



中华人民共和国国家标准

GB/T 20979—2007

信息安全技术 虹膜识别系统技术要求

Information security technology—
Technical requirements for iris recognition system

2007-06-18 发布

2007-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

中 华 人 民 共 和 国
国 家 标 准
信 息 安 全 技 术
虹 膜 识 别 系 统 技 术 要 求

GB/T 20979—2007

*

中国标准出版社出版发行
北京西城区复兴门外三里河北街16号

邮政编码:100045

<http://www.spc.net.cn>

<http://www.gb168.cn>

电话:(010)51299090、68522006

2007年10月第一版

*

书号:155066·1-29961

版权专有 侵权必究
举报电话:(010)68522006

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 基本功能要求	3
4.1 自包含	3
4.2 虹膜图像采集与处理	3
4.3 用户标识	3
4.4 用户登记	4
4.5 用户识别	4
4.6 识别失败的判定及处理	4
4.7 防伪造	5
4.8 警告与报警	5
5 基本性能要求	5
5.1 错误接受率和错误拒绝率	5
5.2 响应时间	5
5.3 适用范围	5
5.4 使用安全条件	5
6 分等级技术要求	5
6.1 第一级技术要求	5
6.1.1 基本功能要求	5
6.1.2 基本性能要求	6
6.1.3 自身安全功能要求	6
6.1.4 自身安全保证要求	7
6.2 第二级技术要求	8
6.2.1 基本功能要求	8
6.2.2 基本性能要求	9
6.2.3 自身安全功能要求	9
6.2.4 自身安全保证要求	10
6.3 第三级技术要求	11
6.3.1 基本功能要求	11
6.3.2 基本性能要求	12
6.3.3 自身安全功能要求	12
6.3.4 自身安全保证要求	14
附录 A (资料性附录) 虹膜识别基本原理	15
A.1 虹膜识别系统的组成与功能	15
A.1.1 组成与相互关系	15

A.1.2 虹膜识别系统功能简要说明	15
A.1.3 虹膜识别系统各模块主要功能说明	15
A.2 虹膜识别系统的工作流程	15
A.3 虹膜识别机制的主体与客体	16
附录 B (资料性附录) 虹膜识别系统功能和性能要素与分等级要求的对应关系	18
附录 C (规范性附录) 主、客体的访问操作关系	19
C.1 适用于第一级的主、客体之间的访问操作关系	19
C.2 适用于第二级和第三级的主、客体之间的访问操作关系	19
C.3 适用于第三级的主客体与图像数据库之间的访问操作关系	20
附录 D (规范性附录) 虹膜特征序列数据库数据结构	21
参考文献	22

前 言

本标准的附录 C、附录 D 是规范性附录，附录 A、附录 B 是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京凯平艾森信息技术有限公司、最高人民法院机关服务局信息技术服务处。

本标准主要起草人：王介生、吉增瑞、孙际泉、王静、王钦、徐金伟、白杰。

引 言

本标准用以指导设计者如何设计和实现具有所要求级别的虹膜识别系统,说明不同级别的虹膜识别系统的不同技术要求。

虹膜是瞳孔和巩膜之间的环状组织,是人眼的可见部分。作为人体生物特征识别的虹膜识别,与其他生物特征识别和非生物特征识别一样,具有鉴别用户身份真实性的功能。虹膜特征识别技术由于其高效、准确、难以伪造等特性受到关注。为了对虹膜识别技术进行规范,推动我国具有自主知识产权的虹膜识别技术的发展,为信息系统安全保护及社会保安提供有效、实用的人体身份鉴别手段,有必要制定虹膜识别系统的安全标准。

附录 A 是对虹膜识别原理的简要介绍。虹膜识别系统由软件系统和硬件系统组成。软件系统即虹膜信息处理系统,用以实现虹膜图像处理、用户登记、用户识别、虹膜图像存储管理、虹膜特征存储管理等功能;硬件系统包括虹膜图像采集系统以及支持虹膜信息处理软件系统运行的硬件环境。上述软硬件系统构成一个完整的信息处理系统,实现虹膜识别功能。虹膜识别系统的输入信息是虹膜图像,输出信息是识别结果。能够对虹膜识别系统的运行进行操作和干预的是系统管理员、系统安全员和系统审计员等特权用户。这些特权用户必须经过确认授权以后,才能实施所规定的操作。

虹膜识别系统可以看成是一个由各个软、硬件模块组成的专用的计算机应用系统。本标准将重点描述:作为专用系统所具备的虹膜识别功能和性能要求;作为计算机应用系统的虹膜识别系统的软、硬件系统的自身安全要求;虹膜识别系统运行环境的安全要求。

根据应用环境的不同,虹膜识别系统可以有独立运行和联机运行两种模式。

独立运行模式:将组成虹膜识别系统的虹膜识别机制全部封装在一个专用的机箱中,构成一个独立的系统,其应用领域是社会公共安全防范(如门禁)。这时,虹膜识别系统通过确定的外部接口为安全防范控制提供支持。其输入信息是所采集的虹膜图像,输出信息是控制传感系统的控制信号。

联机运行模式:将组成虹膜识别系统的虹膜识别机制嵌入在信息系统中,在组成信息系统的计算机系统和网络系统的支持下,构成一个实现虹膜识别的子系统,并通过确定的外部接口为信息系统用户的身份鉴别提供支持。这时,虹膜识别系统的输入信息是虹膜图像,输出信息是为信息系统的用户身份鉴别功能提供支持的虹膜特征识别结果。

上述虹膜识别系统的不同运行模式是根据应用需要确定的。从虹膜识别系统的组成与原理的角度看,并没有本质上的区别。因此,本标准的编写没有对不同运行模式的情况加以区分。需要特别说明的是,本标准所描述的技术要求是指虹膜识别系统所涉及的技术要素的要求。为了满足不同情况对虹膜识别系统的不同要求,本标准分三个级别对虹膜识别系统所涉及的功能和性能的技术要求以及相应的自身安全的技术要求分别进行了描述。其中,第 1 级为最低要求,第 3 级为最高要求。附录 B 的表 B.1 是虹膜识别系统功能和性能要素与分等级要求的对应关系的简明表示。需要指出的是,虹膜识别系统的自身安全保护是与其运行模式和实现的功能密切相关的。比如,独立运行模式不涉及信息的网上传输,因而不涉及网上信息传输的安全保护问题。在理解和使用本标准时,应从实际出发,根据虹膜识别系统的运行模式和实现的功能确定其自身的安全保护要求。

本标准第 4 章和第 5 章分别是对虹膜识别系统基本功能和基本性能要求的综合描述,第 6 章是对不同等级的虹膜识别系统在基本功能与性能、安全功能和安全保证方面的不同技术要求的描述。其中,宋体加粗字表示相应要求在该等级中第一次出现。

信息安全技术

虹膜识别系统技术要求

1 范围

本标准规定了用虹膜识别技术为身份鉴别提供支持的虹膜识别系统的技术要求。

本标准适用于按信息安全等级保护的要求所进行的虹膜识别系统的设计与实现,对虹膜识别系统的测试、管理也可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

3 术语和定义

GB 17859—1999 和 GB/T 20271—2006 确立的以及下列术语和定义适用于本标准。

3.1

人体生物特征识别 Biometrics, biometric authentication

以人体的某种生物特征信息作为身份依据进行用户识别的方法。通过测度该种人体生物特征,为每一个人产生出可以用电子方式存储、检索和比对的特征信息,并用这种特征信息进行用户识别。

3.2

虹膜 iris

人体眼球中介于瞳孔与巩膜之间的环状生理组织,是人眼的可见部分。

3.3

虹膜识别 iris recognition

以虹膜特征作为识别人体身份的方法,是人体生物特征识别方法的一种。

3.4

虹膜识别机制 iris recognition mechanism

按照确定的策略和方法,实现虹膜特征识别功能的所有软、硬件装置的总称。

3.5

虹膜识别系统 iris recognition system

实现虹膜识别功能的专用信息处理系统。虹膜识别系统可以是一个由软、硬件构成的独立系统,也可以是在信息系统已有平台上运行的嵌入式系统。

3.6

虹膜图像采集器 iris image grabber

虹膜识别系统的一个部件,用于进行虹膜图像采集。