 DOI: https://doi.org/10.26549/bdai.v3i4.11953

The Design and Implementation of a Face Recognition Security Mechanism Optimization

Zhengdao Zhang

Shenzhen Xingguang Core Imaging Technology Co., Ltd., Shenzhen, Guangdong, 518000, China

Abstract

With the rapid development of computer technology, face recognition technology is gradually mature, has been widely used in various fields. Face recognition technology is characterized by high accuracy, high efficiency and easy to use, and is widely used in the field of public safety. However, due to the variety of human face image collection methods in the network environment, which are greatly affected by the outside world, the traditional face recognition methods are used by many unsafe factors. In view of the above problems, this paper proposes an improved face recognition security mechanism, to realize the security framework of algorithm optimization based on image feature information, and to optimize the algorithm use for specific application scenarios. The experimental results show that the improved security algorithm can effectively solve the problem of users' personal facial feature information leakage in the network, and ensure that the face recognition system can be well solved in the security. Finally, this model has a good theoretical and application effect through simulation.

Keywords

face recognition; security mechanism; optimization and improvement

一种人脸识别安全机制优化的设计与实现

张正道

深圳市星光芯影像科技有限公司，中国·广东 深圳 518000

摘　要

随着计算机技术的飞速发展，人脸识别技术逐渐成熟，已广泛应用于各领域。人脸识别技术具有精准度高、高效易用等特点，在公共安全领域中有着广泛的应用。由于网络环境下人体脸部图像采集方法多样，受外界影响大，传统的人脸识别方法存在很多不安全因素而被使用的案例。针对以上问题，论文提出一种改进的人脸识别安全机制，实现基于图像特征信息进行算法优化的安全框架，同时针对特定应用场景下优化算法使用。实验结果表明改进后的安全算法能有效解决网络中用户个人面部特征信息泄露问题，保证了人脸识别系统在安全性上得到很好解决。最后通过仿真验证此模型具有很好的理论和应用效果。

关键词

人脸识别；安全机制；优化改进

1 引言

论文结合自身的研究成果，在人脸识别安全机制优化方面给出了以下结论：第一，论文提出的人脸识别安全机制优化体系中，通过设置合理实验步骤对安全性模型进行建模，并进行验证。实验中通过对实验数据分析表明各项安全机制均符合标准要求。第二，论文提出的理论模型在实际业务中得到验证，结果良好 [1]。论文基于自研算法从实际应用中提出了多项改进措施以及对当前核心安全机制的修复情况，并针对实际问题给出了相应改进意见及建议。由于人脸识别涉及采集过程、认证过程等多个环节，各环节相互关联且环环相扣，因此任何环节出问题都会影响到整个系统。因此，论文从系统结构上对人脸识别安全机制优化过程中主要面临的安全问题提出了对应处理策略及流程。最后给出具体改进建议 [2]。

2 人脸识别技术概述

人脸是一种人体器官，人的五官结构复杂，面部表情变化很大，识别困难，因此在识别过程中会涉及一些计算模型。人脸识别的计算模型主要分为两类：一类是静态模型，另一类是动态模型。在静态模型中，人脸的位置和光照都不是固定不变的，它会受到周围环境的影响从而发生变化 [3]。在动态模型中，图像中会包含很多图像信息，在其中包括人脸图像上的所有像素。

2.1 特征提取

人脸特征提取是识别中最基础，也是最关键的一个环

【作者简介】张正道（1991–），男，彝族，中国云南宣威人，本科，高级工程师，从事Camera技术开发研究。

节。通常需要通过三个步骤：①选择像素，这里的像素可以代表人脸特征。②提取原始脸部图像上各个像素点之间的像素值和距离值，这是整个人脸识别的基础。③对人脸进行量化后计算特征值，用于确定人脸识别模型的分类标准 [4]。④在识别过程中利用 RGB 颜色空间分析方法将人脸图像中颜色变化幅度最大的区域进行分类，并计算出每个区域颜色变化系数的平均值。

2.2 识别模型

基于图像相似度，人脸特征提取是人脸识别过程中非常重要的一步。人脸图像在被识别的过程中会受到人脸周围环境因素的影响，如光照、人脸表情等 [5]。为了提高人脸识别的准确性，人脸识别技术应用了多种分类方法。同时为了降低错误率，提高识别的准确率，对于不同分类方法应用于人脸识别系统有不同的实现方案。

2.3 数据预处理

对采集到的数据进行预处理，包括像素点偏移、光照情况的改变，以保证用户端不会受到脸部姿势和光线变化带来的影响，保证能及时准确地获取到用户面部信息。同时对原始图像中所有像素进行了分割，使得图片更加具有细节。同时将脸部特征进行提取，例如面部特征的灰度色调值、人脸轮廓参数值等不同的属性值，并分别以数值形式输出。通过预处理后数据能够保证用户终端在使用时拥有更好的精确度。本方法设计了一种基于人脸特征参数的阈值生成机制，即在识别到特定脸型后会自动触发一系列条件（如年龄、性别、肤色等）使模型更加精准，并且自动将初始数据保存成标准算法中最优序列并生成合适的提取条件集。

3 现有安全机制

由于人脸的生物特征是唯一且动态的，传统的人脸识别技术往往通过采集一张人脸图片来实现用户的身份认证，从而实现人脸样本采集后对用户身份真实性的判断。在静态图片采集环节，大多数情况下会通过用户名与密码等信息来获取用户信息。而在采集完成后，用户身份会被随机提取至验证码窗口并获取用户信息，此时用户身份会因验证码权限过低而无法得到安全认证。一旦验证码失效，用户身份就会受到威胁。另外由于验证码仅供验证码窗口所用，当用户身份信息被泄露时验证码窗口无法正常打开，导致验证码失效，影响用户身份安全。

3.1 静态图片采集模式

静态图片采集模式是人脸识别技术在人脸采集过程中所采用的一种方式，它能够为图片获取提供条件。为了保证用户身份真实性，静态图片采集模式需要在上传静态图片之前先生成动态图片，然后再在生成动态图片后对静态图片中的数据进行特征提取并对其身份信息进行分析。在识别过程中由于静态图片采集时数据往往都是静止的，因此可以对采集完成图和生成的静态图片进行分析比对；在生成静态图片时可先对静态图片进行特征提取，然后通过特征提取结果判断用户身份。目前主流方法包括 PIN 码采集与 JPEG 图像采集。PIN 码中只有数字字符串作为参考格式，所以在提取和判断用户身份时需要通过字符串来判断输入用户信息的有效性，但不需要计算用户数据等其他参数，大大降低了用户身份隐私受到威胁的风险。

3.2 人脸表情提取

为了实现人脸的动态识别，需采用人脸表情来提取人脸表情信息。人脸表情特征是人脸中最重要的特征之一，它与人脸图像中人物的面部表情具有相似度。因此可以利用这种特征来分析人脸特征，提取人脸表情特征信息。

4 算法选择与实现

根据以上对基于人脸识别技术设计方案的安全原理与安全机制优化原理，我们首先要明确论文的安全机制是如何实现人脸识别技术，且对这种安全机制进行优化和完善。一是必须考虑安全的安全性。二是必须满足技术能力和安全性指标。三是对现有安全机制做出一些修补措施防止应用系统被攻击损害或信息丢失造成损失。目前可以接受的情况主要有以下几种：①传统人脸数据库中人脸特征数据存储方式不透明，不能及时获取到被他人浏览过或者获取方式不正确等原因造成数据泄露而无法用于识别。且这些问题会造成一些新的不稳定因素进而影响人脸识别应用。例如，在医疗场景中，人脸一般分为三类：一是完全不可见的人脸；二是面部皱纹等较难识别的人脸；三是皮肤皱褶等非常细小的特征。在目前人脸识别技术中较为常见的算法包括二值图像搜索算法、特征提取方法、人脸模板匹配等。算法性能及精度是确定人脸识别算法模型设计指标之一。目前中国采用最多的是二分类算法、梯度法、基于卷积神经网络算法等。论文采用自研图像分割方法自动进行人脸数据处理，获得不同人脸的生物特征，如人脸颜色变化、轮廓变化或人像轮廓改变等。并对其进行算法优化得到一个高效识别模型即人脸识别方案。论文采用了一种基于序列的算法方法来解决用户个体与终端个体之间匹配程度不一致的问题，论文选择其中一个关键环节——数据预处理 [6]。首先，选取数据预处理时常用的特征提取算法来辅助进行人脸识别；其次，对不同特征数据做一次二分类统计，计算分类精度，然后将用户身份信息（包括姓名、性别、年龄、出生日期等）进行编码处理和统计；最后，对训练好的模型进行训练并评估其性能。

4.1 分类的优化

分类的本质是从样本中提取有用信息，并通过二维特征将这些信息进行转化。针对这种二维特征，论文选用特征二分类算法。在具体算法中，先用最小化一次输入值代替最小二乘处理得到的标签：其中 m 为用户身份信息个数；n=n*n(n+1) 为输入的有效特征数量；[M(t)1] 为验证模型准确率。

4.2 特征统计

特征数据的统计是为了消除不同特征之间不必要的区分，同时也是人脸识别的必要步骤之一。在预处理阶段的基础上，利用最大似然原则进行人脸识别特征的统计，利用二值化理论对各个像素点的识别强度进行计算。利用最大似然原则将不同像素点都进行了二值化处理。采用上述方法将每一个像素点的识别强度值划分成不同等级，并用相应的二值化处理结果来表示人脸与人的相似程度。

5 系统流程设计与测试

我们采用的身份认证方式主要包括以下几个步骤：①用户的手机终端或摄像头采集用户脸图像；②摄像头扫描并选择目标类型；③通过图像预处理模块采集人脸特征信息并进行预处理；④在人脸特征采集完成后通过图像与数据库交互获取该人脸信息，为后续数据处理打下基础。身份认证方式：采用人脸身份认证证书 + 终端密码 / 指纹认证 / 人脸识别两种方式。

目前主要有两种主要方法，如指纹认证、面部识别等。由于人脸不具有唯一性，其识别成功率很低，主要原因是识别方法中存在错误与不安全因素，论文将主要介绍以下两种识别方式：①人脸不确定：该方法可能产生误判，需要重新匹配。②人脸特征丢失后需要恢复。需要针对每张人脸特征提取和判断，才能获取人脸信息。在没有进行人脸处理的情况下可直接使用图像识别算法判断人脸匹配程度来判断脸部特征是否一致。身份认证方式：在实际应用中最常用到基于人脸识别建立二次验证方法来证明你是否已经正确。如果通过二次验证失败就无法使用人脸检测设备采集人脸 。对图像进行预处理：采用低通滤波技术、卷积神经网络等技术提取人脸图像中人脸特征信息。基于特征提取技术能更好地反映用户特征，进一步提升识别精度与效率。同时为提高其安全性和稳定性在提高了对人脸识别效率同时避免了恶意攻击的风险；同时也提高了人脸识别系统应用安全性和便捷性。目前市场上已有许多方案可选：如虹膜认证、密码注册登录、人脸识别功能等，论文主要介绍基于自研人脸指纹 ID 和人脸比对算法模型进行 。

6 结语

论文主要是对人脸识别安全机制模型的深入分析，为应用领域提供参考。随着人工智能概念的普及，越来越多的人开始用人工智能进行工作。同时对于个人隐私泄露问题也越来越重视。近年来，基于人脸识别技术的移动支付功能得到了广泛落地，越来越多的企业开始将人脸识别技术应用于金融行业。本案例中，我们考虑到当前一些应用的安全性问题和设计不足之处才提出了相应的优化方案，同时我们也会继续与研究人员积极讨论和解决目前出现问题。确保每一个过程都是安全与便捷的。最终实现平台级功能，用户无需打开任何 APP 进行身份验证即可直接使用。安全机制的设计能有效提高系统设计质量并且在实际工作中将起到很大的作用。

参考文献

[1] 张文杰.人脸识别嵌入政务服务的个人信息安全风险及规避[J].科技传播,2022,14(18):139-142.

[2] 韩旭至.刷脸的法律治理:由身份识别到识别分析[J].东方法学,2021(5):69-79.

[3] 龙澍地.人脸识别技术应用的法律规制研究[J].法制与社会,2021(23):5-7.

[4] 金贤和.面向社区门禁管理的人脸识别应用研究[D].上海:东华大学,2021.

[5] 刘志勇.基于卷积神经网络的人脸活体检测方法研究[D].济南:齐鲁工业大学,2021.

[6] 王曼曼.基于生成式对抗网络的人脸属性识别对抗攻击研究[D].江苏:东南大学,2021.