二进制代码经过哈希函数(SHA3-512)压缩后作为最终被保护的人脸模板。这种算法在可识别性很低时依旧具有较高的 FRR, 约 5%左右。但由于类内差距较大的影响, FRR 随着匹配分数的升高而不断增大, 最高能到 80%左右。Hassner 等人[18]将人脸进行 3D 对齐后进行切割, 划分成多张图片后利用平均池化技术(Average Pooling)学习人脸特征。平均池化技术极大地减少了模型的时间和空间开销。Bodla 等人[19]考虑到不同的网络会响应不同的人脸特征, 如光照、姿势以及表情等, 提出联合多个浅层网络学习不同的人脸特征, 联合网络通过增加网络宽度提高了可识别性, 却增加了时间和空间的开销。Talreja 等人[20]提出将人脸特征和虹膜特征相结合来进一步保障生物模板的安全性, 利用两个浅层网络设计了双线性转换网络(Bilinear CNN)实现多模态识别。

在特征提取方面, 上述人脸模板保护方案采用的都是人工设计特征或者浅层卷积神经网络, 或是网络太浅导致提取抽象特征的能力不足, 或是网络太宽导致空间和时间开销过大。在确保模型收敛的情况下, 卷积神经网络一般越深就能够更加有效地最小化用户人脸模板的类内差距和最大化类间差距。为了从用户的原始生物信息中提取得到更加独一无二的特征, 本文提出了一种基于深层卷积神经网络的 BinaryFace 网络, 并且为了方便移动端部署, 对其进行了轻量化设计; 在特征转换方面, 将传统三阶段方法中的随机映射改为随机正交映射并融合到 BinaryFace 网络中, 实现模型的端到端训练, 极大地提高了运行效率; 在生物加密方面, 传统的人脸模板保护方案在实现加密时没有考虑到二进制模板的量化损失对可识别性造成的影响, 本文设计了二进制损失(Binary Loss)来尽可能减小转换实值模板带来的量化损失。

本文的主要贡献总结如下:

1) 提出一种新的 BinaryFace 网络。设计新的量化损失和最大熵损失函数实现人脸模板的二进制转换; 对网络进行轻量化设计, 改进的深度可分离瓶颈卷积层极大地减少了参数, 从而在不损失方案可识别性的情况下提升运行效率; 引入新的随机正交映射矩阵形式替代传统的随机映射矩阵形式, 设计的正交损失函数在减少额外信息损失的同时实现正则化。

2) 提出一种新的二阶段人脸模板保护方案。由负责特征转换的 BinaryFace 网络和负责生物加密的模糊承诺方案组成, 并且将两个模块的 Key 进行了统一。此方案在 FEI[1]、CMU-PIE[21]、Color FERET[22]上的可识别性表现好于现有算法, 相比之前的工作在 GAR 上有约 6.5%的提升, 同时将 EER 降低约 4 倍, 并且在安全性方面进行了详细的分析。

2 二阶段方法

如图 1 所示, 原始的人脸图像经过 BinaryFace 后能够得到可取消的二进制模板, 其中的特征提取模块用于生成紧凑的二进制模板, 随机映射模块用于生成具有高度安全性的可取消模板, 然后将深层卷积神经网络提取得到的二进制人脸特征输入模糊承诺方案, 生成最终存储在数据库中的加密模板。二阶段方法相比传统的三阶段方法[11]的不同之处在于将特征提取和随机映射整合到了同一个 BinaryFace 框架中, 因此可以方便地进行端到端的训练, 有利于提升人脸模板保护方案的可识别性。

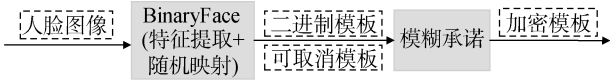


图 1 二阶段人脸模板保护方案

Figure 1 Two-Stage face template protection scheme

如图 3 所示, 人脸模板保护方案由数据预处理、特征转换、生物加密、匹配器 4 部分组成。首先通过传感器(包括注册阶段和验证阶段)获取每一位用户的一张或多张人脸图像, 同时为每一位用户随机生成一组 $\{\theta_1,\theta_2,\cdots,\theta_n\}$,($n=64,128,256,512$), 这组 θ 值将用于生成独一无二的随机映射矩阵, 并作为模糊承诺方案的随机密钥使用。每一张原始注册图像经过人脸检测和人脸对齐模块后会得到标准尺寸的正面人脸图像, 训练图像经过 BinaryFace 后会得到 n 维(n=64,128,256,512)的特征向量。利用先前生成的独一

无二的随机映射矩阵对每一个 n 维特征向量作安全并且可取消的非线性变换, 转换后的的 n 维特征向量经模糊承诺方案处理后会得到帮助数据(Help Data), 最后将帮助数据和随机密钥的哈希值作为被保护的人脸模板存储到数据库中。将验证阶段的测试输出经过模糊承诺方案处理后得到的随机密钥哈希值与人脸模板数据库中对应存储的随机密钥哈希值进行对比, 即可得到最终的匹配结果, 若匹配分数大于设定的阈值, 则表明匹配成功, 反之表明匹配失败。

2.1 BinaryFace

在文献[17]中首次提出利用浅层卷积神经网络(由两个卷积层和两个全连接层组成)学习人脸图像到二进制代码的映射, 但其对图像抽象特征的提取能力受到了网络深度的限制, 并且没有解决二进制模板带来的量化损失。在特征提取方面, 本文采取 Parkhi 等人[13]提出的 VGGFace 作为基础网络。引入深层卷积神经网络 VGGFace 虽然能够极大地提升网络提取抽象特征的能力, 但也会导致模型参数急剧增多。因此针对原始的 VGGFace 进行了轻量化设计, 结合深度可分离卷积和全卷积来减少模型参数; 在模板转换方面, 从实值化模板转换到二进制模板会带来量化损失, 同时将随机正交映射结合到 BinaryFace 会带来正交损失, 由此设计量化损失函数和正交损失函数指导模型学习紧凑的二进制模板。

2.1.1 二进制模板学习

轻量化网络结构: VGGFace 数据集上训练得到的 VGGFace 模型在迁移学习上的表现极佳, 非常适合用作人脸识别的预训练模型。VGGFace 模型将人脸识别作为多分类任务(数据集中有 2622 个人)进行学习, 采用 VGG-19[23]基础网络和三元损失[12] (Triplet Loss)学习人脸特征向量。如图 4 所示, 原始的 VGGFace 有 13 个卷积层和 3 个全连接层, 其参数比较庞大, 不仅影响了模型的收敛速度, 同时极大地降低了测试阶段的效率。如图 5 所示, 为学习用户人脸图像到二进制特征向量的稳健映射, BinaryFace 采用了 VGGFace 的前 10 个卷积层作为基础网络, 并且为了减少模型的参数, 对后 3 个卷积层重新进行设计, 同时将所有全连接层替换成全卷积层。其中新的深度可分离瓶颈卷积层结合残差网络[24](Resnet)的瓶颈结构(Bottleneck)和深度可分离卷积模式[25](Depthwise Separable Convolutions)。如图 2 所示, 深度可分离瓶颈结构中的第一个 1×1 卷积层(Projecton Layer)负责将 512 维的输入特征向量映射为 128 维的输出特征向量, 即减少了后续 3×3 卷积层所需的输入通道数。1×1 卷积层后面添加批标准化层(Batch Normalization)和激活函数层(ReLU)。位于中间的 3×3 卷积层(Depthwise Conv)负责对输入向量的每个通道单独做卷积操作来提取空间信息。最后的 1×1 卷积(Expansion Layer)将由 3×3 卷积层得到的不同通道的输出向量结合起来, 即将 128 维的输入特征向量扩展 128 维的输出特征向量, 从而达到和标准卷积一样的效果。右侧的实线表示恒等映射(Shortcut), 其为模型的梯度反向传播建立新通道, 从而解决梯度消失。同时在 13 个卷积层后添加了一个 7×7 的新卷积层将输入特征向量拓展为 1×1×4096 维, 之后新添加的三个全卷积层的维度分别为 4096,2048,1024, 维度的依次递减增强了网络提取抽象特征向量的能力。由于 BinaryFace 所有层都为卷积层, 因此其网络输入不受图像尺寸的影响, 且最后一层全卷积层的维度也可取为 128,256,512,1024 中的一种, 维度越大表明向量搜索空间越大, 即提取得到的人脸模板越安全。上述的卷积层设计模式在确保深度网络训练可收敛的情况下有效减少了模型的参数量。如表 1 所示, BinaryFace 相比 VGGFace 在参数(代表模型大小, 即空间开销)上减少约 75%, 同时在浮点数(代表计算量, 即时间开销)上减少约 35%。综上所述, 由于方案在空间和时间上的开销都有较大的改善, 因此极大地提升了方案在实际部署时的运行效率。

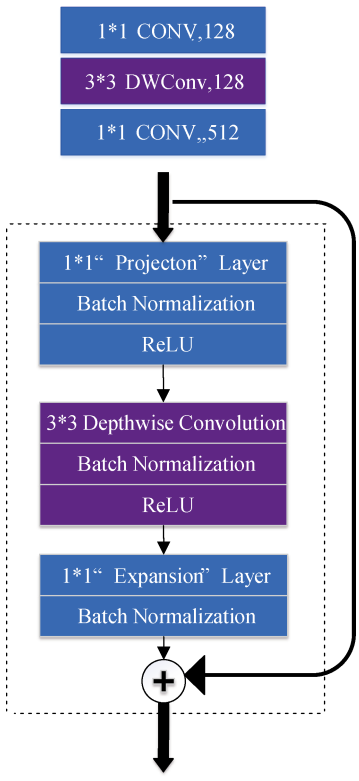


图 2 深度可分离瓶颈层结构

Figure 2 Bottleneck Layer of Depthwise Separable Convolution

表 1 模型大小以及运行开销的比较

Table 1 Comparison of model size and running cost

模型	参数(M)	浮点数(G)
VGGFace	141.9	12.0
BinaryFace	35.3	7.8

多种输出格式: BinaryFace 的网络输出分为三种, 分别为随机正交映射输出, 软最大化函数(Softmax)输出, 阶跃函数(Step Function, Sgn)输出。随机正交映射输出是对提取得到的人脸特征向量做了不可逆的线性变换, 进一步增加了人脸模板的安全性; 软最大化输出是实值化的人脸特征向量, 用于计算三元损失; 阶跃函数输出是二值化的人脸特征向量, 用作模糊承诺方案的输入。

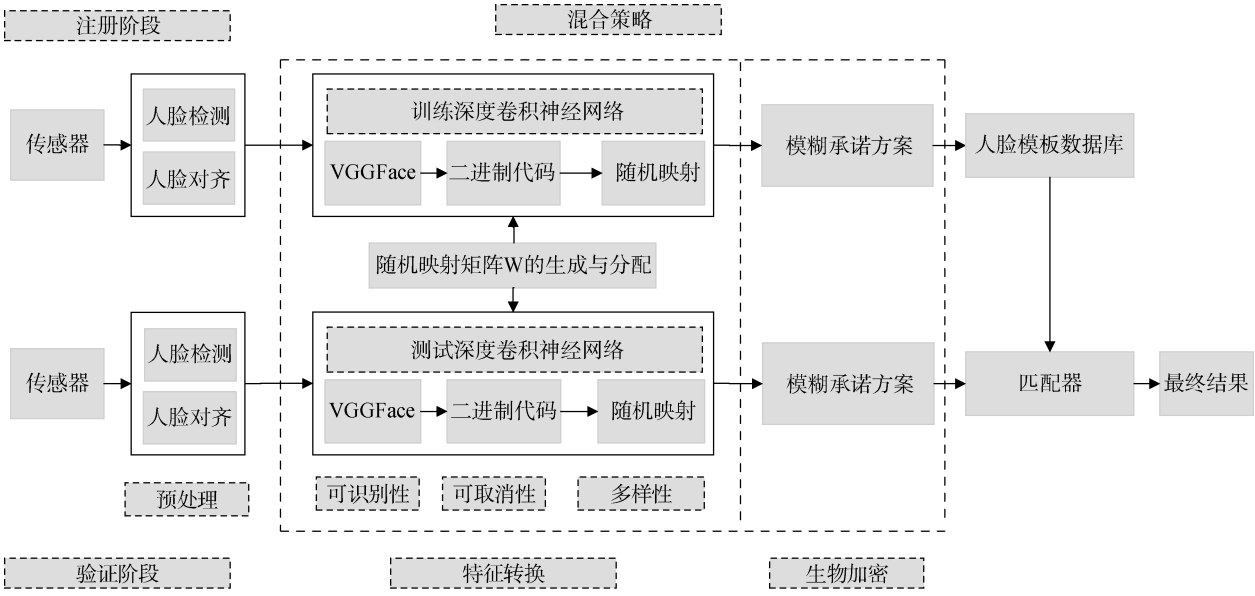


图 3 人脸模板保护方案整体框架

Figure 3 Framework of face template protection scheme

图 4 VGGFace

Figure 4 VGGFace

图 5 BinaryFace

Figure 5 BinaryFace

多个损失函数: 将待训练的人脸样本 x_n (n 为训练集中人脸样本的数量)送入由多个非线性转换堆叠而成的 BinaryFace 后会得到一个二进制向量 b_n。假设深度卷积神经网络有 M+1 层, 第 m 层有 p^m 个神经元, 其中 $m=1,2,\cdots,M$。对于每一个输入的人脸样本 $x_n \in R^d$ (d 为输入图像的维度), 网络第一层的输出为: $h_n = f(W^1 x_n + c^1) \in \Re^{p^1}$, $W^1 \in \Re^{p^1 \times d}$ 为网络第一层需要学习的映射矩阵(也称为卷积核), $c^1 \in \Re^{p^1}$ 是第一层的偏置, $f(.)$ 是激活函数, 在 BinaryFace 中采用的是 ReLU 函数。网络第一层的输出可以视为网络

第二层的输入, 依次类推可以得到网络第 m 层以及网络顶层的输出:

$$h_n^m = f(W^m h_n^{m-1} + c^m) \tag{1}$$

$$h_n^M = f(W^M h_n^{M-1} + c^M) \tag{2}$$

从输入到输出的映射 $\Re^d \to \Re^{p^M}$ 的网络参数可以表示为 $\{W^m, c^m\}_{m=1}^M, 1 \leqslant m \leqslant M$。

然后对网络顶层的输出 h_n^M 做阈值化操作得到二进制特征向量 $\boldsymbol{b}_n$, 具体公式如下:

$$\boldsymbol{b}_n = \mathrm{sgn}(h_n^M) \tag{3}$$

由此可以得到所有人脸训练样本对应的二进特征向量的矩阵表示 $\boldsymbol{B} = [b_1, \cdots, b_N] \in \{-1,1\}^{K \times N}$ 和网络的第 m 层输出 $H^m = [h_1^m, \cdots, h_N^m] \in \Re^{p^m \times N}$。

1) 度量损失(Metric Loss): 人脸识别与图像分类之间的最大区别是其划分粒度特别小, 精细到每一个独一无二的个体。因此需要解决类间差距和类内差距之间的矛盾, 即不同人之间的距离要足够大, 相同人之间的距离要足够小。本文引入了三元损失[18](Triplet Loss)进行度量学习(Metric Learning), 其能够学习到可区分性大并且紧密的人脸特征向量, 度量损失函数公式如下:

$$P_i^M = \mathrm{Softmax}(H_i^M) \tag{4}$$

$$L_{metric} = \sum_{(a,p,n) \in T} \max\{0, \left\| P_a^M - P_p^M \right\|_2^2 - \left\| P_a^M - P_n^M \right\|_2^2 + \alpha\} \tag{5}$$

其中 α 表示学习间距(Learning Margin), 用来控制类间距离和类内距离的平衡, T 是所有训练三元组的集合, 每个三元组(a, p, n)中的三个元素分别表示锚 P_i^M (需要识别的人脸), 正例 P_p^M (与锚差距小的人脸), 反例 P_n^M (与锚差距大的人脸), 通过度量学习能使得锚与正例的差距越来越小, 与反例的差距越来越大, 从而减小类内差距并增大类间差距。

2) 量化损失(Quantization Loss): 为了增强人脸模板的安全性, 需要对从深度网络中提取得到的人脸特征向量进行生物加密处理。本文采用了经典的模糊承诺方案, 其输入必须是离散且平衡的二进制向量, 因此需要将深度卷积神经网络的实值化输出转换为二进制输出。但在连续值转换为离散值的过程中会不可避免地损失很多原始特征向量的细节信息, 为了在生成二进制向量的同时保留人脸特征向量的可识别性, 需要最小化量化损失使得二进制向量尽可能地接近实质化向量, 量化损失函数公式如下:

$$L_{quantization} = \frac{1}{2} \left\| B - H^M \right\|_F^2 \tag{6}$$

其中 B 表示所有样本的二进制输出, H^M 表示所有样本网络顶层的实值化输出, 计算两者的 F 范数即可得到量化损失。

3) 最大熵损失(Maximum Entropy Loss): 为了使得最终输出的二进制向量的每一个比特互相之间处于良好的平衡状态, 即每一位出现的可能性相等, 需要最大化二进制向量的熵, 即让每一个比特之间的综合距离最大。因此本文设计了最大熵损失函数, 其通过计算网络输出矩阵与自身转置的乘积的迹来表示 H^M 的熵, 最大熵损失函数公式如下:

$$L_{entropy} = \frac{1}{2N} \mathrm{tr}(H^M (H^M)^T) \tag{7}$$

其中 N 表示训练集所有人脸样本的数量, tr 表示矩阵的迹, H^M 表示所有样本网络顶层的实值化输出, T 表示矩阵转置。

4) 正交损失(Orthogonal Loss): 为了解决引入随机正交映射矩阵带来的信息损失, 本文设计了正交损失函数。一方面其可以减少额外的信息损失, 另一方面可以最大化每一层参数矩阵之间的独立性, 避免冗余参数的学习, 起到了一定的正则化作用。同时为了进一步扩大正则化的作用, 在正交损失中添加了网络参数的 F 范数来作为惩罚项, 正交损失函数公式如下:

$$L_{orthogonal} = \frac{1}{2} \sum_{m=1}^{M} (\left\| W^m (W^m)^T - \boldsymbol{I} \right\|_F^2 + \left\| W^m \right\|_F^2 + \left\| c^m \right\|_2^2) \tag{8}$$

其中的 $\boldsymbol{I}$ 表示单位矩阵, W^m 表示所有样本网络第 m 层的权重参数, c^m 表示所有样本网络第 m 层的偏置参数。

BinaryFace 有两个输出, 分别为实质化输出和二值化输出, 实值化模板学习的损失函数为度量损失函数, 其通过学习人脸样本之间的类间距离和类内距离得到最合适的实质化模板; 二进制模板学习中的量化损失、最大熵损失、正交损失是通过端到端方式进行训练的, 其目标函数如下:

$$L_{binary} = \lambda_1 L_{quantization} - \lambda_2 L_{entropy} + \lambda_3 L_{orthogonal} \tag{9}$$

其中 $\lambda_1, \lambda_2, \lambda_3$ 分别为三个损失函数的权重, 分别默认设置为 1, 0.5, 0.5。

2.1.2 随机正交映射

随机正交映射(Random Orthonormal Projection, ROP)利用正交矩阵将一组向量投影到其他子空间中,

能够保持转换之后向量之间的欧式距离不变。这项技术作为生物模板的安全转换模块第一次出现在文献[26]中, 其最大的特征就是能够满足生物模板领域的可取消性。但随机正交映射属于加盐法, 加盐法本身的安全性不高, 存在着天然的缺陷。若其密钥被泄露则会导致生物模板可逆, 即可以从加密后的生物模板中恢复出原始的生物信息。因此, 在文献[11]中作者通过添加量化模块在保留可识别性的同时让生物模板变得不可逆。但其在克服了文献[26]中缺点的同时引入了更多的计算量, 导致很难部署在嵌入式或移动式等计算受限的设备中。本文通过引入新的随机映射矩阵形式, 并将随机映射矩阵嵌入到特征提取网络中, 减少了计算量并得到较高的可识别性。

随机映射的主要目的在于创建 k 个与人脸特征向量维度相同的正交向量。为了生成 k 个正交向量, 首先需要生成k个伪随机向量, 然后通过施密特正交变换(Gram-Schmidt Process)进行转换。上述过程成功的前提是每次生成的随机向量互相之间是线性独立的, 而这并不一定能够得到保证, 其次施密特正交变换的计算量巨大。因此若要将模型部署在嵌入式或移动式等计算受限的设备中, 应该避免大量的施密特正交变换运算。在文献[27]中设计了一种新的正交矩阵分发策略, 其核心思想是直接生成小的正交矩阵来避免施密特正交变换计算。矩阵结构如下所示:

$$I_\theta=\begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix}(\forall\theta\in[0,2\pi]) \tag{10}$$

同样地, 可以生成维度为 $2n\times 2n$ 的正交矩阵 $\boldsymbol{A}$, 矩阵 $\boldsymbol{A}$ 的对角线上有 n 个维度为 2×2 的正交矩阵, 其余位置用 0 填充。矩阵 $\boldsymbol{A}$ 的结构如下所示, 其中的角度集合$\{\theta_1,\theta_2,\cdots,\theta_n\}$是$[0:2\pi]$之间的随机数字。

$$\boldsymbol{A}=\begin{bmatrix}\cos\theta_1 & \sin\theta_1 & \cdots & \cdots & 0\\ -\sin\theta_1 & \cos\theta_1 & \cdots & \cdots & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ \vdots & \cdots & \ddots & \ddots & \vdots\\ 0 & 0 & \cdots & \cos\theta_n & \sin\theta_{n1}\\ 0 & 0 & \cdots & -\sin\theta_n & \cos\theta_n\end{bmatrix}(\forall\theta\in[0,2\pi]) \tag{11}$$

特征提取网络输出的特征向量经过随机映射矩阵后会有部分信息丢失, 这会导致模型可识别性的下降。为恢复这部分丢失的信息, 将随机映射矩阵作为全卷积层添加到特征提取网络中, 即将随机映射矩阵的 $2n\times 2n$ 个值作为全卷积层的初始化参数, 并且在训练过程中直接冻结此层的参数, 即不做反向传播运算。恢复丢失信息的关键在于本文设计了一个新的损失函数模块:

$$L_{entropy}=\frac{1}{2N}\mathrm{tr}(H^M(H^M)^T) \tag{12}$$

$L_{entropy}$ 控制特征提取网络中所有参数矩阵的正交性, 一方面能够让网络参数矩阵与随机映射矩阵的结构保持近乎一致, 避免生物模板的部分信息丢失; 另一方面增大所有参数矩阵(线性或非线性变换)之间的独立性, 减少模型的冗余信息, 模型从而能够学得更准更快。

模型在注册阶段会为每一位用户随机生成一组$\{\theta_1,\theta_2,\cdots,\theta_n\}$,($n=64,128,256,512$)。其中 n 的大小决定了在二进制向量空间中进行暴力搜索的难度, n 值越大所对应维度的特征向量越安全。该组 θ 值与用户在注册阶段的原始人脸图像信息无任何联系, 不会导致任何隐私信息泄露。利用该组 θ 值可生成对应的随机正交映射矩阵, 这些随机正交映射矩阵在内部使用并安全存储, 不会暴露给用户, 其既不与用户也不与用户的人脸图像及其特征向量相关, 因此提供了更高的安全性。同时随机正交映射变换也具有可取消性, 即可以取消已经暴露的原始变换并为每个注册用户重新分配不同的随机正交映射矩阵作为新的变换, 具体操作为选择一组新的角度集合$\{\theta_1,\theta_2,\cdots,\theta_n\}$。这种随机正交映射矩阵的生成和分配策略满足了生物模板保护方案的多样性与可取消性的要求。对于不同的应用, 同样可以为每一个注册用户分配不同的随机正交映射矩阵。在同一个应用中, 同样可以对已注册用户更改已有的随机正交映射矩阵或者给新注册的用户分配新的随机正交映射矩阵。

2.2 模糊承诺方案

为了防止原始人脸图像或可取消模板信息的泄露, 需要对提取得到的二进制模板做进一步的加密处理, 借鉴传统的混合策略引入了生物加密中的模糊承诺方案[7]。如图 1 所示, 人脸图像经过BinaryFace(包含了特征提取和随机映射)后得到可取消的二进制模板, 将其再经过模糊承诺方案处理即可得到加密模板, 加密模板包含帮助数据 HD 和 $hash(C)$。需要注意的是随机正交映射矩阵的 Key 和模糊承诺方案中的 Key 是同一组$\{\theta_1,\theta_2,\cdots,\theta_n\}$。模糊承诺是一种结合了纠错码技术与生物特征模糊性的密钥绑定方案, 其包含承诺和解承诺两个步骤。

如图 6 所示, 在注册阶段(即承诺阶段), 将注册模板转换为可取消的二进制模板 B_T。在帮助数据提

取模块(函数F)中根据 Key $\{\theta_1,\theta_2,\cdots,\theta_n\}$ 生成BCH纠错码 C，长度和二进制模板 B_T 相同。定义偏差 $\delta = B_T - C$ (帮助数据 HD)，则承诺{$hash(C)$，HD}，将 $hash(C)$ 和 HD 存储在人脸模板数据库中；在验证阶段(即解承诺阶段)，将验证模板 B 和帮助数据 HD 同时输入模糊承诺方案恢复得到 BCH 纠错码 C'。在数据恢复模块中，$C' = B - HD = B - B_T + C$。如果 B_T 和 B 在汉明距离下足够接近，则经过 BCH 纠错码的处理，可认为 C' 与 C 一致。可以通过校验 $hash(C)$ 和 $hash(C')$ 是否相等来判断认证是否成功。

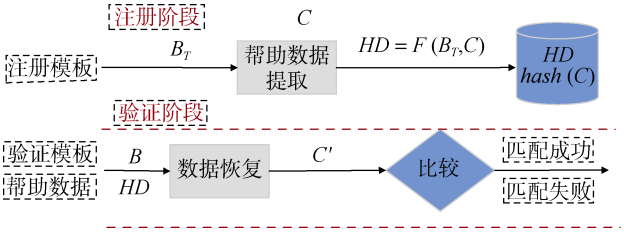


图 6　模糊承诺方案

Figure 6　Fuzzy Commitment scheme

3　实验

本文在三个人脸识别数据集上进行了性能评测，其分别为 FEI[1]、CMU-PIE[21]、Color FERET[22]。考虑到在实际的应用场景中常常面临着人脸训练样本不足的问题，本文研究了人脸的单样本学习和多样本学习在模板保护中的不同性能。单样本学习是指用户在注册时只能提供一张人脸图像，而多样本学习则是指用户可以在注册时提供多张人脸图像。

1) CMU PIE 数据库由 68 个人的 41368 张图像组成。每个人都有 43 种不同照明条件下的图像，13 种不同的姿势和 4 种不同的表情。本文使用 5 个姿势(p05, p07, p09, p27, p29)和所有照明变化。在单样本注册中，为每个用户随机选择一张图像进行训练，其余用于测试。在多样本注册中，随机选择 10 张图像进行训练，其余图像用于测试。

2) FEI 数据库包含 200 个人的 2800 张彩色图像。每个人有 14 个姿势(旋转的范围为 0°~180°)，其中包含两个正面姿势，具有表情变化(非微笑表情和微笑表情)。本文使用 9 个姿势(p03, p04, p05, p06, p07, p08, p11, p12, p13)进行实验。在单样本注册中，为每个用户随机选择一张图像进行训练，其余用于测试。在多样本注册中，随机选择 4 张图像进行训练，其余 5 个用于测试。

3) 在 Color FERET 数据库由 1199 个人的 14126 张图像组成。FERET 数据库中存在姿势，光照，年龄和遮挡变化。在单样本注册中，本文为每个用户随机选择一张图像进行训练，其余的用于测试。在多样本注册中，随机选择 2 张图像进行训练，其余 2 张用于测试。

3.1　实现细节

数据预处理：首先通过传感器获取每一个用户的原始注册人脸图像。传统的人脸数据处理方式常常将人脸检测和人脸对齐分开进行，这种方式极大地影响了预处理阶段的效率。若将人脸检测和人脸对齐联合实现将帮助后续的人脸识别模型提升性能。本文中采用 MTCNN[23]算法对训练集中每一张用户的人脸图像进行人脸检测(找到人脸在哪儿)与人脸对齐(找到人脸关键点)，同时将检测到的人脸图像的尺寸统一转换为 224×224。深度学习网络一般都需要经过大量的数据训练才能表现出良好的性能，而在人脸保护领域的数据采集比较困难，很多用户的图像都只有一张，因此需要对人脸图像进行合理的数据增强，即适当增加每一个用户的人脸图像数量。本文对用户的人脸图像采取了 5 种变换，包括水平翻转、缩放、裁切、光照变换、旋转等。同时对每一张增强后的 224×224 大小图像进行裁切，获取所有 221×221 大小的图像(有(224–221+1)×(224–221+1)=16 张)，并将所有的子图像重新转换 224×224 的大小(对应模型的输入尺寸)。因为在数据增强中采用了 5 种变换方式，所以每一张人脸图像都会对应生成 16×5 张新的图像作为训练集，这种方式能够极大地缓解训练数据不足的问题。

模型训练：BinaryFace 的前 10 个卷积层的参数利用 VGGFace2[29](新版的 VGGFace 模型，数据集有变化，模型不变)前 10 个卷积层的预训练参数进行初始化，后面所有卷积层采用 He 初始化进行设置。在模型的训练过程中利用度量损失指导模型的分类学习，能够减小人脸模板的类内差距并增大其类间差距，同时利用二进制损失指导模型学习紧凑的二进制特征向量。模型的初始学习速率为 0.01，迭代轮次(Epoch)为 90，迭代批次(Batch)为 32，学习率每 30 个迭代轮次衰减至十分之一，采用 Adam[20]算法进行优化，优化算法的参数采用默认设置。在验证阶段，匹配器模块接受两个密钥的哈希值 $hash(K)$ 和 $hash(K')$，并输出真/假匹配分数 S。为了让匹配分数可调，从而可以调整生物识别系统的 FAR 和 FRR 等指标，本文对每个用于验证的图像进行了数据增强，

包括水平翻转、缩放、裁切、光照变换、旋转等。BinaryFace 用于预测对应于每个增强图像的二进制特征向量, 同时将每个预测二进制特征向量与其对应的帮助数据送入模糊承诺方案提取得到 K', 从而产生一组散列 H ($hash(K)$ 和 $hash(K')$)。最终匹配分数被定义为 H 中 $hash(K)$ 和 $hash(K')$ 匹配的数目, 同时对其进行归一化(正确匹配的数目/总数目)。

3.2 性能比较

如图 7 所示, 本文在单样本注册和多样本注册中随机生成了 5 个训练集和测试集, 同时计算了 EER 的平均值和标准偏差和基于不同 FAR 的 GAR 的平均值, 使用了维度 $K = 256$ 和 $K = 1024$ 的二进制特征向量。总体来看多样本注册的 ROC 曲线趋势好于单样本注册, K=1024 的 ROC 曲线趋势劣于 K=256。但是(a)(c)中的 ROC 曲线相比于(b)(d)差距仍在合理的范围内, 这表明 BinaryFace 在单样本注册中依旧能够取得不错的可识别性; (c)(d)中的 ROC 曲线相比于(a)(b)差距同样在合理的范围内, 这表明在输出人脸特征向量的比特数增加为 4 倍后 BinaryFace 仍旧很好地保留了可识别性能。

如表 2 所示, 在 Color FERET 和 FEI 中, Binary 在单样本注册中都实现了 90%以上的可识别性能, 在多样本注册中都实现了 95%以上的可识别性能。但 Color FERET 的可识别性能相对较低, 主要原因为其有姿势, 光照, 年龄和遮挡变化等四种变化, 而 CMU-PIE 和 FEI 数据集仅有姿势和光照两种变化。

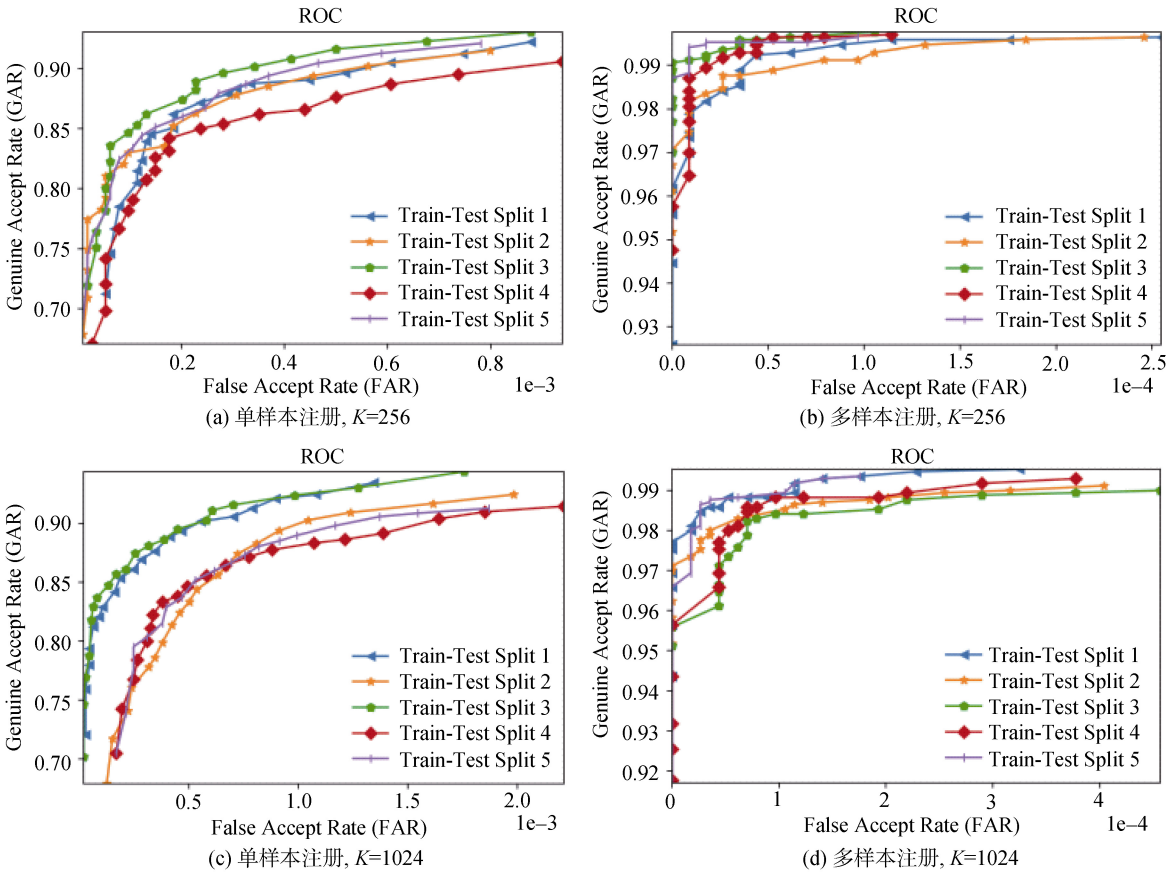


图 7 CMU-PIE 数据集上的 ROC 曲线

Figure 7 ROC curves on CMU-PIE dataset

如表 3 所示, 即使在 CMU-PIE 中进行单样本注册, BinaryFace 与 Hybrid[6]相比仍旧能得到较低的 4%EER(K = 256)和 3.6%EER(K = 1024), 同时在 GAR 上提升了约 1%。在 CMU-PIE 的多样本注册实验中, BinaryFace 在 GAR@FAR 和 EER 方面都优于之前的人脸模板保护方案[1, 6, 8], 当 K=1024 时, GAR 相比当前最优的 MEB Encoding[8]提升了约 6.5%, EER 则降低了约 4 倍。这表明 BinaryFace 在确保高安全性的情况下得到了更好的可识别性能, 降低了生物加密方案对可识别性能的影响。

表 2 CMU-PIE、FEI、Color FERET 的可识别性比较
Table 2 Comparison of Identifiability on CMU-PIE、FEI and Color FERET datasets

数据集	注册方式	*K*	GAR@FAR	EER (%)
CMU-PIE	单样本注册	256	91.81%@0.1%	4.00
		1024	91.24%@0.1%	3.60
	多样本注册	256	97.45%@0%	0.15
		1024	96.68%@0%	0.35
FEI	单样本注册	256	95.05%@0.1%	1.97
		1024	94.19%@0.1%	1.81
	多样本注册	256	97.24%@0%	0.16
		1024	98.27%@0%	0.20
Color FERET	单样本注册	256	85.45%@0.1%	5.50
		1024	80.92%@0.1%	6.67
	多样本注册	256	93.85%@0.01%	2.16
		1024	91.70%@0.01%	3.03

表 3 CMU-PIE 上不同算法的可识别性比较
Table 3 Comparison of different algorithms' identifiability on CMU-PIE dataset

算法	注册方式	*K*	GAR@FAR	EER (%)
Hybrid[11]	多样本注册	210	90.61%@1%	6.81
BDA[14]	多样本注册	76	96.38%@1%	4.58
MEB Encoding[17]	多样本注册	256	93.22%@0%	1.39
		1024	90.13%@0%	1.14
BinaryFace	单样本注册	256	91.81%@0.1%	4.00
		1024	91.24%@0.1%	3.60
	多样本注册	256	97.45%@0%	0.15
		1024	96.68%@0%	0.35

3.3 消除实验

如表 4 所示, 为探究模糊承诺方案对 BinaryFace 可识别性的影响, 本文针对不同的比特数做了一系列的对比实验。实验发现比特数对于场景 1 和场景 2 的 EER 和 Accuracy 几乎没有影响, 两个指标的变化范围很小, 因此可以确定比特数不会造成可识别性的降低; 场景 2 中的 EER 和 Accuracy 普遍低于场景都在 95%左右, 只有约 0.2%的损失。这表明 1, 但在 EER 上只有约 2%的损失, 而在 Accuracy 上 Binayface 在采用模糊承诺方案加强人脸模板保护方案的安全性时对可识别性的影响微乎其微, 做到了最大限度的保留。

表 4 模糊承诺对比实验
Table 4 Comparative experiment on Fuzzy Commitment

比特数	场景 1		场景 2	
	EER (%)	Accuracy (%)	EER (%)	Accuracy (%)
128	1.60	95.67	4.03	95.62
256	1.35	95.92	3.22	95.65
512	1.62	95.22	3.58	95.10
1024	1.38	95.81	3.30	95.66

(注: 在场景 1 中不采用模糊承诺, 在场景 2 中采用模糊承诺)

3.4 安全性分析

在场景 1 中, 由于未采用模糊承诺方案攻击者可以访问被盗的人脸模板和深度卷积神经网络模型, 攻击者将尝试生成攻击, 比如可能会使用大量的人脸集合进行字典攻击来利用系统的低 FAR, 这将可能恢复出部分的原始用户信息。在此攻击情形中, 人脸模板保护方案的 FAR 越低, 安全性越高。

在场景 2 中, 由于采用了模糊承诺方案攻击者只能访问被盗的人脸模板, 并且无法获取深度卷积神经网络模型, 因此其无法从被盗的人脸模板中提取出有关原始人脸二进制特征向量的任何信息, 这是由于密码哈希函数的单向性导致的。同时在模糊承诺方案中采用了安全的密码哈希函数(SHA3-512), 通过利用密码哈希函数的单向性进一步保障了人脸模板的安全性。因此, 在这种情况下只有暴力攻击才能破解人脸二进制特征向量。但是在这种攻击情形下的暴力攻击在计算上是不可行的, 因为对于 256 位和 1024 位二进制特征向量, 搜索空间将是 2 的 256 次方和 2 的 1024 次方。所以 BinaryFace 在采取模糊承诺方案后, 攻击者几乎不可能从被盗的人脸模板中获取到任何原始的用户人脸信息, 从而保护了用户的隐私信息。

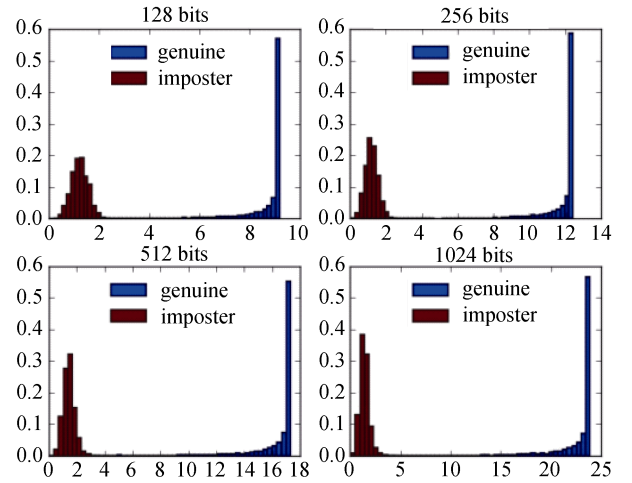
3.5 运行开销

如图 3 所示, 人脸模板保护方案主要由预处理、特征转换和生物加密等组成, 方案的运行开销主要由预处理和特征转换两部分组成, 生物加密部分可忽略不计。在预处理方面, 方案采用 MTCNN 网络替代了传统的 dlib 算法, 其可同时实现人脸检测和人脸对齐功能。如表 5 所示, 在处理一张 224×224 的图片时, MTCNN 在 CPU 和 GPU 上的耗时相比 dlib 均减少了 50%。当图片数量级较大时, 新的检测算法将极大地减少方案的时间开销; 在特征转换方面, 方案对模型中的部分卷积层进行了轻量化设计。如表 1 所示, BinaryFace 相比 VGGFace 在参数(代表模型大小, 即空间开销)上减少了约 75%, 同时在浮点数(代表计算量, 即时间开销)上减少了约 35%。综上所述, 由于方案在空间和时间上的开销都有较大的改善, 因此极大地提升了方案在实际部署时的运行效率。

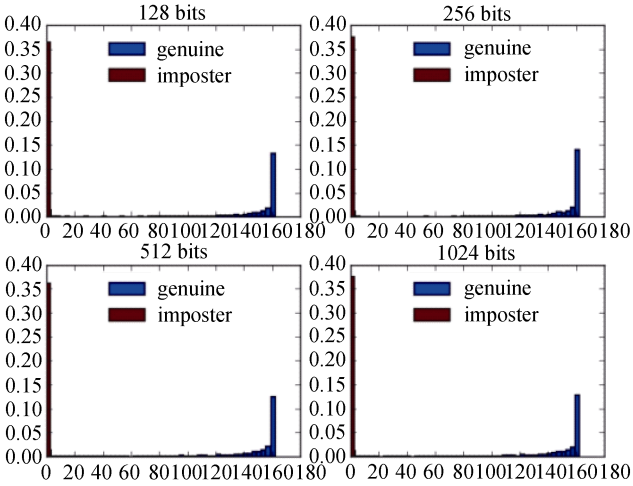
表 5 dlib 和 MTCNN 处理每张图片的耗时比较

Table 5 Time-consuming comparison of dlib and MTCNN on processing each picture

检测算法	图像尺寸	CPU 耗时(ms)	GPU 耗时(ms)
dlib	224*224	92.2	9.3
MTCNN	224*224	45.7	4.6



(a) 场景1-不采用模糊承诺方案



(b) 场景2-采用模糊承诺方案

图 8 不同场景下的真实者和冒名者的统计分布

Figure 8 Statistic distribution of real and imposters in different scenarios

为了更好地评估人脸模板的安全性, 本文对深度卷积神经网络模型 BinaryFace(多样本注册且 K=1024)实施字典攻击后研究了真实者(genuine)和冒名者(imposter)的匹配分数分布。如图 8 所示, 所有图像的纵轴代表频次占比, 横轴表示匹配分数。在(a)中虽然四幅图的比特数不同, 但能看出冒名者匹配分数的分布范围都比较大且与真实者的匹配分数分布之间的距离较小, 两者之间没有很好地分离, 说明模型的安全性能不佳; 而在(b)中冒名者的匹配分数几乎都分布在 0 左右且与真实者的匹配分数分布之间的距离较大, 两者之间得到了很好的分离。这表明 BinaryFace 在采用模糊承诺方案后能够很好地拒绝冒名者的非法访问, 接受真实者的正常访问。

4 总结

本文基于深层卷积神经网络提出一种轻量化且可识别性强的人脸二进制模板转换网络 BinaryFace, 其可以实现特征提取和随机正交映射模块的端到端训练。在通过模糊承诺方案保障人脸模板高度安全性的同时, BinaryFace 与相关人脸模板保护方案相比在 GAR 上有约 6.5%的提升, 同时将 EER 降低了约 4 倍。未来在人脸模板保护方面仍需解决人脸伪造中的对抗攻击, 同时为了进一步保护用户的隐私, 增强登录数据库的安全性, 将考虑对多种生物模板进行融合, 例如指纹、虹膜、声音、步态等。

参考文献

[1] Thomaz C E, Giraldi G A. A New Ranking Method for Principal Components Analysis and Its Application to Face Image Analysis[J]. *Image and Vision Computing*, 2010, 28(6): 902-913.

[2] Jain A K, Nandakumar K, Nagar A. Biometric Template Security[J]. *EURASIP Journal on Advances in Signal Processing*, 2008, 2008(1): 579416.

[3] Rathgeb C, Uhl A. A Survey on Biometric Cryptosystems and Cancelable Biometrics[J]. *EURASIP Journal on Information Security*, 2011, 2011(1): 1-25.

[4] Patel V M, Ratha N K, Chellappa R. Cancelable Biometrics: A Review[J]. *IEEE Signal Processing Magazine*, 2015, 32(5): 54-65.

[5] Zhang N, Zang Y L, Tian J. The Integration of Biometrics and Cryptography—a New Solution for Secure Identity Authentication[J]. *Journal of Cryptologic Research*, 2015, 2(2): 159-176.
(张宁, 臧亚丽, 田捷. 生物特征与密码技术的融合——一种新的安全身份认证方案[J]. 密码学报, 2015, 2(2): 159-176.)

[6] Fang S X, Zhang L W, Wang H L. Research on the Development Trend of Identity Authentication Technology Based on Face Biometrics[J]. *Journal of Information Security Research*, 2017, 3(6): 533-537.
(方淑仙, 张立武, 王惠莅. 基于人脸生物特征的身份鉴别技术发展趋势研究[J]. 信息安全研究, 2017, 3(6): 533-537.)

[7] Juels A, Wattenberg M. A Fuzzy Commitment Scheme[C]. *the 6th ACM conference on Computer and communications security*, 1999: 23-34.

[8] Juels A, Sudan M. A Fuzzy Vault Scheme[J]. *Designs, Codes and Cryptography*, 2006, 38(2): 237-257.

[9] Ratha N K, Chikkerur S, Connell J H, et al. Generating Cancelable

Fingerprint Templates[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007, 29(4): 561-572.

[10] Teoh, Andrew BJ, Alwyn Goh, David CL Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2006, 28(12): 1892-1901.

[11] Feng Y C, Yuen P C, Jain A K. A Hybrid Approach for Generating Secure and Discriminating Face Template[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(1): 103-117.

[12] Schroff, Florian, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering[C]. *the IEEE conference on computer vision and pattern recognition*, 2015: 815-823.

[13] Parkhi, Omkar M., Andrea Vedaldi, and Andrew Zisserman. Deep face recognition. *bmvc*. Vol. 1. No. 3. 2015.

[14] Feng Y C, Yuen P C. Binary Discriminant Analysis for Generating Binary Face Template[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(2): 613-624.[LinkOut]

[15] Erin Liong, Venice, et al. Deep hashing for compact binary codes learning[C]. *the IEEE conference on computer vision and pattern recognition*, 2015: 2475-2483.

[16] Pandey, Rohit K., and Venu Govindaraju. Secure face template generation via local region hashing[C]. *2015 international conference on biometrics (ICB)*. IEEE, 2015: 299-304.

[17] Pandey, Rohit Kumar, et al. Deep secure encoding for face template protection[C]. *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, 2016: 77-83.

[18] Hassner, Tal, et al. Pooling faces: Template based face recognition with pooled face images[C]. *the IEEE Conference on Computer Vision and Pattern Recognition Workshops,* 2016: 59-67.

[19] Bodla, Navaneeth, et al. Deep heterogeneous feature fusion for template-based face recognition[C]. *2017 IEEE winter conference on applications of computer vision (WACV)*. IEEE, 2017: 586-595.

[20] Talreja, Veeru, Matthew C. Valenti, and Nasser M. Nasrabadi. Multibiometric secure system based on deep learning[C]. *2017 IEEE Global conference on signal and information processing (globalSIP)*. IEEE, 2017: 298-302.

[21] Sim, Terence, Simon Baker, and Maan Bsat. The CMU pose, illumination, and expression (PIE) database[C]. *Proceedings of Fifth IEEE International Conference on Automatic Face Gesture Recognition*. IEEE, 2002: 53-58.

[22] Phillips P J, Wechsler H, Huang J, et al. The FERET Database and Evaluation Procedure for Face-recognition Algorithms[J]. *Image and Vision Computing*, 1998, 16(5): 295-306.

[23] Simonyan K, Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition[EB/OL]. 2014: arXiv:1409.1556[cs.CV]. https://arxiv.org/abs/1409.1556.

[24] He, Kaiming. Deep residual learning for image recognition[C]. *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016: 770-778.

[25] Howard A G, Zhu M L, Chen B, et al. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications[EB/OL]. 2017: arXiv:1704.04861[cs.CV]. https://arxiv.org/abs/1704.04861.

[26] Teoh A B J, Goh A, Ngo D C L. Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2006, 28(12): 1892-1901.

[27] Al-Assam, Hisham, Harin Sellahewa, Sabah Jassim. A lightweight approach for biometric template protection[J]. *Mobile Multimedia/Image Processing, Security, and Applications*. 2009, (7351): 258-261.

[28] Zhang K P, Zhang Z P, Li Z F, et al. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks[J]. *IEEE Signal Processing Letters*, 2016, 23(10): 1499-1503.

[29] Cao, Qiong. Vggface2: A dataset for recognising faces across pose and age[C]. *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018)*. IEEE, 2018: 67-74.

赵铖辉 于 2017 年在杭州电子科技大学通信工程专业获得学士学位。现在北京交通大学信息与系统专业攻读硕士学位。研究领域为计算机视觉。研究兴趣包括: 目标检测、人脸识别。Email: 17120177@bjtu.edu.cn

李勇 于 2007 年在中国科学院研究生院获得博士学位。现任北京交通大学电子信息工程学院副教授。研究领域为网络空间安全。研究兴趣包括: 云数据安全与隐私保护、区块链安全、应用密码学。Email: liyong@bjtu.edu.cn

张振江 于 2008 年在北京交通大学通信与信息系统专业获得博士学位。现任北京交通大学电子信息工程学院教授。研究领域为通信与信息系统。研究兴趣包括: 身份认证、边缘计算。 Email: Zhangzhenjiang@bjtu.edu.cn