虹识技术
Hongshi Technologies

武汉虹识技术有限公司

警用系统虹膜登录解决方案

武汉虹识技术有限公司为全球客户提供基于生物识别的全方位安防解决方案、技术支持和售后服务。阁下关于虹识技术的任何问题或见解，可通过下列方式与公司总部、驻地办事处或客服中心取得沟通 ：

Wuhan Hongshi Technologies Co.Ltd. provides biometrics based full security solutions, technical supports and customer services for global clients. Should you have any problem or suggestion about Hongshi Technologies please feel free to communicate with firm headquarters, agent offices or customer service center via following contacts:

公司网址(WEB SITE) ：	http://hongshi-tech.com
公司电话(TEL.) ：	0086-027-59621973　　0086-027-86696097
公司传真(FAX) ：	0086-027-87805598
公司总部地址(ADDRESS) ：	湖北省武汉市东湖高新区高新大道 999 号未来科技城，C1-9F C1-9F Future City CBD, 999# GaoXin Ave. DongHuGaoXin Dist., Wuhan Province, P.R.C
邮政编码(POST CODE) ：	430075
邮箱(E-MAIL) ：	sales@hongshi-tech.com

感谢您体验本公司产品和服务，在体验前请认真阅读本方案并妥善保存，以便随时查阅参考。

Thank you for experiencing products and services of Hongshi Technologies. Before experiencing please read the document carefully and in order to reference afterwards, please conserve properly.

第1章 概述

1.1 建设背景

随着公安机关“金盾工程”的深入实施，公安计算机网络得到了快速发展和应用，公安机关内部计算机拥有数在逐年增多， 基层一线民警基本实现了人手一台电脑， 公安网络建设不断完善和健全；公安信息化平台广泛应用， 如协同办案系统、协同办公系统、派出所基础信息等；网上追逃， 网上比对等网上作战技术也得到普遍使用。公安工作对信息网络的依赖程度越来越高， 网络信息安全就显得越来越重要。 我们在享用网络信息资源带来方便快捷的同时，随之而来的公安网络安全问题也日益突出， 非法授权访问、用户非授权访问、篡改数据、信息泄漏等等， 这类问题若不能引起我们的高度重视， 对公安机关科技强警工作乃至整个公安工作的发展将造成巨大的威胁。

1.2 现状分析

身份认证已成为公安 IT 系统安全应用中一个重要环节， 目前常见的身份认证方式主要有三种， 最常见的是使用用户名加口令的方式， 但这也是最原始、最不安全的身份确认方式， 非常容易由于外部泄漏等原因或通过口令猜测、线路窃听、 重放攻击等手段导致合法用户身份被伪造；第二种现在电子政务和电子商务领域最流行的身份认证方式--基于 USB Key 的身份认证，但 USB Key 的身份认证也存在诸多弊端， USB Key 的遗失，盗用等也让信息安全存在不小的隐患。为此公安系统中的身份认证的真实可靠性必须依靠先进的技术手段来实现。

当前人体生物特征鉴别技术包括指纹、掌纹、面部、 声音、虹膜、行态等， 2001 年 5 月到 10 月，受英国政府通信电子安全组 CESG（Communications ElectronicsSecurity Group）委托， 英国国家物理实验室（NPL）通过广泛的实验研究，对上述各类人体生物特征识别技术作了分析比较并在实验结果中公布：虹膜识别是“最精确的”、“处理速度最快的”以及“最难伪造的”。因此，如果将虹膜识别技术广泛应用于公安 IT 系统中，将大大提高公安 IT 系统的安全性和可靠性， 降低通过身份冒用进行犯罪的可能性， 减少因公安 IT 系统中现存的及潜在的安全漏洞和风险隐患。

随着虹膜识别身份认证技术的不断成熟，技术应用成本的不断降低，公安 IT 系统

安全性要求的不断加强， 虹膜身份认证技术在警务各应用系统中有着广泛的应用前景。

1.3 设计原则

警用虹膜登录系统的设计以确保安全和稳定为基础， 同时兼顾易管理性、实用性及经济性，并以对现有的网络基础设施最大的利用和最少的改动为设计方针。主要优点是非接触式识别、易于管理，可扩展性强。由于上面所提及的虹膜识别技术自身在可靠性、唯一性等方面有其他人体生物识别技术无可比拟的天然优势,从而使以此技术作为人员身份识别的系统， 达到更高的安全级别和更可靠的唯一识别性。

1.3.1 标准化与规范化

警用虹膜登录系统遵循公安机构应用软件开发标准以及相关法律法规的要求，符合国家有关标准要求，符合国家对于信息系统的各项标准和规范。所有系统内的数据开发与目前全国各省当前使用的公安数据管理系统中的执法数据保持一致，以避免其他无效数据参与和干扰数据查询与监控。同时， 警用虹膜登录系统将按照国家计算机网络系统建设技术规范要求提供相应数据接口。在虹膜识别系统投入实际应用的过程中，将根据《信息安全技术虹膜识别系统技术要求》和《中华人民共和国公共安全行业标准·安防虹膜识别应用 ：算法评测方法》 进行系统的数据架构设计， 适应未来生物识别数据和网络拓扑统一联网、 升级改造的需要。同时， 该系统将预留充分的数据接口， 为后期维护和升级减少重复开发的可能。

1.3.2 开放化与可持续化

整合利用现有信息资源， 优化数据管理手段， 以利于带动信息系统建设， 保证系统的规范性、安全性、开放性和持续性，实现优越的综合性能，满足长期持续发展的需要。虹膜识别公安系统在规划、设计、 开发过程中需要可延续应用设计， 便于未来的升级与拓展。同时，虹膜识别警务系统将提供网络架构、系统架构、数据库结构、数据字典项等相关的技术文档， 并预留有充分的数据接口以进行功能拓展。

1.3.3 先进性和通用性

警用虹膜登录系统的采集识别终端设备由搭载乾芯 TM-I 代虹膜识别芯片的虹膜编码识别主板，高速、 超清虹膜相机和 LCD 显示屏组成，是一套基于纯硬件设计的身

份识别系统。系统能快速准确的抓取高质量的虹膜图像，利用全球领先的核心算法完成虹膜识别与身份认证。 虽然系统采用全球领先的虹膜识别算法， 而且提供丰富、完备的接口， 但用户在使用虹膜身份识别系统时， 具备安装简单，识别快捷、操作方便的易用性。

1.3.4 安全性和可靠性

警用虹膜登录系统除了采用高可靠性的虹膜识别算法， 还借助先进的信息化技术，保证系统在运营过程中信息数据的绝对安全， 保证系统在虹膜数据采集时的数据传输安全。系统对经过授权的操作人员进行虹膜信息授权注册和授权管理时， 需要严格按照操作权限的要求进行， 并对每项操作留下完整的日志记录信息以备勘查。

1.4 设计依据

警用虹膜登录系统建设以国家、行业相关规范和以我司参与制定的虹膜识别行业的标准为设计标准及依据，依据和要求如下 ：

- 《信息安全技术虹膜识别系统技术要求》（GB/T20979-2007）
- 《虹膜图像质量国际标准》ISO/IEC19794-6:2005
- 《安全防范工程技术规范》GB 50348-2004
- 《中华人民共和国公共安全行业标准》GA38-2004
- 《计算机信息系统安全》（GA 216.1 - 1999）
- 《计算机信息系统安全等级保护划分准则》 （ GB 17859-1999）
- 《信息系统通用安全技术要求》（GB/T 20271-2006）
- 《数据库管理系统安全技术要求》（GB/T 20273-2006）
- 《信息系统安全工程管理要求》（GB/T 20282-2006）

第2章 方案设计

本方案结合武汉虹识技术有限公司自主开发的虹膜识别系统， 针对现有的 USB KEY 的安全进行升级和改造， 旨在从根本上解决安全问题， 并借力现代高科技生物识别技术，增强信息的安全级别，简化管理流程， 提升安全系统的身份验证效能。

本方案由武汉虹识技术有限公司向客户提供虹膜识别产品和技术支持，方案所涉产品规格和技术阐述最终解释权归武汉虹识技术有限公司。

2.1 系统概述

警用虹膜登录系统由系统硬件设备和系统软件管理组成， 硬件设备包括：USB 虹膜采集识别设备、授权服务器，软件包括虹膜识别身份管理平台、SDK 开发包、数据库等。

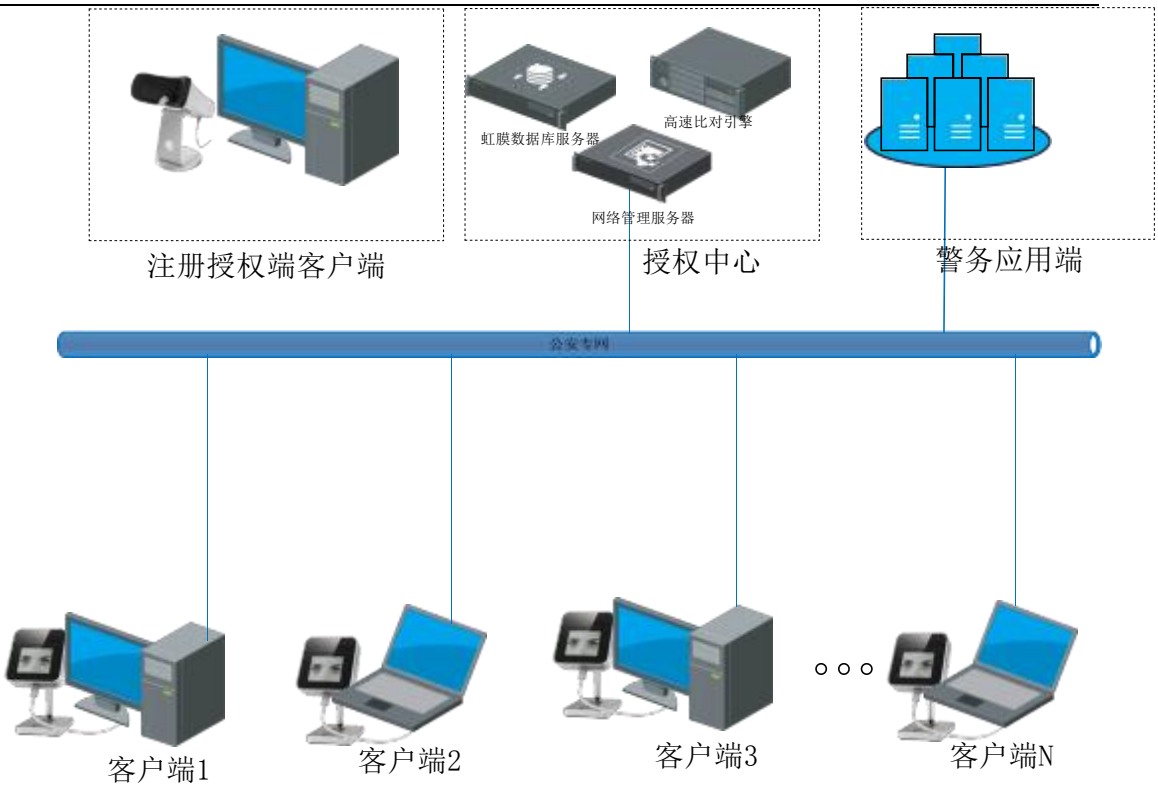
警用虹膜登录系统先通过虹膜采集器采集用户虹膜信息，并注册储存，给予预定的权限， 通过虹膜识别器辩识，使得只有经过授权的人才能登录授权访问的系统。

2.2 系统架构设计

整个警用虹膜登录系统由虹膜注册授权客户端 、虹膜登录客户端、 虹膜授权中心、警务系统应用端四个部分组成。

在公安数据中心建设虹膜授权中心，其中授权中心由虹膜数据库服务器、网络管理服务器及高速比对引擎及配置软件平台组成， 负责对采集上传的虹膜数据进行处理、存储以及客户端的管理、用户权限的管理、客户端访问数据处理、后台高速比对服务接口的提供、其他系统集成服务的提供。

系统拓扑图如下所示：

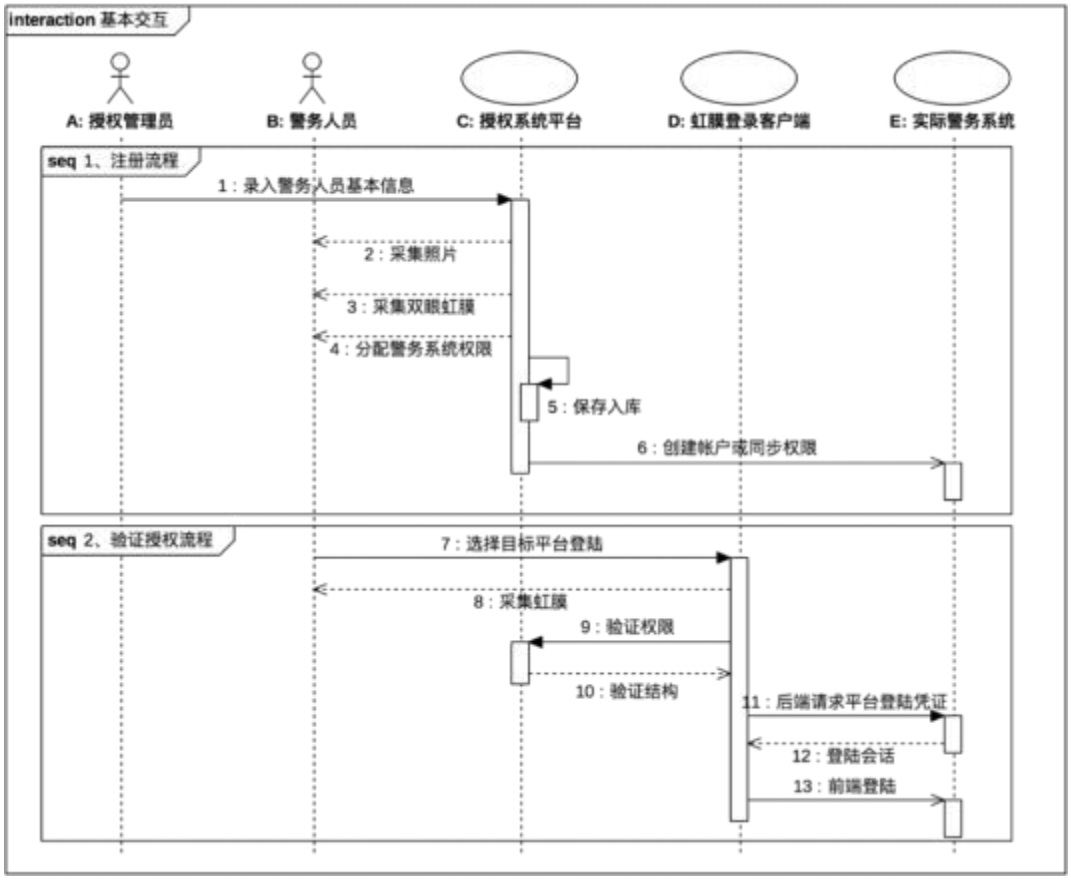


虹膜数据库的用户虹膜特征值数据，由部署在前端的各注册授权客户端采集完成，授权人员根据职务分配业务系统账号及权限，并通过公安专网上传给后台服务器和数据库，完成建库过程。

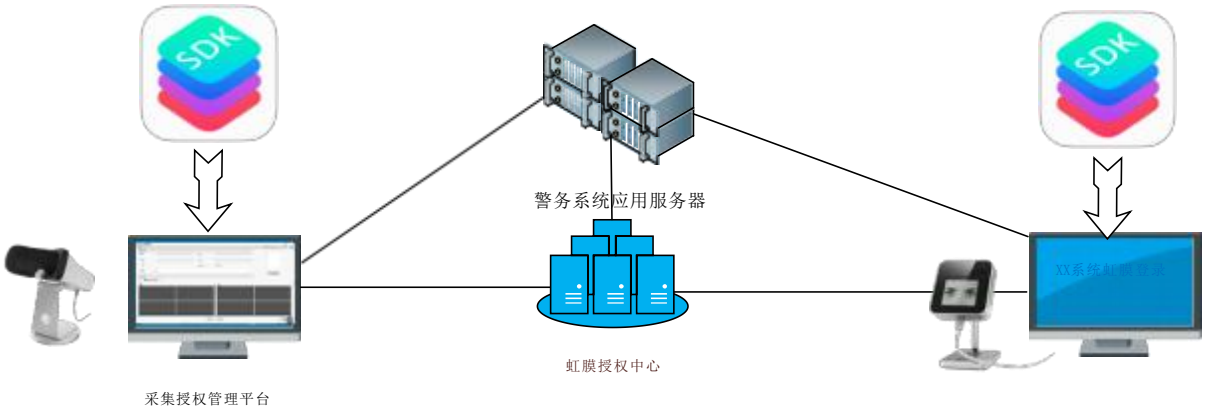
根据用户规模大小，在数据中心部署虹膜识别高速比对卡，负责在识别阶段， 接收虹膜数据库下发的海量虹膜数据信息， 并根据识别设备上传的虹膜特征值，完成由虹膜数据信息的比对和比对结果输出， 保障海量数据环境下虹膜识别技术的识别效率。

前端的业务系统登录客户端负责完成识别过程中的虹膜特征值采集，通过网络上传给后台服务器和数据库，并接收服务器下发过来的虹膜数据比对结果，最后完成前端结果显示，完成认证过程。

2.3 警务系统虹膜注册登录工作流程



警务人员在授权管理员的帮助下，在虹膜注册授权平台， 采集警务人员的基本身份信息、人脸照片和虹膜信息， 保存在本地数据库，并根据职务分配对应业务系统的帐号和权限，保存到授权服务中心的虹膜数据库服务器，帐号信息和权限同步到实际的业务平台。警务人员需要登陆到业务系统时， 通过虹膜登陆客户端采集虹膜，上传到授权服务器进行比对。如果比对成功，则允许登陆；如果比对失败，则拒绝登陆。



2.4 主要产品介绍

2.4.1 虹膜采集器 HS-QDEV-CAP200

基于虹识技术乾芯虹膜识别芯片打造的 HS-QDEV-CAP200 给用户提供了一台简单易用的接触式 VR 虹膜采集器。该设备能够轻松捕捉到双目虹膜图像，只需要用户双眼靠近设备端即可完成虹膜图像的采集。同时，提供不同亮度的光源控制人眼瞳孔的大小，从而采集到不同光照下的虹膜图像，进一步提升虹膜识别的应用场景。

功能描述：

对虹膜进行采集，输出虹膜特征值，必要时可输出图像，放入虹膜数据库。

产品特点：

■搭载全球首发的虹膜识别芯片；

■全硬件超高安全的虹膜识别解决方案；

■业界最快的识别速度；

■识别精度比业界标准至少高一个数量级；

■高速高质量虹膜图像采集；

■高速准确的虹膜图像质量评估；

■无用户容量限制；

■可集成所有带 USB 口的设备；

■可实现虹膜注册、虹膜比对功能；

■自带屏幕可视化操作， 简单直观；

■双目自动采集；

■科技感的外观，增加用户使用欲望；

■眼罩式设计， 提升虹膜使用效率；

■多种瞳孔尺寸的虹膜图像采集；