**2021年全国大学生信息安全竞赛**

**作品报告**

**作品名称： 基于人脸动态表情识别的身份认证方法**

**电子邮箱： 1561739463@qq.com**

**提交日期： 2021.6.6**

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。

**目 录**

[摘要 1](#_Toc33965493)

[第一章 作品概述 3](#_Toc33965494)

1.1背景介绍................................................................................................................................................3

1.2作品简介................................................................................................................................................4

1.2.1人脸动态表情验证.....................................................................................................................4

1.2.2图像加密与情绪分析.................................................................................................................5

1.3作品特点................................................................................................................................................5

1.4作品前景................................................................................................................................................6

[第二章 作品设计与实现 7](#_Toc33965495)

2.1总体设计................................................................................................................................................7

2.2.1系统方案.....................................................................................................................................7

2.2作品原理................................................................................................................................................8

2.2.1动态人脸识别.............................................................................................................................8

2.2.1.1Haar特征级联分类器......................................................................................................8

2.2.1.2直方图均衡化..................................................................................................................9

2.2.1.3基于深度残差网络的人脸对齐与特征采点................................................................11

2.2.1.4基于DT算法人脸动态表情信息采集..........................................................................14

2.2.1.5基于DTW算法的动态表情匹配.......................................................................................15

2.2.2图像加密...................................................................................................................................16

2.2.3情绪识别...................................................................................................................................17

2.3核心功能的具体实现..........................................................................................................................19

2.3.1人脸识别功能...........................................................................................................................19

2.3.2动态表情信息采集与匹配.......................................................................................................21

2.3.2.1动态表情信息采集........................................................................................................22

2.3.2.2动态表情信息匹配........................................................................................................23

[第三章 作品测试与分析........................................2](#_Toc33965496)7

3.1作品测试说明......................................................................................................................................27

3.2.1动态表情匹配功能测试...........................................................................................................27

3.2.2图像加密功能测试...................................................................................................................31

3.2.3情绪识别功能测试...................................................................................................................31

[第四章 创新性说明............................................33](#_Toc33965497)

4.1基于人脸动态表情特征的身份认证系统............................................33

4.2基于密集轨迹(DT)算法的表情抽象化..............................................33

4.3完美解决了特殊场景下的安全问题................................................33

[第五章 总结 3](#_Toc33965498)4

[参考文献 3](#_Toc33965499)6

# 摘要

近年来，随着人工智能在计算机视觉方向的飞速发展，人脸识别技术已经应用到我们生活的方方面面。从宿舍门禁，到移动支付，人脸识别的快捷高效给我们的生活带来了极大的便利。但是与此同时，也有不少专门破解人脸识别的技术出现，在可见的未来，针对人脸这一信息媒介进行的攻防博弈还会越来越多，增强人脸识别的安全性这一任务是紧急的。

当前的人脸识别技术，通常只是通过比对静态的人脸图像来确定用户身份。这种方法可以说是“防君子不防小人”，若被有心之人拍下了其他合法用户的照片再打印出来，就能轻松破解掉这类人脸识别系统，其便捷性虽然很高但安全性堪忧。稍先进一些的人脸识别技术能够探测到五官距离摄像头位置的差异，从而判断面前的是立体人脸还是平面人脸，但随着3D打印技术的发展，打印人脸模型不再是一件难事。在涉及到财产安全的时候，大部分人脸识别技术会要求进行活体检测，如“眨眨眼”、“张张嘴”等。这种人脸识别技术也并不是无懈可击的，双胞胎之间也有很大的机会可以彼此破解对方的账户。

基于以上，我们设想了一种新的基于人脸识别的身份认证系统，即要求用户做出一定的面部表情，以做表情的过程作为其身份认证的密码。正如人人都知道，账户密码由键盘上的某些字符组成却仍然难以破译，人脸动态表情识别也能做到，即使面部信息被不法分子完全掌握也仍然无法破解。我们首先利用opencv中的Haar特征级联分类器，实现了传统静态人脸识别功能。在此基础上利用dlib模型完成人脸面部采点，参考密集轨迹（DT）算法记录人脸各区域在动作时的变化信息。面部动作验证的过程中，利用感知哈希算法确保人脸基本信息不变的基础上，使用动态时间规整的曲线匹配（DTW）算法进行面部动作匹配。与预先设定的动作表情匹配成功后，结合情绪分析判定对应的权限，最终反馈给用户。同时，我们在此基础上对保存在本地的人脸信息进行加密，确保他人无法从我们的人脸数据库得到任何有效的人脸信息，从而实现从前端到后端的双重安全保障。

本作品的特点是具有超强的安全性和广泛的应用性。

本作品的创新点在于实现了高度防伪的基于人脸动态表情特征的身份认证系统，以及结合情绪分析完美解决了特殊场景下的安全问题。

**关键词：**人脸识别、表情密码、活体检测、opencv、dlib模型、DT算法、感知哈希算法、DTW算法、情绪分析

# 第一章 作品概述

**1.1背景介绍**

随着计算机技术的创新和发展，人脸识别技术已经成为一种潮流热门的AI技术。日常生活中利用人脸识别技术的“刷脸”解锁、“刷脸”支付、“刷脸”签到等，为人们生活带来了极大的便利。于此同时，其运用范围也越来越广，逐渐深入到了我们生活的各个角落。

人脸识别分为静态识别和动态识别，静态人脸识别是运用得最为广泛的，它只对人的面部特征进行判定，确保长相一致即通过验证。而传统的动态识别则是在静态识别的基础上增加了活体检测，要求用户“眨眨眼”、“张张嘴”等，安全性较高。

但是实际上，目前传统动态人脸识别仍然存在明显的缺陷，如新闻曾经报导，一对双胞胎姐妹能够轻松利用人脸识别通过对方的手机的身份验证，甚至还能顺利地使用对方地支付宝人脸支付。人脸信息作为一个**不可变**的特征，其安全性存在天然缺陷。

诚然，在一般不涉及到资金交易的人脸识别场景，比如酒店登记、宿舍门禁等场合，人脸信息数据量巨大，安全程度要求相对较低，验证速度和便携性要求较高，传统的人脸识别技术已经可以很好的满足需求。但是涉及到资金交易的银行金融业务等，目前无论是传统的静态人脸识别还是动态人脸识别的安全性都不能满足需求。

针对这一问题，我们的项目立足于增强支付环境下的安全性，提出了自定义的**人脸动态表情匹配**系统的理念。即用户可以自己设计面部动作作为动态表情密码，进行身份识别时必须完成自定义动作才可以通过验证。并且可以针对不同场合设计多个动作，比如当遇到特殊危险被胁迫验证的时候，只要做某个自定义的动作，账户就会锁死。自定义交互式动作活体检测可以面向更多的场景进行应用，也解决了非法用户利用数字人脸图片或模型骗过识别系统等安全问题。在此基础上，我们增加了情绪分析功能，针对日常生活中可能出现的冲动消费、被诈骗现象，当用户处于恐慌、愤怒、激动等情绪下时，系统会对其支付行为进行二次验证。

为减少计算量，项目只提取部分人脸特征进行运算，比如眼睛、鼻子、眉毛等五官的图像信息，并且对于存储的用户的人脸信息进行算法加密。这种验证友好型的人脸存储方式不仅可以满足确认个人身份的识别功能，也能够加快识别的速度，减小系统负担。

**1.2作品简介**

我们的作品将传统的人脸识别、活体检测、自定义密码进行融合，实现了通过识别人脸动态表情的方式对用户身份进行判断的功能。在此基础上设置了双重身份机制，即同一个用户可以通过不同的表情获取不同权限。此外，本作品提供了情绪检测的功能，能够判断用户在人脸识别的过程中的情绪状态。

本作品在本质上提高了安全性的同时，牺牲了一部分便捷性，适合被使用在支付系统、安保系统中。

**1.2.1人脸动态表情验证**

人脸动态表情验证是本作品最核心的功能，它允许用户在摄像头前做出一个变化的表情，如大笑、嘟嘴、挤眉弄眼等等，作为之后验证的密码，实现过程简要介绍如下：

1. 利用opencv中的Haar特征级联分类器，完成传统静态人脸识别功能的实现。
2. 利用dlib模型完成面部采点，结合DT算法记录人脸各区域在动作时的变化信息。
3. 面部动作识别过程中，在利用感知哈希算法确保人脸基本信息不变的基础上，利用动态时间规整的曲线匹配算法进行动作匹配。
4. 与预先设定的动作表情匹配成功后，判定对应的权限，反馈给用户。

**1.2.2图像加密与情绪分析**

作品的第二部分是基于人脸动态表情识别的应用环境下的特色性开发。

由于人脸识别不可避免的要采集客户的面部信息，我们依据AES算法设计了针对图像的加密算法，使本地的用户照片以雪花图的形式保存。

在面部识别的过程中，作品会对用户进行情绪分析，针对恐惧、愤怒、惊慌等异常情绪进行特殊处理。

**1.3作品特点**

1、更强的安全性

本作品能够有效防御包括“人脸照片”、“脸部模型”“人脸视频”等能够破解传统人脸识别系统的攻击手段。能够大大增强在进行支付，或其他对身份验证的安全性要求很高的活动时，使用人脸识别验证的安全性、可靠性。

2、广泛的应用性

当前，使用人脸识别作为验证系统、门禁系统的地方已经越来越多了，这也证明了我们的项目具有广泛的应用场景。在当前环境下，许多需要严密认证用户信息的场景，如支付过程、读取私密文件等等，都可以运用到我们的技术。

**1.4作品前景**

随着时代的发展，由于面部识别的便利性，其运用必然会越来越广。而社会对人脸识别的依赖程度的提高，可能会导致有不法分子试图以其为攻破口，进行非法行为。也因此，未来大家对于人脸识别的安全性需求必然会逐渐提高，故而本作品绝对不会缺乏用武之地。

同时，当前对于人脸识别的运用场景上还是单薄的，一般仅仅将其作为身份验证技术。我们的项目创新性地将人脸识别与情绪分析相结合，除了能验证用户身份外，还能获取其当前情绪状态，结合当下场景给出反馈，这种互动式的验证手段，大大增加了人脸识别的可玩性，未来具有巨大的开发空间。

# 作品设计与实现

**2.1总体设计**

作品的实现包含三个部分：第一部分是获取人脸信息、第二部分是动态表情识别、第三部分是图像加密与情绪分析。

获取人脸信息部分实现了：采集用户人脸图像、人脸识别功能。

动态表情识别部分实现了：采集用户自定义的表情动作并按部位转化为密码、动态表情密码的匹配。

情绪分析部分实现了：识别用户情绪以及获取当前场景，程序会基于此做出多样性反馈。

**2.1.1系统方案**

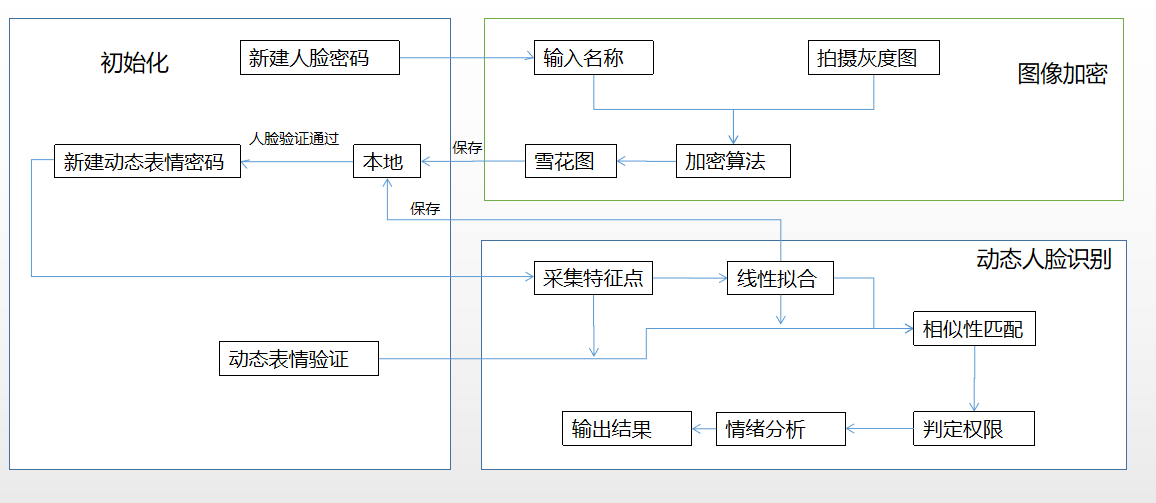


图2-1 程序功能流程图

运行流程概括如下：

1.对于新用户，首先自定义用户名称，之后程序会调用摄像头完成人脸数据的采集。

2.程序自动完成人脸模型训练，图像信息会经加密算法被转化为雪花图并保存到本地。

3.选择导入动态表情密码。经过身份核验后，合法的用户被允许导入动态表情密码。程序会以一定时间间隔自动定位并采集用户面部的若干关键区域信息，并分析各部位的变化趋势，进而转化为表情密码。

4.情绪分析。程序会基于用户表情特征分析出用户情绪，可用以帮助控制冲动消费、预防用户被胁迫、被诈骗等特殊情况。

**2.2作品原理**

以下对人脸动态表情识别、图像加密以及情绪分析三部分功能的实现原理进行分析。其中人脸动态表情识别的实现过程包含人脸识别、表情动作记录、表情动作匹配三部分。

**2.2.1动态人脸识别**

作品的第一部分是实现人脸动态表情识别功能。它避免了传统模式下静态人脸识别易被攻破的缺陷。这部分主要运用了opencv下Haar特征的级联分类器、直方图均衡化、dlib面部特征采点、DT算法、对离散点的线性回归和DTW算法。

**2.2.1.1Haar特征级联分类器**

Haar-like features是用于物体识别的一种数字图像特征。它是第一种即时的人脸检测算子，通常用于人脸检测。

  哈尔特征通过检测窗口中指定位置的相邻矩形，计算每一个矩形的像素和并取其差值。然后用这些差值来对图像的子区域进行分类。在检测阶段，一个与目标物体同样尺寸的检测窗口将在输入图像上滑动，在图像的每一个区域都计算一个Harr特征。这些差值会与一个预先计算好的阈值进行比较，将目标与非目标区分开来。因为这样的一个Harr特征是一个弱分类器，为了达到一个可信的判断，就需要一大群这样的特征，并将这些特征组合成一个级联分类器，最终形成一个强分类器。

  哈尔特征最主要的优势是它的计算非常快速。使用积分图结构，任意尺寸的哈尔特征可以在常数时间内进行计算。

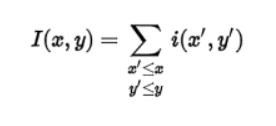


图2-2 积分图公式

对于每一点（x，y），积分图公式会求出这个点对应左下角区域所有值的和，因此只需要遍历一遍图像就可得到完整积分图。对于任意一点(x,y) 积分图可通过计算 I(x,y)= i(x,y)+I(x-1,y)+I(x,y-1)-I(x-1,y-1)得到。利用积分图就可以很高效的计算出图像中的特征区域。

由此，便可以找到到图像中包含人脸的区域。

**2.2.1.2直方图均衡化**

将获取的面部照片转化为灰度图后，要统一进行直方图均衡化处理。直方图是表示数字图像中每一灰度出现频率的统计关系。它能给出图像灰度范围、每个灰度的频度和灰度的分布、整幅图像的平均明暗和对比度等概貌性描述。灰度直方图是灰度级的函数, 反映的是图像中具有该灰度级像素的个数, 其横坐标是灰度级, 纵坐标是该灰度级出现的频率( 即像素的个数), 整个坐标系描述的是图像灰度级的分布情况, 由此可以看出图像的灰度分布特性, 即若大部分像素集中在低灰度区域, 图像呈现暗的特性; 若像素集中在高灰度区域, 图像呈现亮的特性。

直方图均衡化的本质是对图像进行非线性拉伸,并且重新分配图像的象元值,使一定灰度范围内象元值的数量大致相等。最终效果是使得直方图的峰顶部分对比度得到增强,而两侧的谷底部分对比度降低,处理后输出图像的直方图是一个较平缓的分段直方图。

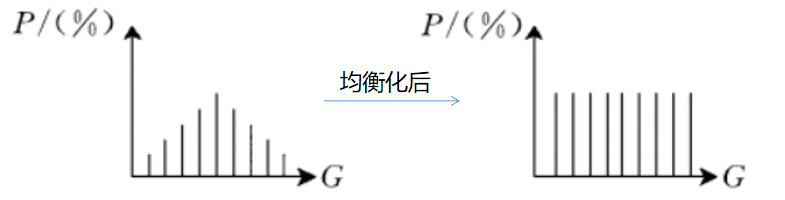


图2-3均衡化示意图

 直方均衡化后——》 

**2.2.1.3基于深度残差网络的人脸对齐与特征采点**

人脸对齐就是在已经检测到的人脸的基础上，自动找到人脸上的眼睛鼻子嘴和脸轮廓等标志性特征位置。我们通过级联的残差回归树（GBDT）实现，目的是在已知的人脸方框上定位其准确形状，并按照一定间隔进行采点。

残差网络（ResNet)属于深度神经网络模块，对于一个堆积层结构（几层堆积而成）当输入为x时其学习到的特征为H(x) ，我们希望其可以学习到残差 F(x) = H(x) - x。残差学习的结构如图2-4所示，是一种短路连接。

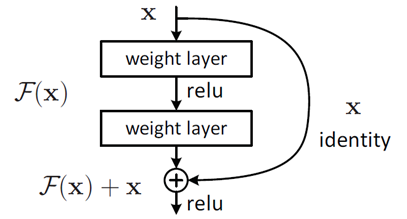


图2-4 残差学习单元

目前人脸对齐的算法主要分为两大类：基于优化的方法（Optimization-based method）和基于回归的方法（Regression-based method）。GBDT属于基于回归的方法。其特征为：

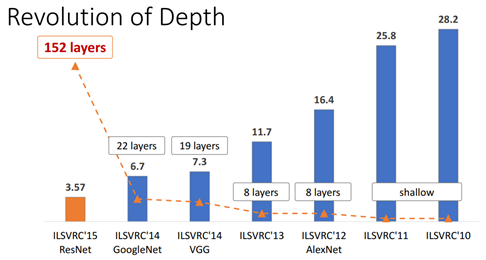
每一棵树之间的关系是串行的，并非是并行的关系，也就是说后一棵树的建立在前一棵树的基础之上。

每一棵树的叶子节点上存的是残差，也只有通过叶子节点上保存的残差，才能使形状不断地回归，从而回归到真实形状。

构建GBDT的步骤如下：

1. 对于获取的N幅图像，将它们作为训练样本，用所有图像的平均形状来作为这个初始形状。
2. 分裂树时，依据当前形状从该图片中提取出的特征（如像素差）来进行节点的分裂操作，直至到达树的叶子节点。 当把N张图片都输入这第一棵树，每一张图片最终都会落入其中的一个叶子节点，比如第1张图片落入了第3个叶子节点，第2张图片落入了第1个叶子节点等等。
3. 计算残差，即每一个图片的当前形状和真实形状的差值，之后，在同一个叶子节点中的所有图片的差值作平均，就是该叶子节点应当保存的残差。当所有叶子节点都保存了残差后，第一棵树构造完毕。
4. 把每张图片的当前形状做一个更新，也就是要将当前形状更新成：当前形状+残差。之后再用同样的方法构建第二棵树，直至建立的树足够多，可以最后的当前形状表示真实形状，那么这一个GBDT的建立就完成了。

对于一个GBDT（很多棵子树构成）而言，要建立一个特征池，这个特征池里是随机挑选的一些点的坐标。在树的节点分裂时，计算每一张图片在这两个点处的像素值以及像素差，之后根据分裂阈值进行判断，如果一幅图像的像素差小于这个阈值，就往左分裂，否则往右分裂，将所有图片都这样判断一次，就将所有图片分成了两部分，一部分在左，一部分在右。重复上面这个过程若干次，保存分裂的样本方差小的两个点的坐标值和分裂阈值。这样一个节点的分裂就完成了。然后每一个节点的分裂都按照这个步骤进行，直到分裂到叶子节点。这样就能确定人脸的轮廓了。

用残差网络训练模型的优势如下： 

残差网络解决了CNN模型难训练的问题，从上图中可以看到14年的VGG才19层，而15年的ResNet多达152层，这在网络深度完全不是一个量级上。

网络的深度对模型的性能至关重要，当增加网络层数后，网络可的以进行更加复杂的特征模式的提取，所以当模型更深时理论上可以取得更好的结果.但事实上，深度网络出现了退化问题（Degradation problem）：网络深度增加时，网络准确度出现饱和，甚至出现下降。而ResNet通过残差学习能解决深度网络的退化问题。

**2.2.1.4基于DT算法人脸动态表情信息采集**

本项目中，采集人脸动态表情信息的过程分为2步。

1. 密集采样

密集采样特征点具体分为以下几个步骤：

* 将视频的每一帧图像按五官部位划分为为多个小块，如左右眉毛、鼻梁、鼻翼、上下嘴唇等
* 对以上部位进行采点，去除掉一些无法跟踪的特征点，在时间轴上形成轨迹序列

2.轨迹描述

对于每一帧，在每个空间尺度上分别跟踪特征点。某个特征点在连续的L帧图像上则可以形成一段轨迹为（pt,pt+1,…pt+L-1）.在得到众多轨迹后，后期删除静态的轨迹和突出增大位移的轨迹，保留正常轨迹。

对于正常轨迹，其轨迹特征描述子为

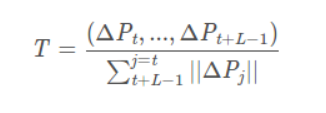


图2-4 轨迹特征描述子公式

项目中采取的L为8，故最终得到的轨迹特征为8\*2=16维（每帧分别在x，y方向的位移矢量）。

**2.2.1.5 基于DTW算法的动态表情匹配**

完成对面部动作进行曲线拟合后，验证阶段要进行曲线相似性比对，我们考虑了以下几点：

1. 边界对齐。每次验证动作的开始时间未必是一致的，考虑到用户的反应时间，在记录动作的过程中，绘制的两条曲线需要尽量保证在开始处有相同的变化趋势，这里可以利用对一条曲线进行时间轴上平移实现。
2. 连续性。匹配过程中可能出现多对一或者一对多的现象，用来弥补用户每次身份识别时，面部动作可能存在局部的快慢变化产生的误差。但是这种对应应该被限制在一个较小的时间跨度内，不同时间跨度内的点不能进行匹配，不能跳过某个时间跨度进行匹配，以确保连续性，防止动作缺失。
3. 单调性。由于每一次表情验证的时间较短，我们限制了每个部位的变化应该是单调的。眨眼等快速变化的非单调性动作将不参与匹配。

之后按照对应区间，对两条曲线求出欧式距离即可。

**2.2.2图像加密**

该部分采用了仿AES的矩阵加密算法，确保用于训练人脸识别模型的用户照片在任何时间都处于加密状态，进一步增强隐私性和安全性。由于不是项目重点，在此处只做简要介绍。

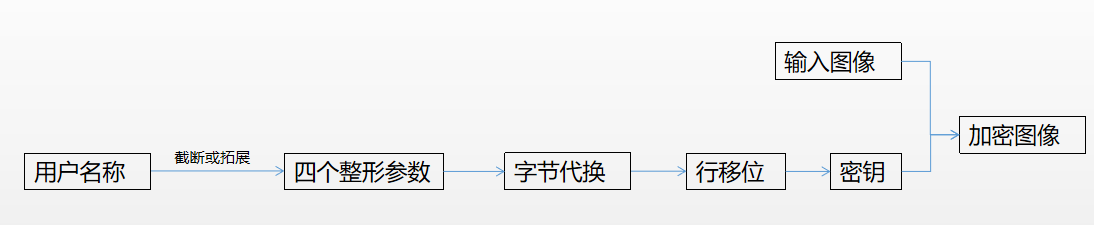


图2-8 图像加密流程图

矩阵加密算法中，我们借鉴了当前使用最广泛的AES算法，并将其改造为适合于矩阵加密。

大致流程如下：

1.获取用户输入的名称，将其截断或扩展为3个字符，再转化为ascii码，通过运算得到四个起始参数，通过依次令每个数字加上自己的行、列数，再与256取模，填充到92\*112大小的矩阵中。此步模拟的是AES算法中的字节代换步骤。区别在于AES首先确定了任意的代换表，而此算法的代换由矩阵的行、列数和以及矩阵的赋值顺序决定。

2.对第一步得到的矩阵进行行移位，第i行循环向右移动i位，此时得到了密钥矩阵。

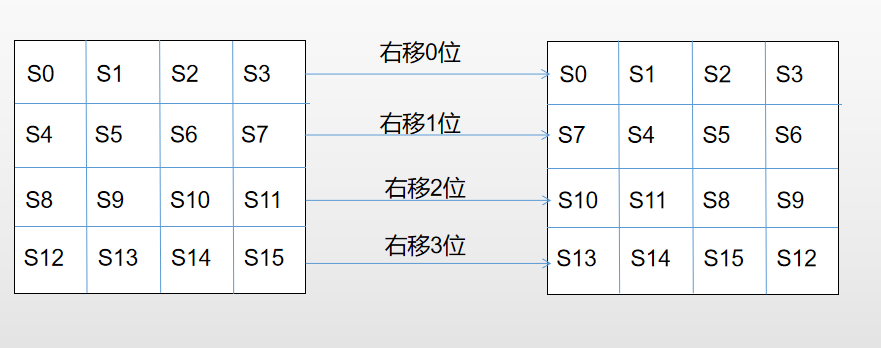


图2-9 行移位示意

1. 将密钥矩阵与图像进行按位异或，最终得到加密后图像。值得一提的是，该加密算法的加密与解密都是在程序运行过程中自动进行的，不存在一个实际存在的密钥文件。用于产生密钥的称号也可以被用户本人随时修改。

图像加密后——》

**2.2.3情绪识别**

要实现人脸表情识别，首先要对表情进行划分，我们将表情分为7种，分别为：惊奇，恐惧，厌恶，愤怒，高兴，悲伤，正常，不同的表情特征代表一种情绪，见下图。

****

图2-10 七种情绪的面部特征

训练识别模型的主要步骤如下：

1. 和训练人脸分类器类似，首先要收集人脸表情数据，再进行预处理，这里我

们需要收集的数据是不同的表情图片，并对不同表情的图片打上对应的标签，此处不再赘述。

二、搭建网络结构，这里我们在caffe框架中对AlexNet进行适当的修改，在训练过程配置学习率、动量、学习率衰减等参数，从而得到一个卷积神经网络模型，再通过第一步准备的人脸表情数据训练得到最终模型，从而能够识别人脸表情。

Caffe是一种开源软件框架，内部提供了一套基本的编程框架，用以实现GPU并行架构下的深度卷积神经网络。caffe的模型与相应优化都是以文本形式而非代码形式给出，其给出了模型的定义、最优化设置以及预训练的权重。其最常见的应用就是搭建一个卷积神经网络模型来解决一个识别问题，具有速度快、模块化和开放性等优点。

三、最后，通过人脸检测的相关接口，将我们所关注的人脸部分截取下来，利用模型进行识别后将结果输出。

**2.3核心功能的具体实现**

本作品的核心功能为人脸动态表情识别功能，下面详细介绍该功能的开发过程，具体分为如下三步：

1. 实现人脸识别，此部分主要是实现目前最为常用的人脸识别技术，在实现的

过程中学习人脸识别的相关知识。这部分涉及到人脸检测、图像处理与分类器训练，在整体工程中作为基础。

2.实现动态表情信息的采集，这部分我们使用了dlib的人脸矫正获取面部特征点坐标，再参考DT算法流程，利用线性拟合将离散的面部点沿时间轴拟合为曲线。

3.实现动态表情匹配，这部分我们首先利用感知哈希算法确保验证过程中人脸的基本信息是一致的（目的是规避掉在做动作的与初始识别到的是不同脸的特殊情况，即中途换人），再依据DTW算法实现曲线的相似性判断。最后综合分析所有的曲线匹配结果，得到最终输出。

**2.3.1 人脸识别功能**

该部分功能已经有很成熟的设计流程，我们依据项目需求，从网络上学习并运用。

下面用流程图说明其运行流程

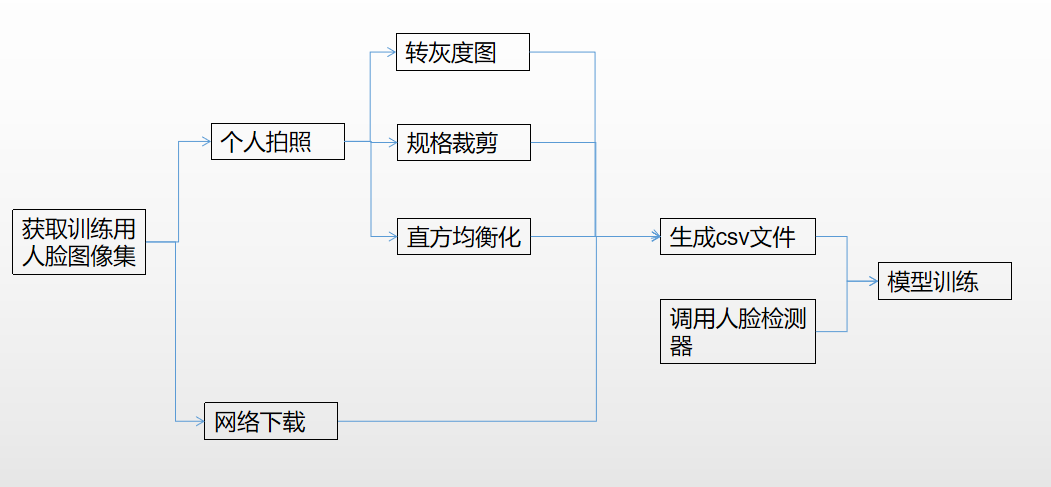
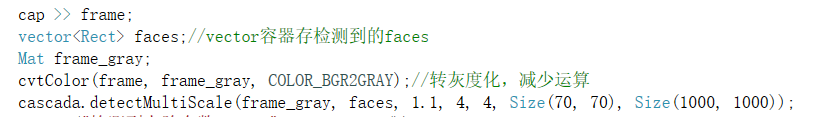


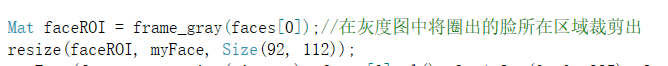
图2-11 人脸识别功能实现流程

首先，用读写文件操作从旧的csv文件中提取已保存的最后一个用户的序号，在此基础上自增一并保存为新用户序号，用来标记即将保存的用户照片。

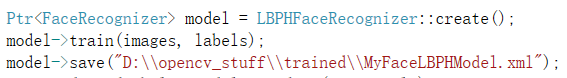
之后调用级联分类器，电脑对屏幕前用户拍照，程序将照片中的人脸框起，再将人脸照片转化为灰度图以减小运算量。



限定图像规格为92\*112，以保持图像大小的一致性。



通过准备好的图库和csv文件进行模型训练，将训练好的模型保存。



此后每次进行人脸识别，调用该模型即可。若要导入新的人脸数据，则需要按照

上述步骤重新训练模型。

值得一提的是，作品在训练模型的过程中会自动完成对图像的加密即解密。即导入新照片时，将图像加密保存至本地，训练模型时，依靠运算获取解密后的图像，在这个过程中不改变本地图像的加密形式。

**2.3.2动态表情信息采集与匹配**

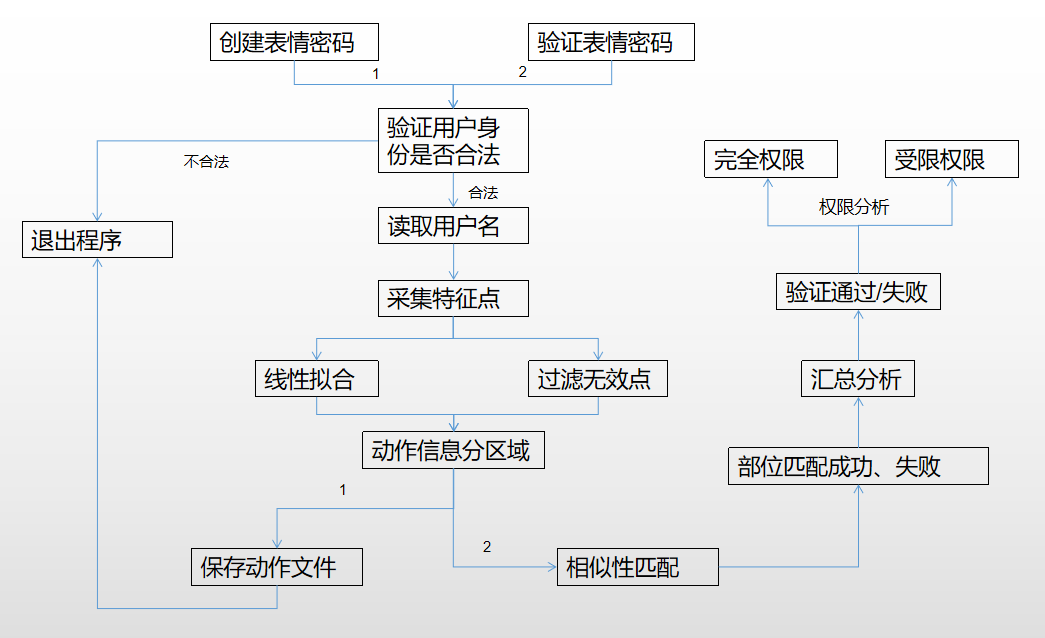


图2-12动态表情识别流程图

**2.3.2.1动态表情信息采集**

在导入一个新的动态表情密码之前，首先要通过第一步实现的静态人脸识别进行身份验证，确定当前在进行操作的用户信息是合法的。

对于通过身份识别的用户，首先利用进行人脸对齐与面部采点，我们考虑的特征点是如下68个。

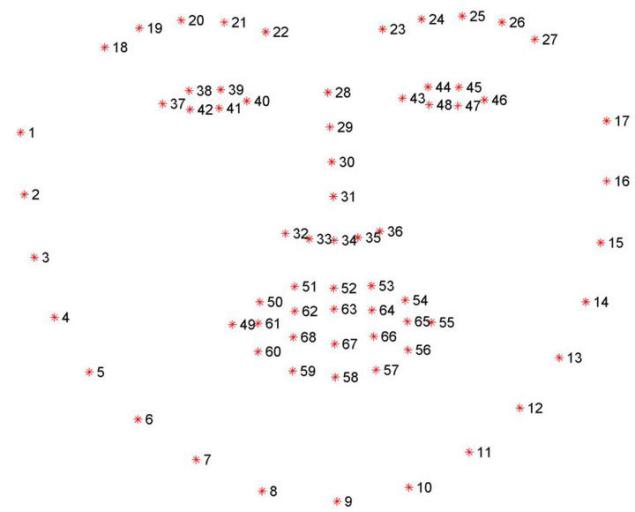


图2-13 面部采点序列

首先以上述图所示的关键点中，脸颊、鼻子、左眼、右眼及上嘴唇部分为基准关

键点，同时获取当前图像检测出的对应位置的关键点。计算上述两个点集之间的相似变换矩阵，获取当前人脸图像相对于基准人脸间的旋转角度、缩放系数及应该获取的人脸区域的rect坐标，以实现将用户人脸对齐到基准人脸上。

同时设置一个循环，每一次面部扫描依次记录下对齐后人脸每一个特征点的当前

坐标，在这个过程中，抛弃掉一些变化异常的点，那可能是采点过程中给由于光线角度或强度的突然变化造成的。直到采集到足够多的特征点坐标，跳出循环。

下一步是对于每个关键点的坐标关于时间拟合，拟合过程的伪代码如下：

输入：脸部特征变化的坐标集合

输出：线性回归之后的参数对（a，b）。

1. 坐标文件转化为数组存储
2. 对每列数据进行平移处理，每列减去每列的最小值。data=data-min(data.col)
3. 计算每列数据极差max-min，如果小于beta，则认为该点在记录时间内近似不动。
4. 如果大于beta，则用最小二乘法对该列数据进行线性拟合

e）将各点的数据分区域储存，即可综合得到每一个面部部位在观测时间内的向各方向的变化趋势，进而反映出面部表情变化。

记录下拟合后有意义的动作曲线，保存在本地。

在这个过程中，需要特别注意的是，由于每个点都在两个维度（x,y)上关于t变化，这两个维度的变化信息可能并不是都有意义的，有时我们会去掉一整个点，因为它的变化趋势异常，或者只是去掉某个点的某一个维度的变化曲线。

**2.3.2.2动态表情信息匹配**

在进行动作匹配的时候，我们已经获取了至少两个保存有两套表情动作信息的文件夹。文件夹中存放着面部的各个区域中多个关键点的变化趋势，我们将这些点依据变化幅度分为四类：关键点、次关键点、平凡点、近似不动点。并设计了两次审核。

1.局部审核

1.1突出动作匹配

首先要考察所有的突出动作。突出动作由关键点产生，关键点往往是一个动作中位移最大的那些点，比如微笑时的嘴角，耸鼻时鼻梁最下端的一点，扬眉时的眉梢。对于这些点，我们给予了它们最高的优先级，在任意一个部位中，首先要匹配通过所有的突出动作，这要求在变化方向，变化程度这两个方面上，待验证的动作和密码动作必须是一致的。若任意一个突出动作不满足该条件，那么局部审核就不会被通过。

1.2伴随动作匹配

在关键点满足匹配条件之后，我们再来考虑次关键点与平凡点。它们往往是一个动作中相邻于关键点的那些点，比如微笑时的上下嘴唇，耸鼻时鼻梁中央，扬眉时的眉心部位。在一个区域内有突出动作的前提下，考虑伴随动作才有意义。由于伴随动作对于判断动作变化的整体影响并不是很大，某一个特定次关键点或平凡点并不能直接决定局部审核是否应该通过。因此我们采用了积分制，对于每一对伴随动作的匹配，我们会考虑这次匹配结果是否与突出动作指向的结果一致，并依此来为它积分。匹配程度高的，则累加正积分，匹配指向矛盾的，则累加负积分，根据多次实验调试，我们决定当最终正积分的数量大于总积分数量的一半时，才反馈局部动作通过的信号。这意味着该部位的所有关键点完成了匹配，并且至少有半数的非关键点也完成了匹配。

1.3静态部位匹配

前两次匹配都是针对“动”的点，第三次则针对原本应该保持静止的点，若发生

了较大的变化，使其变成了次关键点甚至是关键点，就依据重要程度为该部位累加负积分。这可以防止验证者在完成了密码要求中的动作后，还携带了冗余的动作却也能通过测试的情况。

1. 整体审核

接受到所有局部审核返回的信号后，接下来要在整体上对其进行审核。我们将特征部位分为两类，那些拥有至少一个关键点的部位，根据关键点数量、匹配结果确定为一个值参与到整体审核中，而那些不具有关键点的部位，如果它们在局部审核表现正常，那么将其定义为模糊部位，即不参与整体审核。若表现异常，则作为异常部位参与整体审核。

由以上过程，可以判断用户的动作与作为密码的动作是否匹配。但此时存在的一点漏洞是，如果非法用户首先通过欺骗手段如橡胶头套等通过了静态人脸识别，而之后的动作检测部分不再会对人脸进行匹配，那么非法用户只需要知道该动作，并用自己的面部复现该动作就能通过检测，这于我们设想的“以正确的脸做正确的动作”作为密码的理念不符。

故我们使用了感知哈希算法，来确保用户面部特征的一致性。这是一种通常用于相似图片匹配的算法，实现过程如下：

（1）缩小尺寸：去除高频和细节，通过保存在静态识别阶段的图片，将图片缩小到8x8的尺寸，总共64个像素。

（2）简化色彩：将8\*8的小图片转换成灰度图像。

（3）计算平均值：计算所有64个像素的灰度平均值。

（4）比较像素的灰度：将每个像素的灰度，与平均值进行比较。大于或等于平均值，记为1；小于平均值，记为0。

（5）计算hash值：将上一步的比较结果，组合在一起，就构成了一个64位的整数，作为这张图片的指纹。

最后，在动作匹配阶段，定时采集用户图像，按以上步骤获取hash值后计算两个指纹的汉明距离。如果这个值为0，则表示这两张图片非常相似，如果汉明距离小于5，则表示有些不同，但比较相近，如果汉明距离大于10则表明完全不同的图片。此时就证明目前做动作的并非是合法用户，系统将予以拒绝。

# 作品测试与分析

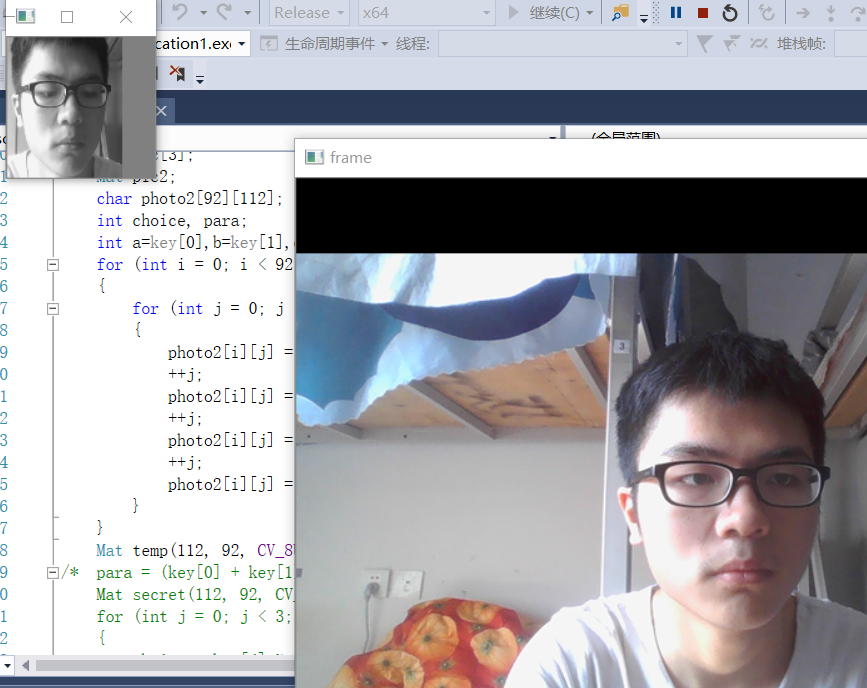
**3.1作品测试说明**

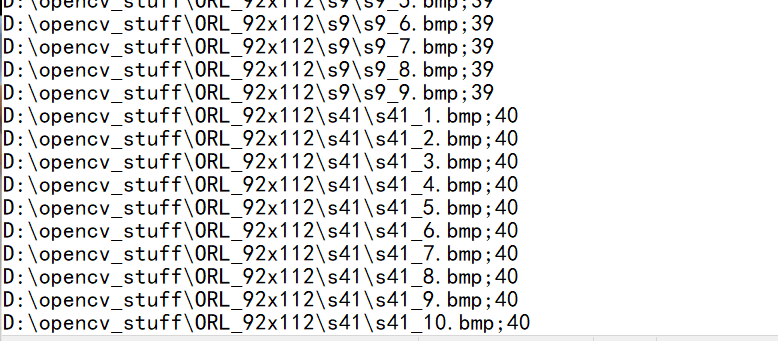
本测试环境为windows 10 x64系统，在visual studio 2015下运行，需配置好opencv环境。

本作品主要实现了动态人脸识别功能以及图像加密功能两部分，下面对这两项功能进行测试。

**3.2.1动态表情匹配功能测试**

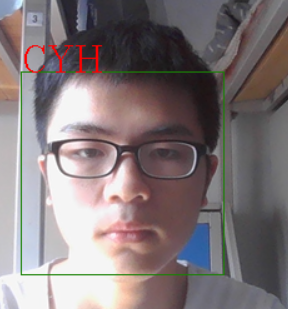
首先运行程序，在模式下选择“导入新的人脸数据”，输入称号，即自动开始捕捉人脸。





自动生成的csv文件，可以看到它标记了每张照片的路径，并在末尾给予其编号。

此时人脸识别模型以及识别完成了，测试一下能否正确识别我。



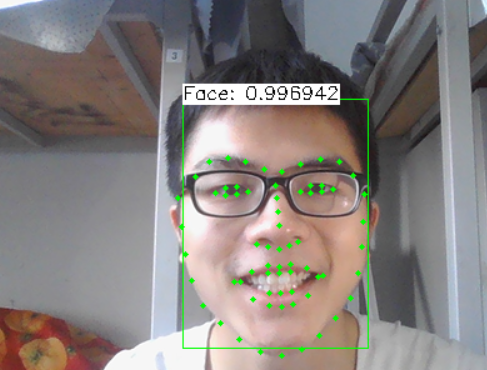


可以看出识别率还是比较高的，正脸和侧脸都能正确认出并标记出用户名称。不过要提及的一点是识别过程中对光线均匀度要求比较高，当面部处于暗亮很不一致的环境下时，有可能出现识别失败的情况。视频见下：



接下来试着导入表情密码

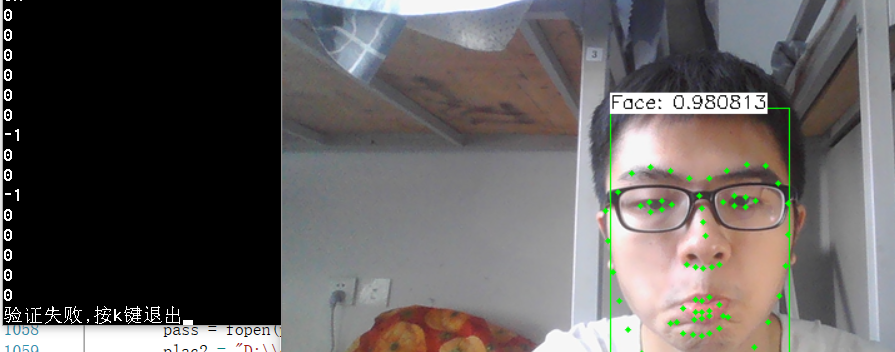
我做出了微笑的表情，可以看到采点程序正常进行



之后做同样的表情，检测验证结果是否正确



可以看到，当再次做出笑脸时，显示匹配结果正确。



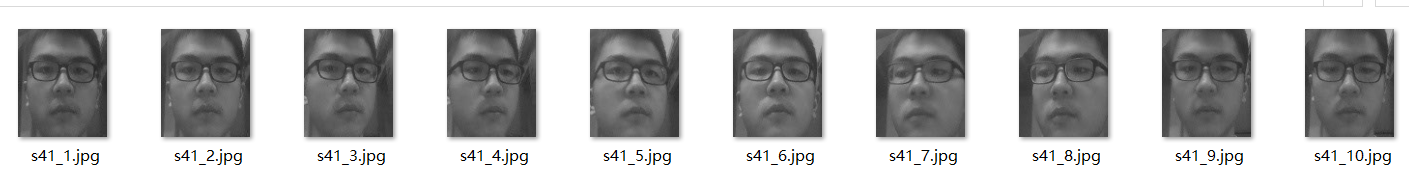
当做出沮丧的表情时，显示匹配结果错误

需要特别指出的是，动态表情匹配与表情匹配的区别之处在于，我们的程序更注重于**变化的过程**。就以上的例子来说，若被检测的表情自始自终都是笑脸时，那么会匹配失败，因为检测不到表情变化。

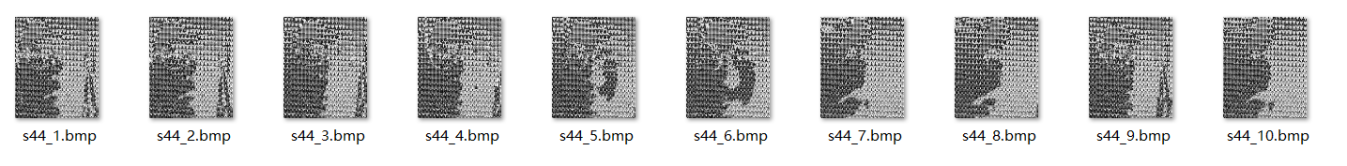
视频测试如下：第一组做出正确表情，第二组做出错误表情，第三组表情正确，但是是静态的，五官未发生移动。

**3.2.2图像加密功能测试**

我们实现拍了一组未经加密的照片，用于以加密后的图像进行比较，转化为灰度图后效果如下



加密后的图像呈现如下



可以看到加密程序正常执行了。由于人脸识别功能的正常运行，也可以推断在训练人脸检测模型时解密功能也能够正常执行。

**3.2.3情绪识别功能测试**

一共有七种可识别情绪，在此做部分展示如下：

# 创新性说明

本作品实现了基于人脸动态表情的身份识别系统，主要创新点如下：

**4.1基于人脸动态表情特征的身份认证系统**

我们的作品实现了自定义的人脸动态表情匹配系统，即用户可以自己设计面部动作作为动态表情密码，进行身份识别时必须完成自定义动作才可以通过验证。这一设计是创新性的，能够极大地增强以人脸识别的作为身份认证系统的安全性。

**4.2基于密集轨迹(DT)算法的表情抽象化**

DT算法通常用于行为识别，使用此方法能够有效跟踪一定区域内特征点的变化趋势，并最终得到其轨迹。我们创新地利用此方法对面部各部位进行采样，在一次动作中获取人脸动态表情信息，并将其作为密码用于身份认证。

**4.3完美解决了特殊场景下的安全问题**

自定义交互式动作活体检测可以面向更多的场景进行应用，基于我们的作品，可以针对不同场合设计多个动作。比如当遇到特殊危险被胁迫验证的时候，只要做某个自定义的动作，账户就会锁死。在此基础上，我们增加了情绪分析功能，针对日常生活中可能出现的冲动消费、被诈骗现象，当用户处于恐慌、愤怒、激动等情绪下时，系统可以对其支付行为进行二次验证。

# 第五章 总结

目前人脸识别应用广泛，随之而来的是人脸信息的泄露与滥用。因为针对某个特定的人，他的人脸信息是相对恒定的，而且市场上应用最为广泛的静态人脸识别技术仅仅依靠人脸的生物特征进行匹配，这就给了不法分子可乘之机，他们只需要通过其他方式获取用户的人脸信息，就有可能突破人脸识别系统，从而对用户的生命和财产安全造成威胁。而我们作品立足于增强支付环境下的安全，提出了自定义的人脸动态表情匹配系统的理念，即用户可以自己设计面部动作作为动态表情密码，进行身份识别时必须完成自定义动作才可以通过验证。这完美解决了非法用户利用数字人脸图片或模型骗过识别系统等安全问题。在此基础上，我们增加了情绪分析功能，针对日常生活中可能出现的冲动消费、被诈骗现象，当用户处于恐慌、愤怒、激动等情绪下时，系统会对其支付行为进行二次验证。

我们作品立足支付安全，具有强大安全性，能够有效防御包括“人脸照片”、“脸部模型”“人脸视频”等能够破解传统人脸识别系统的攻击手段。能够大大增强在进行支付，或其他对身份验证的安全性要求很高的活动时，使用人脸识别验证的安全性、可靠性。并且随着人脸识别的广泛应用，许多需要严密认证用户信息的场景，都可以运用我们的技术。

由于面部识别的便利性，其运用必然会越来越广。而社会对人脸识别的依赖程度的提高，可能会导致有不法分子试图以其为攻破口，进行非法行为。也因此，未来大家对于人脸识别的安全性需求必然会逐渐提高，故而本作品绝对不会缺乏用武之地。同时，当前对于人脸识别的运用场景上还是单薄的，一般仅仅将其作为身份验证技术。我们的项目创新性地将人脸识别与情绪分析相结合，除了能验证用户身份外，还能获取其当前情绪状态，结合当下场景给出反馈，这种互动式的验证手段，大大增加了人脸识别的可玩性，未来具有巨大的开发空间。

# 参考文献