基于人脸识别的
解锁屏安保系统应用报告

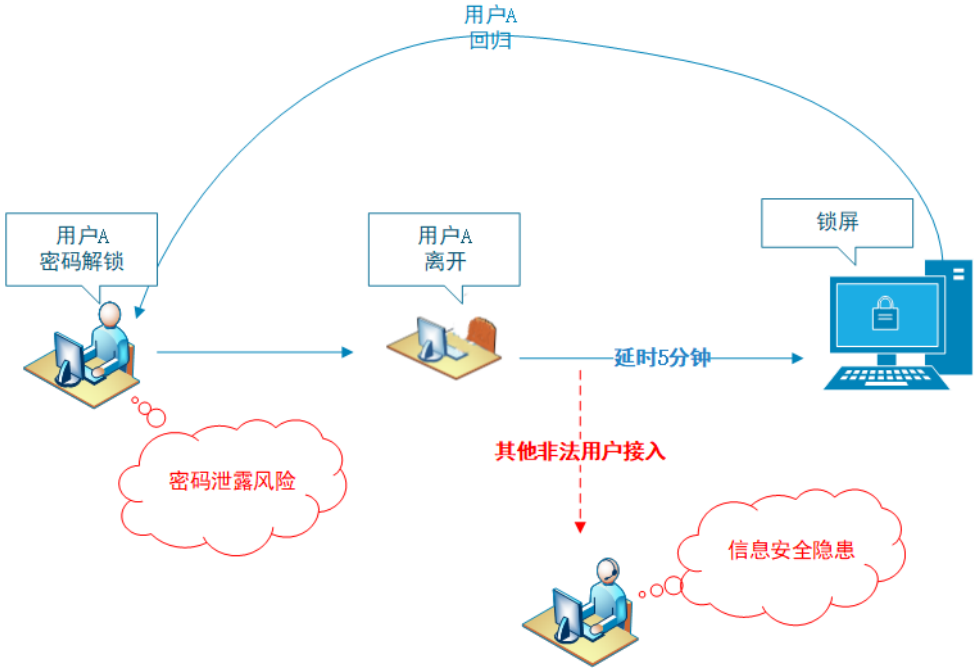
区块链与生物识别实验室

2018年11月

目录

1.1 背景

存在的安全隐患：1、密码泄露风险；2、延时保护时间太长，信息泄露风险



1.2 背景

为了加强柜面、个人办公电脑、运维机器等其他多个场景下的信息安全保护，积极跟踪金融科技发展趋势，我行区块链与生物识别实验室（简称“实验室”）开展人脸技术研究，通过对同业应用场景以及业界人脸技术调研,结合业务需求，实验室提出我行可将人脸识别技术应用于锁屏功能，以力争在金融同业中占领先发优势，提供更安全、灵活的技术保证，提高工作效率。实验室结合人脸识别技术，已经实现了一个解锁屏安保系统工具，该工具运行在Windows（Win7以上版本，下文不再区分）系统，其能提供便捷的安全管理、并具有系统资源占用少、用户无感知、使用简单等优点。

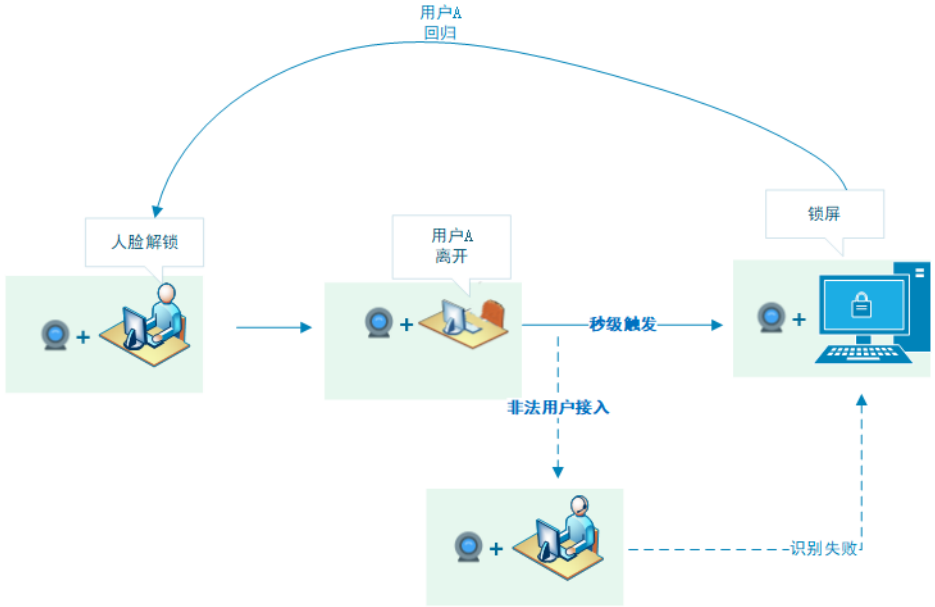
1.3 目标

本应用的目标是为我行所有运行Windows的终端提供更加安全、便捷的身份认证。

目录

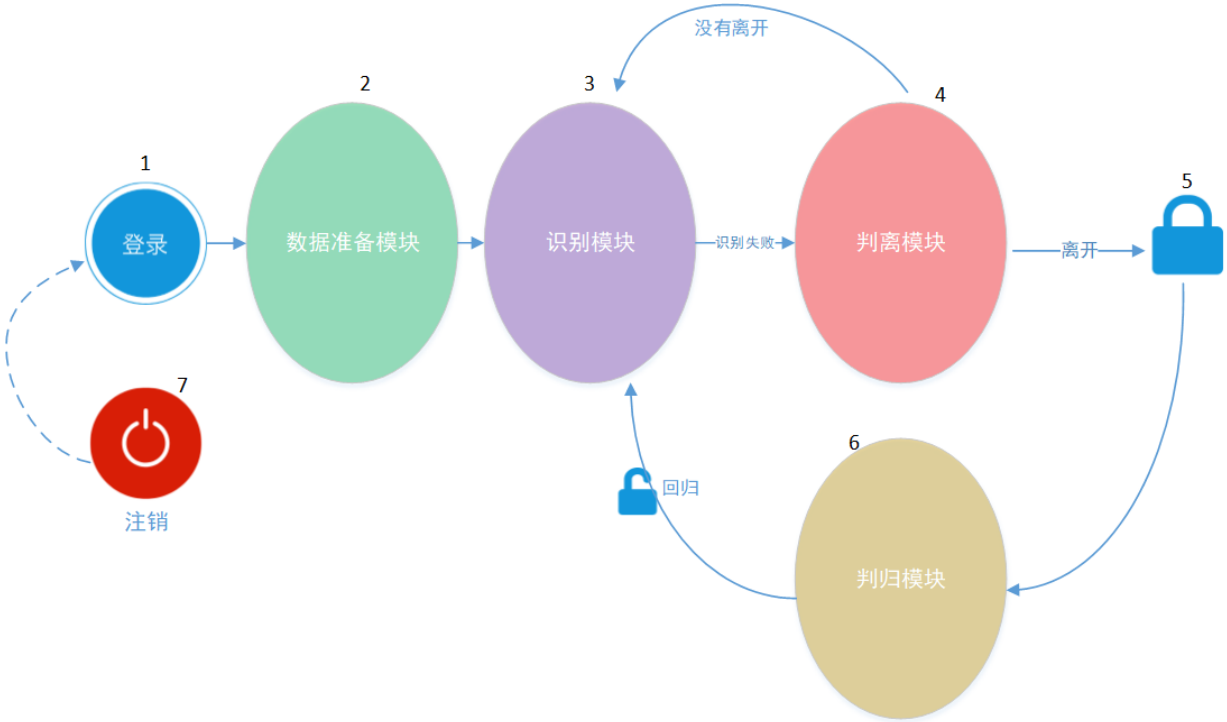
2.1 解锁屏安保系统简介

解锁屏安保系统是一个运行在Windows系统之上，结合人脸识别技术的安全工具。该系统能自动识别操作机器的人员是否有具有权限，当用户离开或者其他非法用户操作机器时，计算机自动锁定；用户回归时，计算机自动解锁。



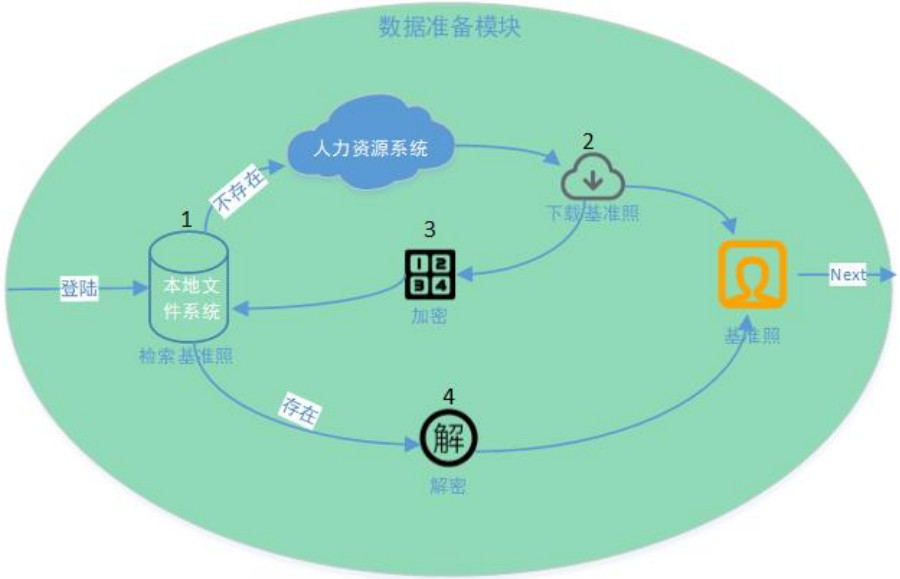
2.2 整体设计思路

解锁屏安保系统包括数据准备模块、识别模块、判离模块、判归模块四个核心模块



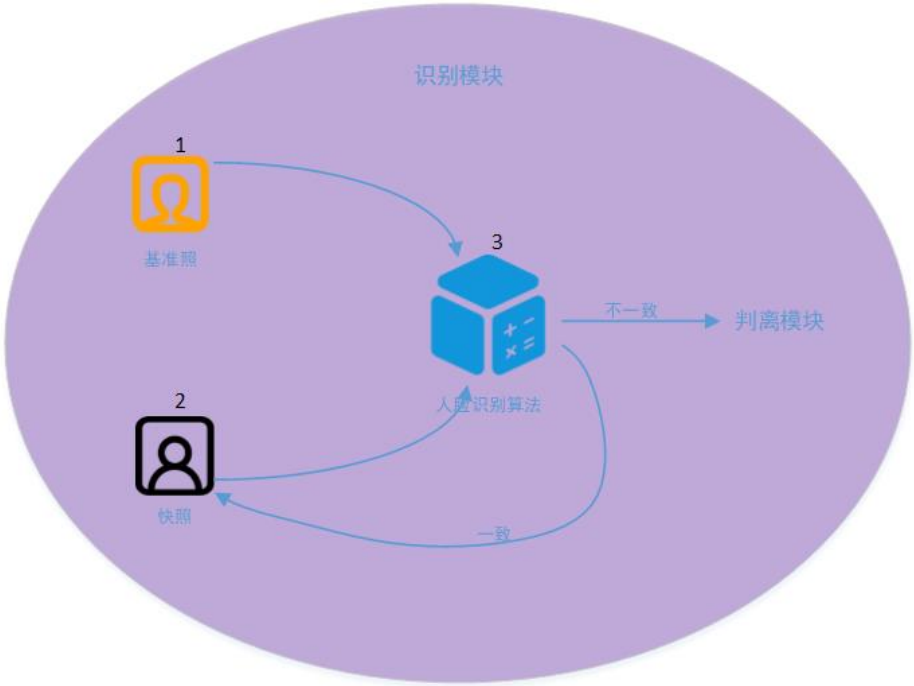
2.3 数据准备模块

数据准备模块为当前用户初始化数据，如果系统本地没有存放该用户的基准照片，锁屏安保系统将在该模块去人力资源系统下载基准照片，并加密基准照片保存，下次直接从本地读取，减少对网络的依赖。



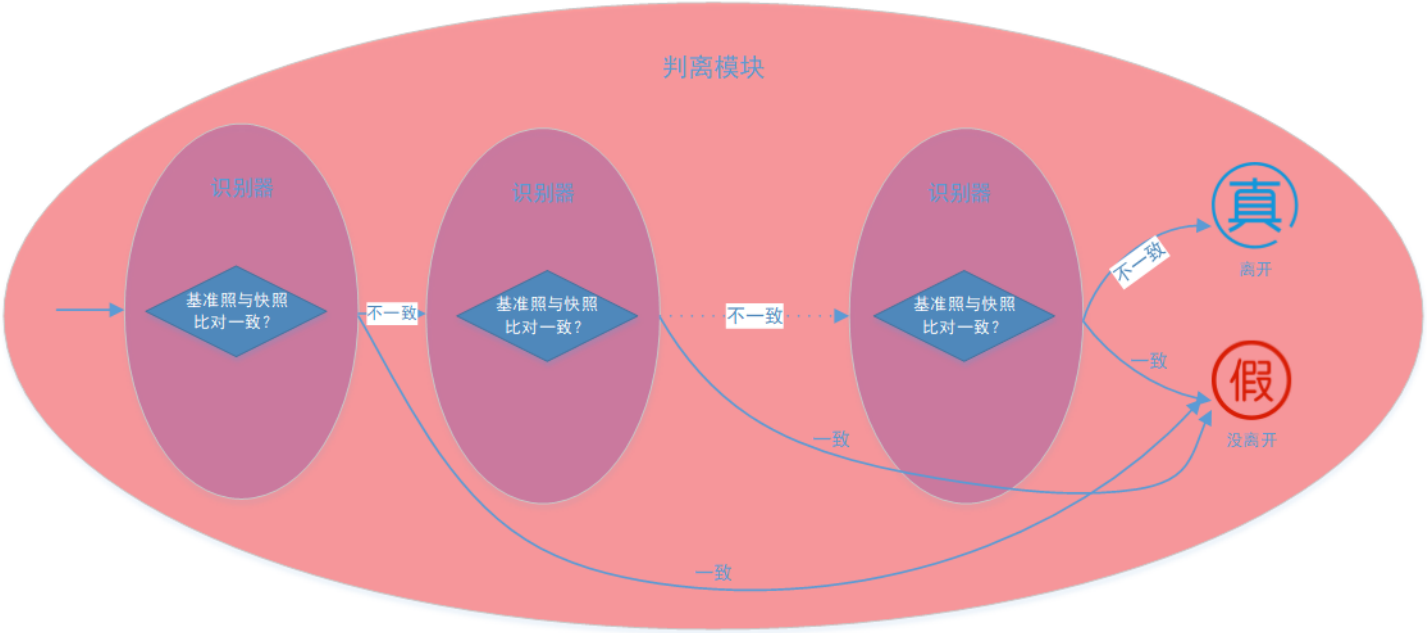
2.4 识别模块

识别模块主要利用人脸识别算法，实现1:1人脸认证。



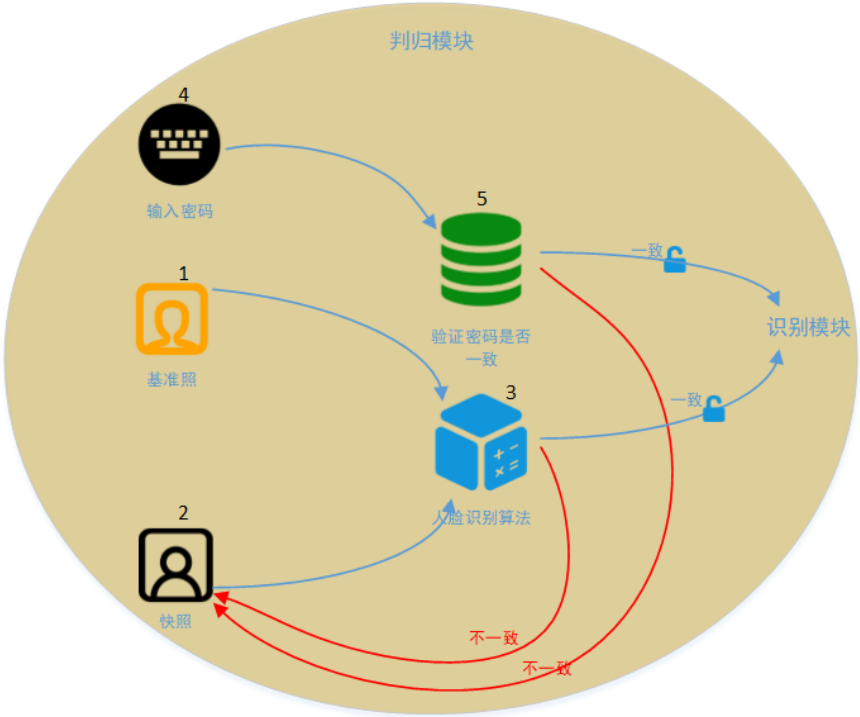
2.5 判离模块

判离模块是用于判断用户是否真的已经离开，对识别模块的结果进一步确认分析，确认是否需要锁屏，这是对上一步识别结果的修正判断。



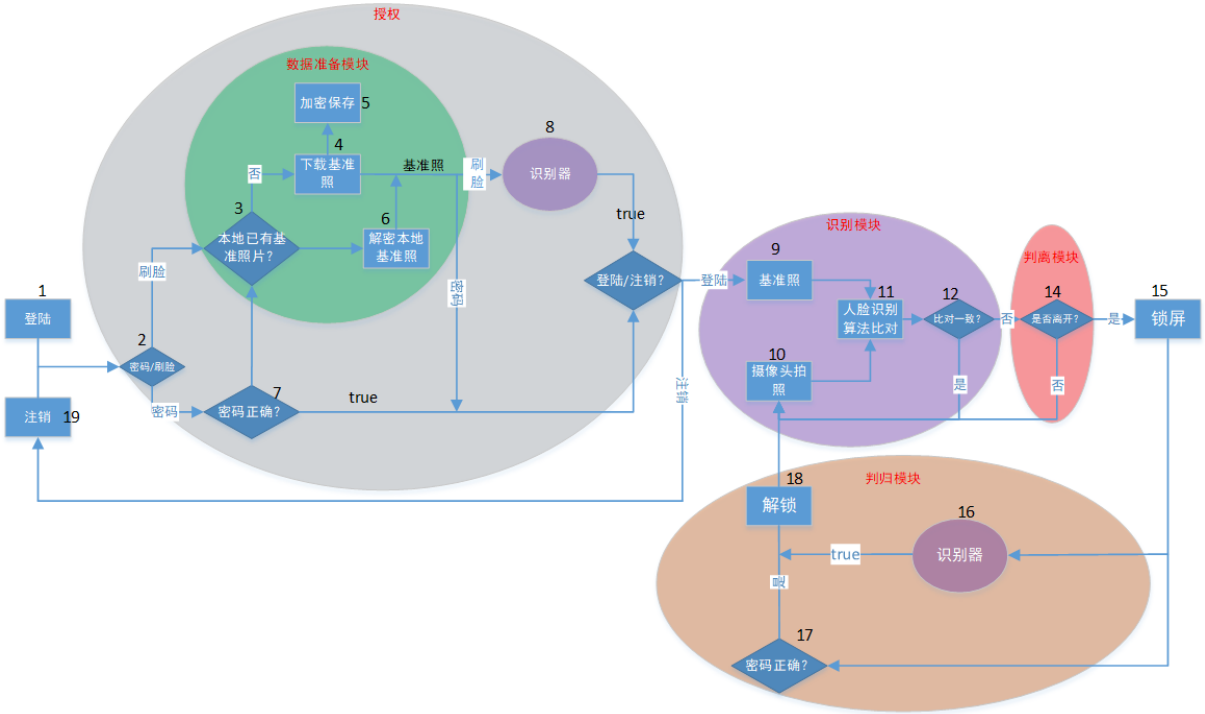
2.6判归模块

判归模块是用于判断用户是否已经回归，如果用户回归将解锁计算机。



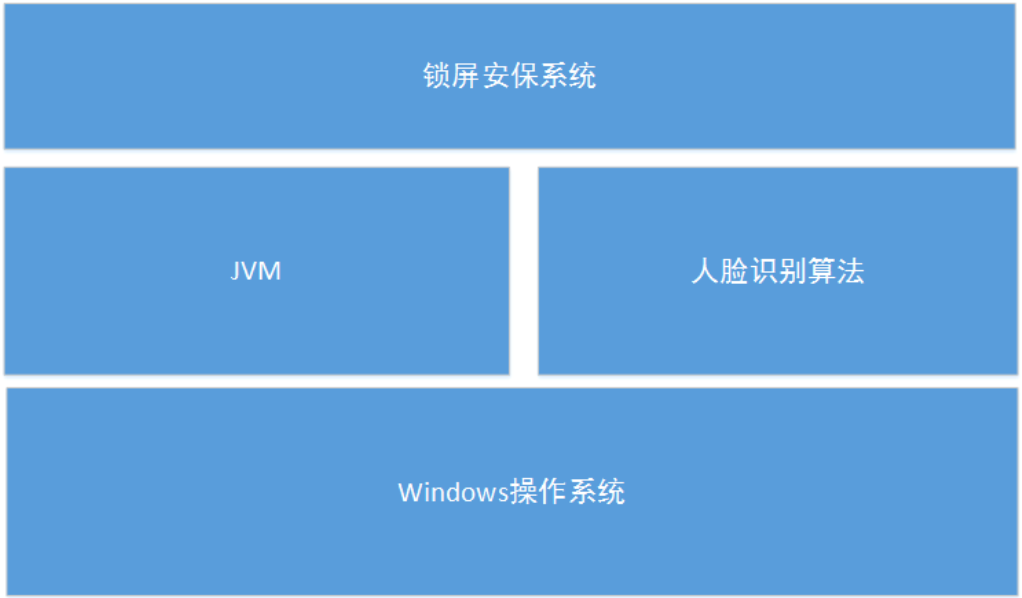
2.7 详细流程图

其通过统一认证号登陆，运行在操作系统之上，利用接入摄像头采集的照片实现离线人脸识别。该系统后台自动运行，系统开销小，运行后对用户透明。



2.8 架构设计

解锁屏安保信息系统运行在桌面操作系统之上，由JVM作为运行环境支撑，结合人脸识别算法的一个轻量级安全工具。



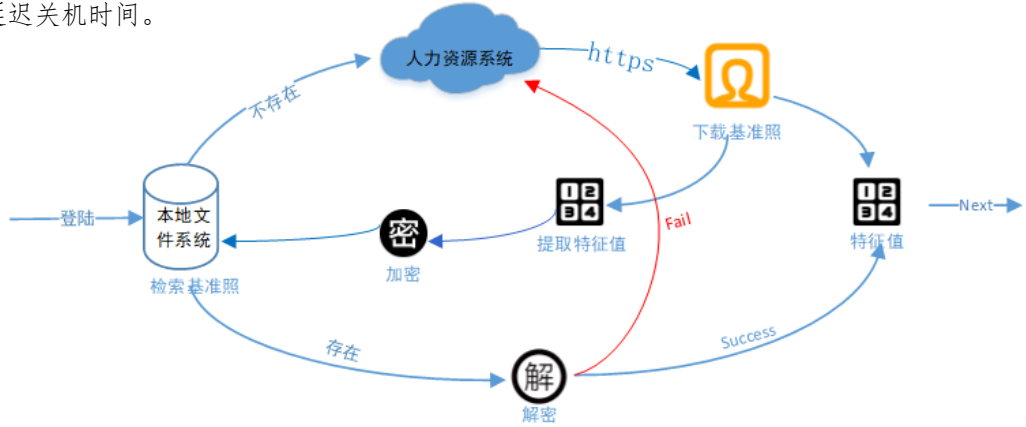
2.9 基础数据安全性考虑

- https安全协议：针对基准照在传输的过程中可能遭到攻击。
- MAC绑定+哈希摘要+对称加解密：

*加密：*1、获取机器MAC地址。2、MAC地址 + 特征值生成元数据。3、哈希元数据生成信息摘要。4、对称加密信息摘要。5、信息摘要和特征值一起保存。

*解密：*1、对称解密得到信息摘要。2、获取机器MAC地址、读取基准值。3、哈希元数据生成信息摘要。4、比对信息摘要是否一致

MAC地址绑定的目的是为了解决破坏者将基准值**拷贝**到其他机器使用；哈希摘要+对称加解密的目的是为了防止存放在本机上的基准值被**篡改**，如果被篡改将导致解密失败，并重新从云端获取最新基准值；本地基准值被**删除**，将导致解密失败，并重新从云端获取最新基准值。如果信息被篡改、删除，而且网络不可用，将会导致解锁屏系统登陆失败，此时系统会提示用户需要修复网络，并延时强制关机，用户可通过输入密码延迟关机时间。



2.11 效果对比

方式	锁屏触发时间	信息安全性	系统安全性	便捷性	系统开销
基于人脸	秒级	非法用户无法操作、信息安全	*1、系统未登录自动关机提示* 2、*ObRegisterCallbacks内核函数保护进程不被关闭*	部署简单、用户无感知、刷脸解锁、自动锁定	i7-8550U@1.8GHZ：内存消耗<200M。采样频率2秒，CPU消耗平均每秒增长<15%；采样频率3秒，CPU消耗平均每秒增长<9%；
传统模式	5分钟	非法用户有机会操作、密码泄露、信息泄露风险	能被轻易破解	手动解锁	非常小

2.12 局限性和适用条件

因为，解锁屏安保系统基于人脸1:1认证算法，所以，系统对从摄像头获取的快照有一定要求，即要求快照包含完整的清晰正面人脸。因此，在空间上限制了摄像头与用户的位置关系。随着对姿态、人员轨迹等方向的进一步研究，这一局限性能够得到较好的解决。

在这之前，该系统适用于摄像头能获取清晰人脸，且用户与摄像头空间位置关系相对稳定的情形。

目录

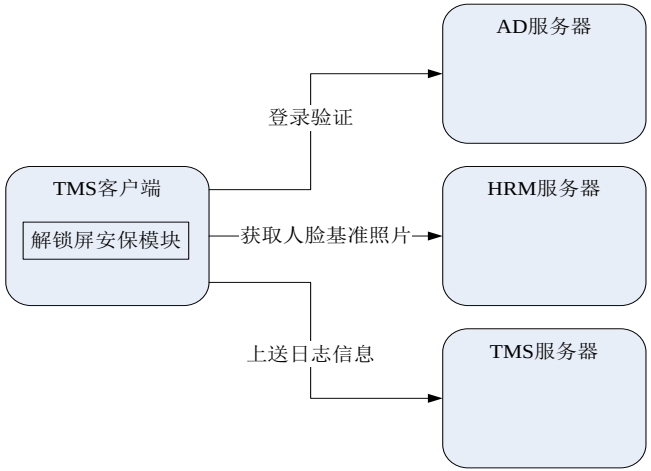
3.1 功能优化

解锁屏安保系统基于人脸识别算法实现，能够提供便捷的安全管理，其既可以单独完成安全管理任务，也可以配合其他安全技术协同应用到其他诸多场景。但是其也还存在改进的地方，留待后续进一步完善。现其优势和进一步改进点总结如下：

序号/标题	优势	后续计划
1	软件上只依赖于Windows操作系统，系统开销小； 硬件上只依赖于普通摄像头。	进程安全控制
2	基于人脸识别算法，智能、高效，集成活体检测功能，能抵御欺诈攻击	丰富活体检测功能

3.2 与TMS集成

目前我行Windows终端已安装并运行TMS客户端程序作为终端管控程序，可考虑将解锁屏安保工具作为功能模块集成到TMS客户端产品中，复用TMS客户端的AD登录和上送日志信息功能。



目录

经过研究，人脸识别技术已经成熟，其应用已经渗透到我们生活的方方面面。解锁屏安保系统作为便捷安全管理工具，是顺应时代技术发展的产物，其让安全管理工作更加便捷、可靠。因此，实验室建议可将其应用于柜面、个人办公电脑、运维机器的等场景的安全管理。从边缘业务逐步应用到核心业务，从结合其他安全管理技术（如密码安全管理）逐步单独完成安全管理任务。

目录

六、待审议要点

- 是否同意本报告提出的技术路线
- 是否同意本报告提出的后续具体实施路线

谢 谢！

联系人：徐植君
办公电话：020-83927794