ICS 35.040
L 80

# 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

# 目　　录

# 前　　言

（略）

# 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 authentification

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。

3.7

**自包含** self-contained

虹膜识别系统的一项重要的功能特性。如果一个虹膜识别系统具有虹膜图像采集器和虹膜信息处理软、硬件，能够独立实现虹膜图像采集、虹膜图像处理、虹膜特征序列生成及虹膜特征序列比对等虹膜识别系统的各项功能，则称其为自包含式系统，或称其具有自包含功能。

3.8

**用户** user

指虹膜识别系统用以识别的对象，分为一般用户和特权用户。

3.9

**一般用户和特权用户** general user and special user

一般用户和特权用户由虹膜识别系统的管控人员根据应用需求确定。例如，当虹膜识别用于信息系统的用户身份鉴别时，具有普通权限的用户可为一般用户，具有特殊权限的用户（如信息系统管理员、安全员和审计员等）可为特权用户。

3.10

**用户登记** user enrollment

分析用户虹膜图像、提取虹膜数字特征、产生并存贮模板特征序列的过程。

3.11

**用户识别** user recognition

分析用户虹膜图像、提取虹膜数字特征、产生样本特征序列，并将该样本特征序列与已存贮的模板特征序列进行比对，用以识别用户身份的过程。用户识别分为用户辨识和用户确认。

3.12

**用户辨识** user identification

将所产生的样本特征序列与已存贮的指定范围内的所有用户的模板特征序列进行比对（1：N 比对），选出相符的用户，以揭示用户的实际身份。

3.13

**用户确认** user validation

将所产生的样本特征序列与按用户标识信息给定的已存储的用户的模板特征序列进行比对（1：1 比对），以确定用户所声称的身份。

3．14

**特征序列** characteristic sequence

由虹膜图像数字特征组成的数据序列。虹膜图像数字特征是通过对虹膜图像进行分析提取的。特征序列包括模板特征序列和样本特征序列。

3.15

**模板特征序列** template characteristic sequence

对采集到的用户登记虹膜图像进行分析提取所生成的特征序列。产生模板特征序列的目的必须是用于用户登记。

3.16

**样本特征序列** sample characteristic sequence

对采集到的用户虹膜图像进行分析提取所生成的特征序列。产生样本特征序列的目的必须是用于用户识别。

3.17

**虹膜识别数据** iris authentication data

用于进行虹膜识别的数据，包括模板特征序列数据和样本特征序列数据以及虹膜识别过程中用到

的其它数据。

3.18

**候选者** candidate

通过用户辨识所确定的用户。该用户是在已进行过用户登记的所有用户中选出的符合当前样本特征序列数据要求的用户。

3.19

**虹膜特征序列数据库** iris characteristic sequence database

专门用于存放虹膜模板特征序列数据的数据库，简称为虹膜特征序列数据库。

3.20

**不透明数据** （opaque data）

不透明数据是虹膜特征序列数据库记录的组成部分，由模板特征序列、有效载荷和防伪数据组成。

3.21

**有效载荷** payload

封装在不透明数据中的由用户给出的数据，如：密钥等，在用户识别成功时可以将有效载荷释放出来，用以对该用户进行授权等操作。

3.22

**比对次数** march time

在测试过程中，同一虹膜组织的所有模板特征序列与同一虹膜组织的所有样本特征序列之间的所有比对，计为一次比对。在统计比对次数时，同一虹膜组织生成的所有模板特征序列或由其生成的所有样本特征序列都分别被看作是同一特征序列。不同比对的总次数称为总比对次数。

3.23

**错误接受率** false accept rate

在进行样本特征序列与模板特征序列的比对过程中，对于本该产生拒绝结果的比对，错误地产生了接受结果，产生这类错误结果的比对次数，与总比对次数的比率的测定值。

3.24

**错误拒绝率** false reject rate

在进行样本特征序列与模板特征序列的比对过程中，对于本该产生接受结果的比对，错误地产生了拒绝结果，产生这类错误结果的比对次数，与总比对次数的比率的测定值。

## 4 基本功能要求

### 4.1 自包含

一个完整的虹膜识别系统应具有自包含功能。

### 4.2 虹膜图像采集与处理

应提供对虹膜图像进行采集与处理的功能。虹膜图像采集与处理应满足以下要求：

——由虹膜图像采集设备按要求进行虹膜图像的采集；

——按要求对采集到的虹膜图像进行处理，产生用于进行用户登记和用户识别的虹膜特征序列数据信息。

### 4.3 用户标识

应提供用户标识功能。用户标识应满足以下要求：

——所有用户在用户登记时都进行用户标识；

——用户标识以用户名和用户标识符（ID）实现；

——应确保同一信息系统中用户标识的唯一性。

### 4.4 用户登记

#### 4.4.1 基本要求

应提供用户登记功能。用户登记应满足以下要求：

——只应将获准进行登记的用户的虹膜特征序列作为模板特征序列存入特征序列数据库；

——同一用户在相关的信息系统中的模板特征序列应具有相同的数据库记录结构（见附录D），以保持模板特征序列的一致性，便于信息共享和集中管理；

——用户登记是一次性过程，即对同一特征序列数据库的用户只应登记一次；

——应对用户登记进行审计。

#### 4.4.2 两幅图像要求

以两幅以上（含两幅）图像生成的虹膜特征序列实现用户登记。

#### 4.4.3 四幅图像要求

以四幅以上（含四幅）图像生成的虹膜特征序列实现用户登记。

### 4.5 用户识别

#### 4.5.1 基本要求

应提供用户识别功能。用户识别包括用户辨识和用户确认两种功能。

a) 用户辨识应满足以下要求：

——进行用户辨识时，用户虹膜图像是唯一的用户辨识信息；

——将实时采集的用户虹膜图像生成的样本特征序列与存贮的模板特征序列逐一进行比对，产生用于用户辨识的比对结果。

b) 用户确认应满足以下要求：

——进行用户确认时，需要虹膜图像信息和用户标识信息；

——根据用户标识信息，从特征序列数据库中检索出该用户的模板特征序列；

——将实时采集的用户虹膜图像生成的样本特征序列与检索出的用户模板特征序列进行比对，产生用于用户确认的比对结果。

#### 4.5.2 两幅图像要求

以两幅图像以上（含两幅）生成的虹膜特征序列实现用户识别。

#### 4.5.3 四幅图像要求

以四幅图像以上（含四幅）生成的虹膜特征序列实现用户识别。

### 4.6 识别失败的判定及处理

虹膜识别系统在识别过程中，当出现以下情形中的一项或多项时，系统应能准确地判断出识别失败：

a） 设备故障：不能成功采集图像；

b） 像质障碍：采集的图像质量不适于生成模板特征序列或生成样本特征序列；

c） 超时断开：终端操作超时断开；

d） 数据库故障：特征序列数据库故障且在规定尝试次数内未能消除；

e） 尝试超次：对用户确认与用户辨识，应分别设定警告次数阈值，连续警告次数大于该阈值时视作失败。

对识别失败的处理，应提供以下功能：

——制定识别失败返回值表；

——在出现识别失败情况时，按照失败返回值表返回错误代码或错误值；

——针对不同识别失败原因进行相应处理。

### 4.7 防伪造

虹膜识别系统应具有防伪造功能。根据不同等级的要求，防伪造功能应有选择地满足以下要求：

a） 防照片伪造：应能检测或防止使用照片伪造识别图像；

b） 防隐形镜片伪造：应能检测或防止在隐形镜片上复制伪造识别图像；

c） 防复制伪造：应能检测或防止对当前用户识别数据的复制和非授权保存；

d） 防录像伪造：应能检测或防止使用录像伪造识别图像；

e） 防死亡虹膜伪造：应能检测或防止用已经死亡的虹膜组织取代活体虹膜组织。

### 4.8 警告与报警

虹膜识别系统的警告与报警应满足以下要求：

——进行用户确认时，如用户不是所给 ID 或其他用户身份信息的持有者，或在进行用户辨识时，已存贮的模板特征序列中无用户的候选者，应给出警告信息；

——检测出伪造识别图像、识别数据，或复制图像、数据，或非授权保存图像、数据，或非授权数据库操作时，应给出报警信息。

## 5 基本性能要求

### 5.1 错误接受率和错误拒绝率

虹膜识别系统的错误接受率和错误拒绝率应能进行调节，使其中之一变大时另一个变小，以满足不同的应用需要。不同等级的虹膜识别系统应分别满足以下的错误接受率和错误拒绝率要求：

a） 在总测试次数不小于一万次时，错误接受率不大于万分之一，错误拒绝率不大于百分之一；

b） 在总测试次数不小于十万次时，错误接受率不大于十万分之一，错误拒绝率不大于百分之一；

c） 在总测试次数不小于三十万次时，错误接受率不大于三十万分之一，错误拒绝率不大于千分之一。

### 5.2 响应时间

虹膜识别系统功能的实现，应在充分考虑承载其运行的处理器速度 、存储器容量、数据处理量和其它相关因素的基础上，采取有效的算法，确保其时间与速度能满足使用的需要。

### 5.3 适用范围

虹膜识别系统的适用范围应满足：

——适用于各种人种的虹膜识别，既能用于深色虹膜人种，也能用于浅色虹膜人种；

——既能用于本地用户的虹膜识别，也能用于远程用户的虹膜识别；

——既能用于一般用户的虹膜识别，也能用于特权用户的虹膜识别。

### 5.4 使用安全条件

虹膜识别系统所提供的使用安全条件应满足：

——采用无伤害照明。

## 6 分等级技术要求

### 6.1 第一级技术要求

#### 6.1.1 基本功能要求

##### 6.1.1.1 自包含

应按 4.1 的要求实现自包含功能。

##### 6.1.1.2 虹膜图像采集与处理

应按 4.2 的要求实现图像处理功能。

##### 6.1.1.3 用户标识

应按 4.3 的要求实现用户标识功能。

6.1.1.4 用户登记

应按 4.4 的要求从以下方面实现用户登记功能：

a) 对一般用户和特权用户，按 4.4.1 和 4.4.2 的要求进行用户登记；

b) 以数据库或文件形式将用户模板特征序列进行存储；

c) 有效载荷数据部分可为空。

d) 签名部分可为空。

6.1.1.5 用户识别

应按 4.5 的要求从以下方面实现用户识别功能：

a) 对一般用户和特权用户，按 4.5.1 和 4.5.2 的要求进行用户识别；

b) 用样板特征序列进行用户辨识和用户确认。

6.1.1.6 识别失败判定及处理

应按 4.6 的要求，从以下方面实现识别失败判定及处理功能：

a) 对设备故障、像质障碍、超时断开所引起的识别失败事件进行判定；

b) 在同一用户连续 4 次未能通过用户确认或用户辨识时，做出识别失败判定；

c) 在用户未能通过用户确认或用户辨识时显示识别失败信息；

d) 按 4.6 中的相应要求，实现识别失败处理功能。

6.1.1.7 防伪造

应具有以下防伪造功能：

a) 按 4.7 中防复制伪造的要求检测并防止伪造用户识别图像；

b) 在检测出伪造或非授权操作事件时应终止违例进程并取消服务。

6.1.2 基本性能要求

6.1.2.1 错误接受率和错误拒绝率要求

应按 5.1 的要求进行错误接受率与错误拒绝率设计，并同时满足：

a) 错误接受率不大于万分之一；

b) 错误拒绝率不大于百分之一。

6.1.2.2 响应时间要求

应按 5.2 关于响应时间的要求进行虹膜识别系统的设计。

6.1.2.3 适用范围要求

应按 5.3 关于适用范围的要求进行虹膜识别系统的设计。

6.1.2.4 使用安全条件要求

应按 5.4 关于使用安全条件的要求进行虹膜识别系统的设计。

6.1.3 自身安全功能要求

6.1.3.1 物理安全要求

6.1.3.1.1 环境安全

应按 GB/T 20271-2006 中 6.2.1.1 的要求，对运行虹膜识别的软、硬件环境进行保护。

6.1.3.1.2 设备安全

每台虹膜识别设备都应有明显的无法除去的标记，以防更换和方便丢失后查找。

6.1.3.1.3 记录介质安全

应按 GB/T 20271-2006 中 6.2.1.3 的要求，对存放虹膜特征序列数据的脱机存储介质应进行保护。

6.1.3.2 运行安全要求

6.1.3.2.1 风险分析

应按 GB/T 20271-2006 中 6.2.2.1 的要求，从以下方面进行虹膜识别系统的风险分析：

a) 根据用户使用要求和使用环境，对虹膜识别系统进行设计前的风险分析，确定系统的安全需求；

b) 对运行中的虹膜识别系统，定期或根据需要进行动态风险分析，发现安全漏洞，确定安全对策。

6.1.3.2.2 系统安全性检测分析

应按 GB/T 20271-2006 中 6.2.2.2 的要求，从以下方面对虹膜识别系统的安全性进行检测分析：

a) 对支持虹膜识别系统运行的操作系统进行安全性检测分析，发现其安全性问题，提出补救措施；

b) 对虹膜识别系统自身的安全性进行检测分析，发现其安全性问题，提出补救措施。

6.1.3.2.3 安全审计

应按 GB/T 20271-2006 中 6.2.2.3 的要求，从以下方面设计虹膜识别系统的安全审计功能：

a) 按要求对需要审计的事件做出响应；

b) 按要求产生审计数据；

c) 按要求对审计数据进行保护；

d) 按要求提供审计事件的查阅功能。

6.1.3.2.4 备份与故障恢复

应按 GB/T 20271-2006 中 6.2.2.5 的要求，设置虹膜识别系统的信息备份与恢复功能。

6.1.3.3 数据安全要求

6.1.3.3.1 系统管理员身份鉴别

应按 GB/T 20271-2006 中 6.2.3.1 的要求，对虹膜识别系统的系统管理员进行身份鉴别，确认其身份的真实性。

6.1.3.3.2 访问控制

应按 GB/T 20271-2006 中 6.2.3.2 的要求，根据附录 C 表 C.1 所表示的主、客体对应关系及操作规则，实现对虹膜识别数据的访问控制。

6.1.3.3.3 数据完整性保护

应按 GB/T 20271-2006 中 6.2.3.3 的要求和 GB/T 20273-2006 中 5.2.1.4 的要求，从以下方面实现对虹膜识别数据的完整性保护：

a) 对被存储的模板特征序列数据和样本特征序列数据进行完整性保护；

b) 对被传输的模板特征序列数据和样本特征序列数据进行完整性保护；

c) 对被处理的模板特征序列数据和样本特征序列数据进行完整性保护。

6.1.3.3.4 数据保密性保护

应按 GB/T 20271-2006 中 6.2.3.4 的要求和 GB/T 20273-2006 中 5.2.1.5 的要求，从以下方面对虹膜识别数据进行保密性保护：

a) 对被存储的模板特征序列数据和样本特征序列数据进行保密性保护；

b) 对被传输的模板特征序列数据和样本特征序列数据进行保密性保护；

c) 对动态使用资源中的模板特征序列数据和样本特征序列数据进行剩余敏感信息保护。

6.1.4 自身安全保证要求

6.1.4.1 虹膜识别系统自身安全保护

按 GB/T 20271-2006 中 6.2.4 的要求，从以下方面设计和实现虹膜识别系统的自身安全保护：

a) 确保虹膜识别系统程序的完整性；

b) 确保虹膜识别系统的正确、不间断运行；

c) 确保虹膜识别系统有可靠的时间戳支持；

d) 确保虹膜识别设备在受到物理攻击时能及时进行报告。

6.1.4.2 虹膜识别系统设计与实现

按 GB/T 20271-2006 中 6.2.5 的要求，从以下方面设计和实现虹膜识别系统：

a) 按 GB/T 20271-2006 中 6.2.5.1 的要求，实现虹膜识别系统的配置管理；
b) 按 GB/T 20271-2006 中 6.2.5.2 的要求，实现虹膜识别系统的分发和操作；
c) 按 GB/T 20271-2006 中 6.2.5.3 的要求，实现虹膜识别系统的开发；
d) 按 GB/T 20271-2006 中 6.2.5.4 的要求，进行虹膜识别系统的文档编写；
e) 按 GB/T 20271-2006 中 6.2.5.5 的要求，实现虹膜识别系统的生命周期支持设计；
f) 按 GB/T 20271-2006 中 6.2.5.6 的要求，进行虹膜识别系统的测试；
g) 按 GB/T 20271-2006 中 6.2.5.7 的要求，进行虹膜识别系统的脆弱性评定。

#### 6.1.4.3 虹膜识别系统安全管理

按 GB/T 20271-2006 中 6.2.6 的要求，从以下方面实现虹膜识别系统的安全管理，制定相应的操作、运行规程和行为规章制度：

a) 虹膜识别系统的功能管理；
b) 虹膜识别系统的安全属性管理；
c) 虹膜识别系统的数据管理。

### 6.2 第二级技术要求

#### 6.2.1 基本功能要求

##### 6.2.1.1 自包含

应按 4.1 的要求实现自包含功能。

##### 6.2.1.2 虹膜图像采集与处理

应按 4.2 的要求实现图像处理功能。

##### 6.2.1.3 用户标识

应按 4.3 的要求实现用户标识功能。

##### 6.2.1.4 用户登记

应按 4.4 的要求从以下方面实现用户登记功能：

a) 对一般用户和特权用户，按 4.4.1 和 4.4.2 的要求进行用户登记；
b) 以数据库形式将用户模板特征序列进行存储；
c) 有效载荷数据部分的数据不应为空；
d) 签名数据部分可为空。

##### 6.2.1.5 用户识别

应按 4.5 的要求从以下方面实现用户识别功能：

a) 对一般用户和特权用户，按 4.5.1 和 4.5.2 的要求进行用户识别；
b) 用样板特征序列进行用户辨识和用户确认。

##### 6.2.1.6 识别失败的判定及处理

应按 4.6 的要求，从以下方面实现识别失败的判定及处理功能：

a) 对 4.6 中设备故障、像质障碍、超时断开、数据库故障所引起的识别失败事件进行判定；
b) 在同一用户连续 4 次未能通过用户确认或用户辨识时，做出识别失败判定；
c) 应在虹膜特征序列数据库出现故障时显示故障信息；
d) 应在用户未能通过用户确认或用户辨识时显示识别失败信息；
e) 按 4.6 中的相应要求，实现识别失败处理功能。

##### 6.2.1.7 防伪造

应具有以下防伪造功能：

a) 按 4.7 中防照片伪造、防隐形镜片伪造、防复制伪造的要求检测并防止伪造用户识别图像；
b) 在检测出伪造或非授权操作事件时应终止违例进程并取消服务。

6.2.1.8 警告与报警

应按 4.8 的要求实现警告与报警功能。

6.2.2 基本性能要求

6.2.2.1 错误接受率和错误拒绝率要求

应按 5.1 的要求进行错误接受率与错误拒绝率设计，并同时满足：

a) 错误接受率不大于十万分之一；

b) 错误拒绝率不大于百分之一。

6.2.2.2 响应时间要求

应按 5.2 关于响应时间的要求进行虹膜识别系统的设计。

6.2.2.3 适用范围要求

应按 5.3 关于适用范围的要求进行虹膜识别系统的设计。

6.2.2.4 使用安全条件要求

应按 5.4 关于使用安全条件的要求进行虹膜识别系统的设计。

6.2.3 自身安全功能要求

6.2.3.1 物理安全要求

6.2.3.1.1 环境安全

应按 GB/T 20271-2006 中 6.3.1.1 的要求，从以下方面对虹膜识别系统的运行环境进行安全保护：

a) 对安装虹膜图像采集器的环境应进行保护；

b) 对运行虹膜识别系统的软、硬件环境应进行保护。

6.2.3.1.2 设备安全

每台虹膜识别设备都应有明显的无法除去的标记，以防更换和方便丢失后查找。

6.2.3.1.3 记录介质安全

应按 GB/T 20271-2006 中 6.3.1.3 的要求，对存放虹膜特征序列数据的脱机存储介质进行保护。

6.2.3.2 运行安全要求

6.2.3.2.1 风险分析

应按 GB/T 20271-2006 中 6.3.2.1 的要求，从以下方面进行虹膜识别系统的风险分析：

a) 根据用户使用要求和使用环境，对虹膜识别系统进行系统设计前的风险分析，确定系统的安全需求；

b) 对设计完成的虹膜识别系统，进行运行前的静态风险分析，以发现系统的潜在安全隐患，并提出改进措施；

c) 对运行中的虹膜识别系统，定期或根据需要进行动态风险分析，发现安全漏洞，确定安全对策。

6.2.3.2.2 系统安全性检测分析

应按 GB/T 20271-2006 中 6.3.2.2 的要求，从以下方面对虹膜识别系统的安全性进行检测分析：

a) 对支持虹膜识别系统运行的操作系统进行安全性检测分析，发现其安全性问题，提出补救措施；

b) 对支持虹膜识别系统运行的数据库管理系统进行安全性检测分析，发现其安全性问题，提出补救措施；

c) 对支持虹膜识别系统运行的网络系统进行安全性检测分析，发现其安全性问题，提出补救措施；

d) 对虹膜识别系统自身的安全性进行检测分析，发现其安全性问题，提出补救措施。

6.2.3.2.3 安全审计

应按 GB/T 20271-2006 中 6.3.2.4 的要求，从以下方面设计虹膜识别系统的安全审计功能：

a) 按要求对伪造虹膜图像、伪造特征序列数据或篡改识别结果数据、企图保存虹膜图像、非授权保存特征序列数据、非授权进行数据库操作等事件做出响应；
b) 按要求产生审计数据；
c) 按要求对审计数据进行保护；
d) 按要求对审计事件进行分析；
e) 按要求提供审计事件的查阅功能；
f) 按要求对网络环境的审计进行集中管理。

#### 6.2.3.2.4 备份与故障恢复

应按 GB/T 20271-2006 中 6.3.2.6 的要求，从以下方面设置虹膜识别系统的备份与故障恢复功能：

a) 设置信息备份功能，并在虹膜识别系统运行中出现致使信息丢失的故障时，能进行信息恢复；
b) 设置系统备份功能，并在虹膜识别系统运行中出现致使系统无法运行的故障时，能进行恢复。

### 6.2.3.3 数据安全要求

#### 6.2.3.3.1 系统管理员身份鉴别

应按 GB/T 20271-2006 中 6.3.3.1 的要求，对虹膜识别系统的系统管理员进行身份鉴别。确认其身份的真实性。

#### 6.2.3.3.2 访问控制

应按 GB/T 20271-2006 中 6.3.3.4 和 6.3.3.5 的要求，根据附录 C 表 C.2 所表示的主、客体对应关系及操作规则，通过对主、客体设置敏感标记，实现对虹膜识别数据和虹膜特征序列数据信息的访问控制。

#### 6.2.3.3.3 数据完整性保护

应按 GB/T 20271-2006 中 6.3.3.7 的要求和 GB/T 20273-2006 中 5.3.1.7 的要求，从以下方面实现对虹膜识别数据的完整性保护：

a) 对被存储的虹膜识别数据进行完整性保护；
b) 对被传输的虹膜识别数据进行完整性保护；
c) 对被处理的虹膜识别数据进行完整性保护。

#### 6.2.3.3.4 数据保密性保护

应按 GB/T 20271-2006 中 6.3.3.8 的要求和 GB/T 20273-2006 中 5.3.1.8 的要求，从以下方面对虹膜识别数据进行保密性保护：

a) 对被存储的虹膜识别数据进行保密性保护；
b) 被传输的虹膜识别数据进行保密性保护；
c) 对动态使用资源中的虹膜识别数据进行剩余信息保护。

### 6.2.4 自身安全保证要求

#### 6.2.4.1 虹膜识别系统自身安全保护

应按 GB/T 20271-2006 中 6.3.4 的要求，从以下方面设计和实现虹膜识别系统的自身安全保护：

a) 确保虹膜识别系统程序的完整性；
b) 确保虹膜识别系统的正确、不间断运行；
c) 确保虹膜识别机制不会被旁路；
d) 确保虹膜识别系统有可靠的时间戳支持；
e) 确保虹膜识别设备在受到物理攻击时能及时进行报告；
f) 通过故障容错、服务优先级和资源分配，增强虹膜识别系统自身安全性；
g) 通过对与虹膜识别系统的会话限制，保护虹膜识别系统免遭相应攻击。

6.2.4.2 虹膜识别系统设计与实现

应按 GB/T 20271-2006 中 6.3.5 的要求，从以下方面设计和实现虹膜识别系统：

a) 按 GB/T 20271-2006 中 6.3.5.1 的要求，实现虹膜识别系统的配置管理；
b) 按 GB/T 20271-2006 中 6.3.5.2 的要求，实现虹膜识别系统的分发和操作；
c) 按 GB/T 20271-2006 中 6.3.5.3 的要求，实现虹膜识别系统的开发；
d) 按 GB/T 20271-2006 中 6.3.5.4 的要求，进行虹膜识别系统的文档编写；
e) 按 GB/T 20271-2006 中 6.3.5.5 的要求，实现虹膜识别系统的生命周期支持设计；
f) 按 GB/T 20271-2006 中 6.3.5.6 的要求，进行虹膜识别系统的测试；
g) 按 GB/T 20271-2006 中 6.3.5.7 的要求，进行虹膜识别系统的脆弱性评定。

6.2.4.3 虹膜识别系统安全管理

应按 GB/T 20271-2006 中 6.3.6 的要求，从以下方面设计和实现虹膜识别系统的安全管理，制定相应的操作、运行规程和行为规章制度：

a) 虹膜识别系统的功能管理；
b) 虹膜识别系统的安全属性管理；
c) 虹膜识别系统的数据管理；
d) 虹膜识别系统安全角色的定义与管理；
e) 虹膜识别系统安全机制的集中管理。

6.3 第三级技术要求

6.3.1 基本功能要求

6.3.1.1 自包含

应按 4.1 的要求实现自包含功能。

6.3.1.2 虹膜图像采集与处理

应按 4.2 的要求实现虹膜图像的采集与处理功能。

6.3.1.3 用户标识

应按 4.3 的要求实现用户标识功能。

6.3.1.4 用户登记

应按 4.4 的要求从以下方面实现用户登记功能：

a) 对一般用户，按 4.4.1 和 4.4.2 的要求进行用户登记；
b) 对特权用户，按 4.4.1 和 4.4.3 的要求进行用户登记；
c) 有效载荷、模板特征序列应以相应级别的密码进行加密保护；
d) 以数据库形式将用户模板特征序列进行存储；
e) 虹膜特征序列数据库数据结构中的签名数据部分不应为空；
f) 用户虹膜图像可根据需要以数据库形式保存；
g) 用户面部照片可根据需要采集并保存。

6.3.1.5 用户识别

应按 4.5 的要求从以下方面实现用户识别功能：

a) 对一般用户，按 4.5.1 和 4.5.2 的要求，以两幅虹膜图像生成的虹膜特征序列作为样板特征序列进行用户识别；
b) 对特权用户，按 4.5.1 和 4.5.3 的要求，以四幅虹膜图像生成的虹膜特征序列作为样板特征序列进行用户识别；
c) 用样板特征序列进行用户辨识和用户确认。

6.3.1.6 识别失败的判定及处理

应按 4.6 的要求，从以下方面实现识别失败的判定及处理功能：

a) 能对 4.6 中设备故障、像质障碍、超时断开、数据库故障、尝试超次等所引起的识别失败事件进行判定；
b) 能在同一用户连续 3 次未能通过用户确认或用户辨识时，做出识别失败判定；
c) 应在虹膜特征序列数据库出现故障时显示故障信息；
d) 应在用户未能通过用户确认或用户辨识时显示识别失败信息；
e) 按 4.6 中的相应要求，制定明确的识别失败处理策略，实现识别失败处理功能

#### 6.3.1.7 防伪造

应具有以下防伪造功能：

a) 按 4.7 中防照片伪造、防隐形镜片伪造、防复制伪造、防录像伪造、防死亡虹膜伪造的要求检测并防止伪造用户识别图像；
b) 在检测出伪造或非授权操作事件时应终止违例进程并取消服务。

#### 6.3.1.8 警告和报警

应按 4.8 的要求实现警告和报警设计。

### 6.3.2 基本性能要求

#### 6.3.2.1 错误接受率和错误拒绝率要求

应按 5.1 的要求进行错误接受率与错误拒绝率设计，并同时满足：

a) 错误接受率不大于三十万分之一；
b) 错误拒绝率不大于千分之一。

#### 6.3.2.2 响应时间要求

应按 5.2 关于响应时间的要求进行虹膜识别系统的设计。

#### 6.3.2.3 适用范围要求

应按 5.3 关于适用范围的要求进行虹膜识别系统的设计。

#### 6.3.2.4 使用安全条件要求

应按 5.4 关于使用安全条件的要求进行虹膜识别系统的设计。

### 6.3.3 自身安全功能要求

#### 6.3.3.1 物理安全要求

##### 6.3.3.1.1 环境安全

应按 GB/T 20271-2006 中 6.4.1.1 的要求，从以下方面对虹膜识别系统的运行环境进行安全保护：

a) 对安装虹膜图像采集器的环境应进行保护；
b) 对运行虹膜识别的软、硬件环境应进行保护；
c) 对传输虹膜识别系统信息的网络环境进行保护。

##### 6.3.3.1.2 设备安全

每台虹膜识别设备都应有明显的无法除去的标记，以防更换和方便丢失后查找。

##### 6.3.3.1.3 记录介质安全

应按 GB/T 20271-2006 中 6.4.1.3 的要求，从以下方面对脱机存放虹膜识别系统数据的介质进行安全保护：

a) 对存放虹膜特征序列数据的脱机存储介质应进行保护；
b) 对存放虹膜图像数据、面部照片的脱机存储介质进行保护。

#### 6.3.3.2 运行安全要求

##### 6.3.3.2.1 风险分析

应按 GB/T 20271-2006 中 6.4.2.1 的要求，从以下方面进行虹膜识别系统的风险分析：

a) 根据用户使用要求和使用环境，对虹膜识别系统进行系统设计前的风险分析，确定系统的安全需求；

b) 对设计完成的虹膜识别系统，进行运行前的静态风险分析，以发现系统的潜在安全隐患，并提出改进措施；

c) 对运行中的虹膜识别系统，定期或根据需要进行动态风险分析，发现安全漏洞，确定安全对策。

#### 6.3.3.2.2 系统安全性检测分析

应按 GB/T 20271-2006 中 6.4.2.2 的要求，从以下方面对虹膜识别系统的安全性进行检测分析：

a) 对支持虹膜识别系统运行的操作系统进行安全性检测分析，发现其安全性问题，提出补救措施；

b) 对支持虹膜识别系统运行的数据库管理系统进行安全性检测分析，发现其安全性问题，提出补救措施；

c) 对支持虹膜识别系统运行的网络系统进行安全性检测分析，发现其安全性问题，提出补救措施；

d) 对虹膜识别系统自身的安全性进行检测分析，发现其安全性问题，提出补救措施。

#### 6.3.3.2.3 安全审计

应按 GB/T 20271-2006 中 6.4.2.4 的要求，从以下方面设计虹膜识别系统的安全审计功能：

a) 按要求对伪造虹膜图像、伪造特征序列数据或篡改识别结果数据、企图保存虹膜图像、非授权保存特征序列数据、非授权进行数据库操作等事件做出响应；

b) 按要求产生审计数据；

c) 按要求对审计数据进行保护；

d) 按要求对审计事件进行分析；

e) 按要求提供审计事件的查阅功能；

f) 按要求对网络环境的审计进行集中管理。

#### 6.3.3.2.4 备份与故障恢复

应按 GB/T 20271-2006 中 6.4.2.6 的要求，设置虹膜识别系统的备份与故障恢复功能：

a) 设置信息备份功能，并在虹膜识别系统运行中出现致使信息丢失的故障时，能进行信息恢复；

b) 设置系统备份功能，并在虹膜识别系统运行中出现致使系统无法运行的故障时，能进行恢复。

### 6.3.3.3 数据安全要求

#### 6.3.3.3.1 系统管理员身份鉴别

应按 GB/T 20271-2006 中 6.4.3.1 的要求，对虹膜识别系统的系统管理员进行身份鉴别，确认其身份的真实性。

#### 6.3.3.3.2 访问控制

应按 GB/T 20271-2006 中 6.4.3.4 和 6.4.3.5 的要求，根据附录 C 表 C.2 和表 C.3 所表示的主、客体对应关系及操作规则，通过对主、客体设置附加敏感标记，实现对虹膜识别数据、虹膜特征序列数据、面部照片及有效载荷数据信息的访问控制。对虹膜特征序列数据库的访问控制粒度应为库/表级、记录级、字段级。

#### 6.3.3.3.3 数据完整性保护

应按 GB/T 20271-2006 中 6.4.3.7 的要求和 GB/T 20273-2006 中 5.4.1.7 的要求，从以下方面实现对虹膜识别数据的完整性保护：

a) 对被存储的虹膜识别数据进行完整性保护；

b) 对被传输的虹膜识别数据进行完整性保护；

c) 对被处理的虹膜识别数据进行完整性保护。

#### 6.3.3.3.4 数据保密性保护

应按 GB/T 20271-2006 中 6.4.3.8 的要求和 GB/T 20273-2006 中 5.4.1.8 的要求，从以下方面对虹膜识别数据进行保密性保护：

a) 对被存储的虹膜识别数据进行保密性保护；

b) 对被传输的虹膜识别数据进行保密性保护；

c) 对动态使用资源中的虹膜识别数据进行剩余信息保护。

### 6.3.4 自身安全保证要求

#### 6.3.4.1 虹膜识别系统自身安全保护

应按 GB/T 20271-2006 中 6.4.4 的要求，从以下方面设计和实现虹膜识别系统的自身安全保护：

a） 确保虹膜识别系统程序的完整性；

b） 确保虹膜识别系统数据的完整性；

c） 确保虹膜识别系统的正确、不间断运行；

d） 确保虹膜识别机制不会被旁路；

e） 确保虹膜识别机制不会被替换；

f） 确保虹膜识别系统有可靠的时间戳支持；

g） 确保虹膜识别设备在受到物理攻击时能及时进行报告；

h） 通过故障容错、服务优先级和资源分配增强虹膜识别系统自身安全性；

i） 通过对与虹膜识别系统的会话限制保护虹膜识别系统的免遭相应攻击。

#### 6.3.4.2 虹膜识别系统设计与实现

应按 GB/T 20271-2006 中 6.4.5 的要求，从以下方面设计和实现虹膜识别系统：

a） 按 GB/T 20271-2006 中 6.4.5.1 的要求，实现虹膜识别系统的配置管理；

b） 按 GB/T 20271-2006 中 6.4.5.2 的要求，实现虹膜识别系统的分发和操作；

c） 按 GB/T 20271-2006 中 6.4.5.3 的要求，实现虹膜识别系统的开发；

d） 按 GB/T 20271-2006 中 6.4.5.4 的要求，进行虹膜识别系统的文档编写；

e） 按 GB/T 20271-2006 中 6.4.5.5 的要求，实现虹膜识别系统的生命周期支持设计；

f） 按 GB/T 20271-2006 中 6.4.5.6 的要求，进行虹膜识别系统的测试；

g） 按 GB/T 20271-2006 中 6.4.5.7 的要求，进行虹膜识别系统的脆弱性评定。

#### 6.3.4.3 虹膜识别系统安全管理

应按 GB/T 20271-2006 中 6.4.6 的要求，从以下方面设计和实现虹膜识别系统的安全管理，制定相应的操作、运行规程和行为规章制度：

a） 虹膜识别系统的功能管理；

b） 虹膜识别系统安全属性的管理；

c） 虹膜识别系统数据的管理；

d） 虹膜识别系统安全角色的定义与管理；

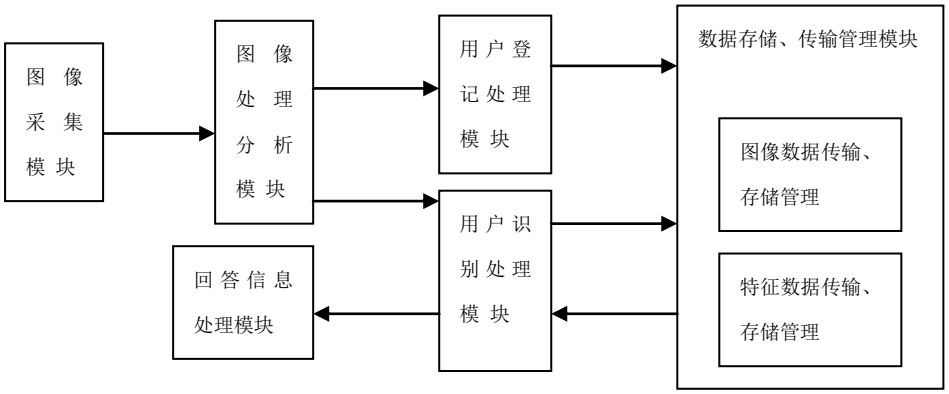
e） 虹膜识别系统安全机制的集中管理。

# 附录A
# （资料性附录）
# 虹膜识别基本原理

## A.1 虹膜识别系统的组成与功能

### A.1.1 组成与相互关系

图 A.1 给出了虹膜识别系统的基本组成与相互关系。




### A.1.2 虹膜识别系　　图 A.1 虹膜识别系统的组成与相互关系

虹膜识别系统包含图像采集、图像处理分析、用户登记处理、用户识别处理、数据存储传输管理、回答信息处理等功能模块。这些模块用以实现两种基本功能：用户登记和用户识别。进行用户登记或识别时，由图像采集模块采集用户虹膜图像，经图像处理分析模块处理，当用户登记时，由用户登记处理模块生成用户登记信息并存入数据库；当用户识别时，由用户识别处理模块生成用户识别信息，并将识别信息与登记信息进行比对，得出识别结果。用户登记是一次性过程，一个用户只登记一次。用户登记信息应具有一致的形式，以加强安全管理并节省资源。

### A.1.3 虹膜识别系统各模块主要功能说明

虹膜识别系统各模块主要功能说明如下：

a) 虹膜图像采集模块：按要求采集被识别对像的虹膜图像；

b) 虹膜图像处理模块：按要求对采集到的虹膜图像进行分析处理，产生用于进行用户登记和用户识别处理的虹膜特征序列数据信息。图像处理分析模块包括图像处理和图像分析两个子模块。图像处理子模块将虹膜图像变化为经过一定数字处理的虹膜图像；图像分析子模块是将经过数字处理的虹膜图像信息转化为某种非图像信息；

c) 用户登记处理模块：根据虹膜图像处理模块提供的信息，进行用户登记处理，并将虹膜特征数据信息和/或虹膜图像数据信息提交数据存储管理模块进行存储；

d) 用户识别处理模块：根据虹膜图像处理模块提供的信息，以及由数据存储管理模块所提供的信息，进行用户识别处理，并按识别结果形成回答信息；

e) 虹膜数据存储传输管理模块：按确定的数据结构，对虹膜图像数据和虹膜特征数据进行存储管理，为用户登记处理和用户识别处理提供支持，

f) 回答信息处理模块:根据需要将来自用户识别处理模块的回答信息转换成所要求的表示形式，为上层应用提供支持。

## A.2 虹膜识别系统的工作流程

图 A.2 展示虹膜识别的工作流程。

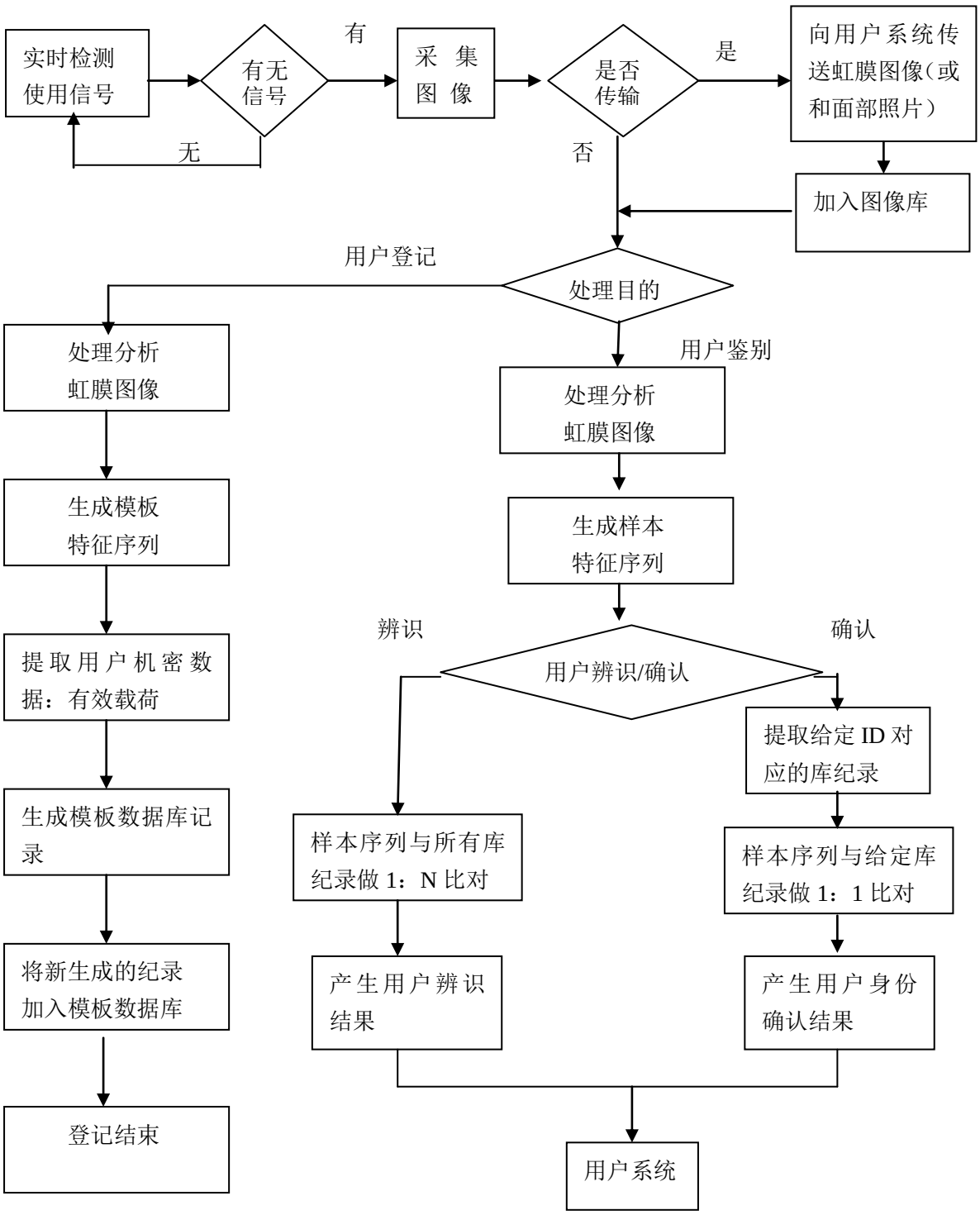



图 A.2　虹膜识别的工作流程

## A.3　虹膜识别机制的主体与客体

作为用于用户身份鉴别的专用信息安全机制，虹膜识别系统是一个专用的信息处理系统。其主体与客体分别是在一定范围内的实体成分。

### A.3.1 主体

虹膜识别机制中有两类主体：一类是特权用户，包括系统管理员、系统安全员和系统审计员；另一类是处理专门事务的系统进程。

系统管理员的主要职责是，通过专门为管理员提供的操作界面进行系统安装、启动，并对存放虹

膜图像的图像库和存放模板特征序列的数据库进行维护，以及进行用户登记；系统安全员的主要功能是，进行主、客体敏感信息的设置，这些敏感信息是实现主、客体之间访问控制的基础；系统审计员的主要功能是设置审计机制，查看和处理审计信息。嵌入在信息系统中的虹膜识别机制，其系统管理员、系统安全员和系统审计员可以由信息系统的相应人员承担。

A.3.2 客体

虹膜识别机制中的客体是指主体所能操作的对象，包括作为数据存储的对象和为用户服务的进程。前者主要包括：虹膜图像、面部照片、模板特征序列、样本特征序列、特征序列数据库、有效载荷、用户确认结果、用户辨识结果；后者主要包括：系统管理员操作进程、数据库操作进程、安全员操作进程、审计员操作进程。

# 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

表 B.1　虹膜识别系统功能和性能要素与分等级要求的对应关系

| 功能与性能要素 | 第一级要求 | 第二级要求 | 第三级要求 |
|---|---|---|---|
| 4 基本功能要素 | * | * | * |
| 4.1 自包含功能 | * | * | * |
| 4.2 虹膜图像采集与处理功能 | * | * | * |
| 4.3 用户标识 | * | * | * |
| 4.4 用户登记 | * | * | * |
| 4.4.1　基本要求 | * | * | * |
| 4.4.2　两幅图像要求 | * | * | * |
| 4.4.3　四幅图像要求 | | | * |
| 4.5 用户识别 | * | * | * |
| 4.5.1　基本要求 | * | * | * |
| 4.5.2　两幅图像要求 | * | * | * |
| 4.5.3　四幅图像要求 | | | * |
| 4.6 识别失败的判定及处理 | * | * | * |
| a)设备故障 | * | * | * |
| b)像质障碍 | * | * | * |
| c)超时断开 | * | * | * |
| d)数据库故障 | | * | * |
| e)尝试超次 | | | * |
| 4.7 不可伪造识别 | * | * | * |
| a)防照片伪造 | | * | * |
| b)防隐形镜片伪造 | | * | * |
| c)防复制伪造 | * | * | * |
| d)防录像伪造 | | | * |
| e)防死亡虹膜伪造 | | | * |
| 4.8 警告与报警 | | * | * |
| 5 基本性能要素 | * | * | * |
| 5.1 错误接受率和错误拒绝率 | * | * | * |
| a)不大于万分之一和百分之一 | * | | |
| b)不大于十万分之一和百分之一 | | * | |
| c)不大于三十万分之一和千分之一 | | | * |
| 5.2 响应时间 | * | * | * |
| 5.3 适用范围 | * | * | * |
| 5.4 使用安全条件 | * | * | * |
| 注：表中“*”表示该级对相应的功能或性能要素有要求。 | | | |

# 附录C
# （规范性附录）
# 主、客体的访问操作关系

## C.1 适用于第一级的主、客体之间的访问操作关系

表 C.1 表示适用于第一级的虹膜识别系统中主体与客体之间的访问操作关系。

**表 C.1 适用于第一级的访问操作关系（模板特征序列以数据库或文件形式存贮）**

| 主体 | 对应客体 | 允许操作 | 不允许操作 |
|---|---|---|---|
| 特征序列生成进程 | 虹膜图像<br>模板特征序列<br>样本特征序列 | 图像变换、图像分析、特征表述 | 复制、传输、修改、保存 |
| 用户登记进程 | 模板特征序列 | 将模板特征序列存入数据库或文件系统 | 复制、传输、修改、保存 |
| 用户识别进程 | 样本特征序列<br>特征序列文件 | 样本特征序列与数据库或文件系统中的模板特征序列比对 | 复制，传输，修改，保存 |
| 应用系统通信接口进程 | 用户确认结果<br>用户辨识结果（候选者） | 传送识别（确认或辨识）结果 | 修改 |

## 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

表 C.2 表示适用于第二级和第三级的虹膜识别系统中主体与客体之间的访问操作关系。

**表 C.2 适用于第二级和第三级的访问操作关系（模板特征序列以数据库形式存贮）**

| 主体 | 对应客体 | 允许操作 | 不允许操作 |
|---|---|---|---|
| 特征序列生成进程 | 虹膜图像<br>模板特征序列<br>样本特征序列 | 图像变换、图像分析、特征表述 | 复制、传输、修改、保存 |
| 用户登记进程 | 模板特征序列<br>有效载荷<br>特征序列数据库 | 将模板特征序列及有效载荷组合为不透明数据，将纪录头及不透明数据组合为数据库记录，数据库 INSERT 操作 | 复制、传输、修改、保存 |
| 用户识别进程 | 样本特征序列<br>特征序列数据库 | 数据库 SELECT 操作，样本特征序列与库记录中的模板特征序列比对 | 复制、传输、修改、保存 |
| 应用系统通信接口进程 | 用户确认结果<br>用户辨识结果（候选者） | 传送识别（确认或辨识）结果 | 修改 |
| 系统管理员 | 系统管理员操作进程<br>数据库操作进程 | 安装、图像库或数据库维护 DELETE 、 REFERENCES 、 UPDATE 操作，用户登记 | 非授权操作 |
| 系统审计员 | 系统审计员操作进程 | 安全审计 | 非授权操作 |
| 系统安全员 | 系统安全员操作进程 | 主、客体敏感标记 | 非授权操作 |

## 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

表 C.3 表示适用于第三级的主体与图像数据库之间的访问操作关系。

表 C.3 适用于第三级的主体与图像数据库之间的访问操作关系

| 主体 | 对应客体 | 允许操作 | 不允许操作 |
|---|---|---|---|
| 图像处理进程 | 虹膜图像<br>面部照片 | 图像分离，图像压缩 | 复制、传输、修改、保存 |
| 存贮 / 读取图像进程 | 虹膜图像<br>面部照片 | 图像库 INSERT、SELECT 操作 | 复制、传输、修改、保存 |

# 附录 D
# （规范性附录）
# 虹膜特征序列数据库数据结构

虹膜特征序列数据库数据结构如图 D.1 所示。

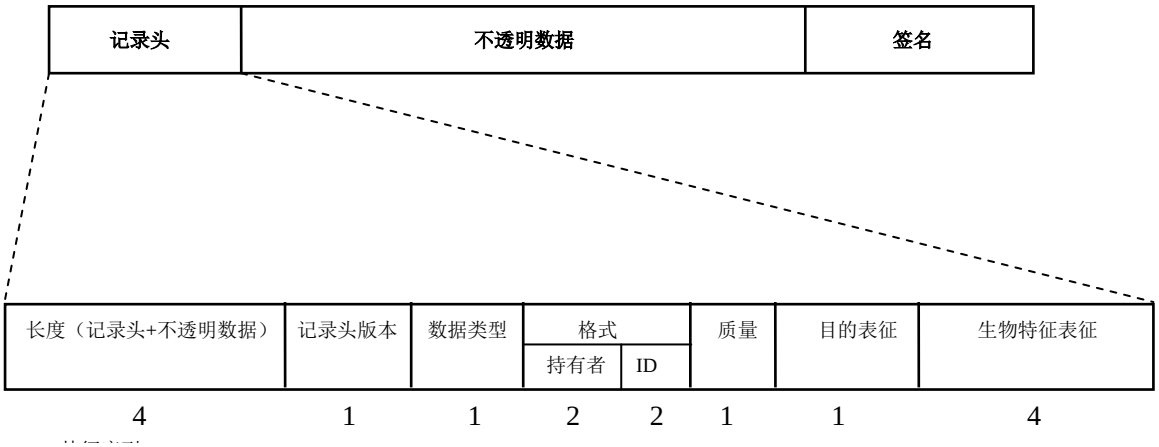



图 D.1 中，记录头数据

**图 D.1　虹膜特征序列数据库数据结构**

长度域：4 字节，用以给出记录长度，记录长度为记录头长度与不透明数据长度之和。

记录头版本域：1 字节，用以标记记录头版本。

数据类型域：1 字节，用以标明该记录是否加过标记或加过密，或既加过标记也加过密。

格式 • 持有者域：2 字节，用以标明持有或允许使用给定的不透明数据格式的机构，该域值应具有唯一性。

格式 • ID 域：2 字节，格式持有者赋予该格式的标识符。

质量域：1 字节，用以标示该记录在用来实现由目的表征码域规定之目的时的可用性程度。

目的表征域：1 字节，用以标明该记录用于实现用户登记、用户确认、用户辨识三种目的中的一种。

生物特征表征域：4 字节，其值为 0x00000010。

图 D.1 中，不透明数据应由以下各域顺序组成：

特征域：256 字节，用以存放虹膜图像经用户登记处理生成的模板特征序列。

特许域：64 字节，用以装入有效载荷。

防伪域：32 字节，用以检验或防止使用伪造数据或使用伪造图像的信息。

图 D.1 中，签名数据长度为 256 字节，可用以存放模板特征序列摘要的数字签名。

# 参　考　文　献

[1] GB/T 18336-1：2001　信息技术　安全技术　信息技术安全性评估准则　第1部分:简介和一般模型(idt ISO/IEC 15408-1:1999)

[2] GB/T 18336-2：2001　信息技术　安全技术　信息技术安全性评估准则　第2部分：安全功能要求(idt ISO/IEC 15408-2:1999)

[3] GB/T 18336-3：2001　信息技术　安全技术　信息技术安全性评估准则　第3部分：安全保证要求(idt ISO/IEC 15408-3:1999)

[4] ISO/IEC 15408-1：1999 Information technology—Security techniques—Evaluation Criteria for IT Security　Part1:Introduction and general model Part 1:Introduction and general model，Version 2.0

[5] ISO/IEC 15408-2：1999 Information technology—Security techniques—Evaluation Criteria for IT Security　Part2:Security functional requirements Part2:Security functional requirements，Version 2.0

[6] ISO/IEC 15408-3：1999 Information technology—Security techniques—Evaluation Criteria for IT Security　Part3:Security assurance requirements Part3:Security assurance requirements，Version 2.0