ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38671—2020

信息安全技术
远程人脸识别系统技术要求

Information security technology—
Technical requirements for remote face recognition system

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:公安部第一研究所、北京数字认证股份有限公司、浙江蚂蚁小微金融服务集团股份有限公司、北京旷视科技有限公司、重庆中科云从科技有限公司、中国信息安全测评中心、中国金融认证中心、中国电子技术标准化研究院、四川远鉴科技有限公司、深圳市亚略特生物识别科技有限公司、深圳市腾讯计算机系统有限公司、广州广电运通金融电子股份有限公司、中科天地科技有限公司。

本标准主要起草人:郑征、刘军、胡志昂、张翔、李敏、陈星、吕盟、李军、王宇航、李哲、王学华、刘琳、卢玉华、许玉娜、郝春亮、沈思成、王玉坚、汤海鹏、刘梦涛、张默男。

信息安全技术
远程人脸识别系统技术要求

1 范围

、
、 。

，

。

2 规范性引用文件

。 ，
。 ， （ ） 。

GB/T 18336.3—2015 3 ：
GB/T 20271—2006
GB/T 26238—2010
GB/T 29268.1—2012 1 ：
GB/T 36651—2018

3 术语、定义和缩略语

3.1 术语和定义

GB/T 20271—2006、GB/T 26238—2010、GB/T 29268.1—2012 GB/T 36651—2018
。

3.1.1

生物特征识别 biometrics；biometric recognition

， 。

注：“ ” 。

3.1.2

人脸识别 face recognition

。

， ，

。

注： ， 。

3.1.3

活体人脸 live face

。

3.1.4

face verification

,

(1∶1), 。

3.1.5

face identification

,

(1∶*N*), 。

3.1.6

characteristic sequence

。

: 。

3.1.7

template characteristic sequence

。

: 。

3.1.8

sample characteristic sequence

。

: 。

3.1.9

similarity

; 。

3.1.10

threshold

( )。

3.1.11

false accept rate

, , 。

: 。

3.1.12

false reject rate

, , 。

: 。

3.2

。

CG: (Computer Graphics)

EAL: (Evaluation Assurance Level)

FAR: (False Accept Rate)

FRR: (False Reject Rate)

SE: (Secure Element)

TEE: (Trusted Execution Environment)

TCM:可信密码模块(Trusted Cryptography Module)

UID:用户标识(User IDentification)

4 概述

4.1 系统参考模型

远程人脸识别系统由客户端、服务器端、安全传输通道组成。系统由客户端实现人脸的采集,经安全传输通道传输,在服务器端远程进行比对。

客户端由环境检测、人脸图像采集、活体检测、质量检测、安全管理等模块组成,模块通常在可信环境中执行。可信环境指用户设备上的安全区域,可保证加载到其内部数据的安全性,包括保密性、完整性和可用性等,如 TEE、SE、TCM 或其他具备安全边界的保护区域。本标准不规定可信环境的具体实现方式。

服务器端由活体判断、质量判断、人脸数据注册、人脸数据库、人脸识别、比对策略、安全管理等模块组成。

系统参考模型如图 1 所示。

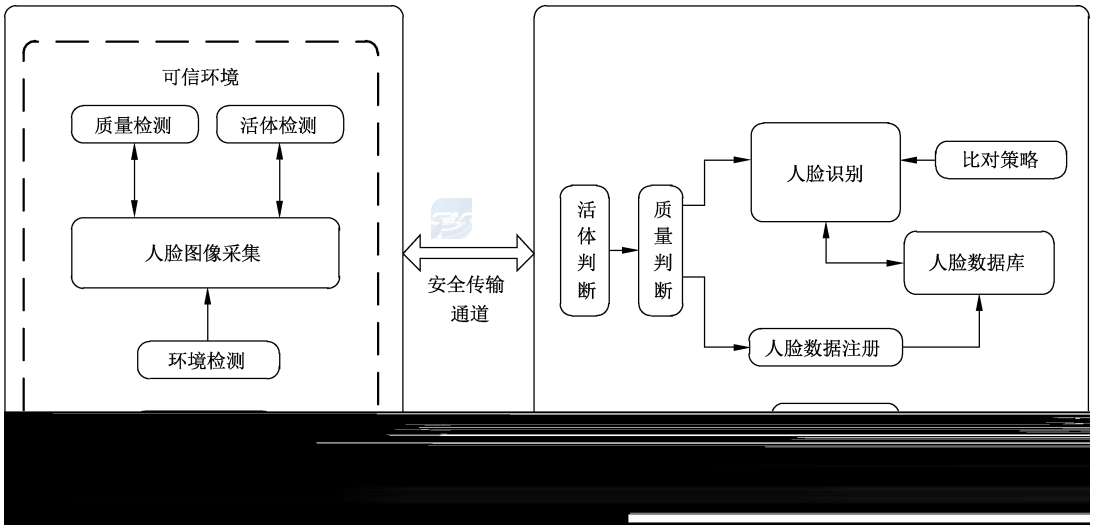


图 1 系统参考模型图

4.2 客户端说明

4.2.1 环境检测

对人脸采集的环境条件进行检测,判断人脸特征采集所处的环境是否满足采集要求,从而决定是否启动人脸采集。

4.2.2 人脸图像采集

对输入的图片或者视频等样本数据进行分析处理,提取满足质量条件的人脸图像,以便进行人脸特征提取和比对。

4.2.3 活体检测

对采集主体是否为活体人脸、是否受到假体人脸攻击进行检测和判断。条件允许时,可在客户端判

。 。

4.2.4 质量检测

。 ，

。 。

4.2.5 安全管理

、 、 。

4.3 服务器端说明

4.3.1 活体判断

， ，

。

4.3.2 质量判断

。

4.3.3 人脸数据库

， 、 、 、

。 ， 、

。 。 ，

UID、 。

4.3.4 人脸数据注册

、 。

， （ ）

。

4.3.5 人脸识别

4.3.5.1 人脸验证

， 。

4.3.5.2 人脸辨识

， ，

， 。

4.3.6 比对策略

、 ， 。

4.3.7 安全管理

、 、 。

4.4 安全传输通道

，。

5 安全分级

、，
，A，B。
，；、、、
。

6 功能要求

6.1 基本级要求

6.1.1 用户标识

：

a) ；
b) ；
c) 、，、。

6.1.2 人脸图像采集与处理

：

a) ；
b) 、；
c) ，；
d) ；
e) 。

6.1.3 人脸图像质量判断

，：

a) ；
b) ；
c) ；
d) 。

6.1.4 活体检测

6.1.4.1 主动配合式活体检测

，
，：

a) 、、、、；
b) 、。

6.1.4.2

，：

a）；

b），。

1：，，。

2：、，、，。

6.1.5

6.1.5.1

、。

，。

6.1.5.2

：

a）。

b）。

c），，，。

6.1.5.3

，：

a）、、；

b）；

c）；

d）。

6.1.6

6.1.6.1

，，。

6.1.6.2

，：

a），UID；

b），；

c），；

d），

；

e）；

f）。

6.1.6.3

，：

a) ，

；

b) ；

c) 。

6.1.6.4

。

6.1.6.5

，：

a) ：；

b) ：（：、

、）；

c) ：；

d) ，。

6.1.6.6

：

a) ，，；

b) ，；

c) ，，。

6.1.6.7

。

，

。。

。

6.1.6.8

6.1.6.8.1

（）

，

。

6.1.6.8.2

，，：

a) ：，；

b) ：；

c) ：；

d) ：；

e) ：，，

。

6.1.6.8.3

：

a) ；

b) ，；

c) ；

d) ，；

e) 。

6.1.6.9

：

a) ，，

，，，；

b) 、，、、，，

。

6.2

6.2.1

：

a) ；

b) ；

c) 、，、。

6.2.2

：

a) 、；

b) ，；

c) ，；

d) 、；

e) ，；

f) ，；

g) 。

6.2.3

，：

a) ；

b) ；

c) ；

d) ；

e) 。

6.2.4

6.2.4.1

，

，：

a) 、 、 、 、 ；

b) 、 。

6.2.4.2

，：

a) ；

b) ， 。

1：， ，

。

2： 、 ， 、

， 。

6.2.5

6.2.5.1

、 。

， 。

6.2.5.2

：

a) ；

b) ；

c) ， ， ， 。

6.2.5.3

，：

a) 、 、 ；

b) ；

c) ；

d) ；

e) ， 。

6.2.6

6.2.6.1

， 。

6.2.6.2

，：

a) ， UID；
b) ， ；
c) ， ；
d) ， ；
e) ，
；
f) ；
g) 。

6.2.6.3

， ：
a) ， ；
b) ，
；
c) ；
d) 。

6.2.6.4

。

6.2.6.5

， 、 、
。

6.2.6.6

， ：
a) ： ；
b) ： （ ： 、
、 ）；
c) ： ；
d) ： 、 、 ；
e) **CG** ： **CG**
3D ；
f) ： **3D** （ 、 ）
；
g) ， 。

6.2.6.7

：
a) ， ， ；
b) ， 。

6.2.6.8

。

当用来对用户身份鉴别的人脸特征模板等秘密信息由人脸识别系统产生时，系统应可生成符合秘密信息质量要求的秘密信息。秘密信息质量包括模板大小等。秘密信息质量量度的要求由安全管理员制定。

6.2.6.9 鉴别失败

6.2.6.9.1 基本要求

通过对不成功的鉴别尝试的值(包括尝试次数和时间的阈值)进行预先定义，并明确规定达到该值时应采取的措施来实现鉴别失败的处理。

6.2.6.9.2 失败判定

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

a) 设备故障：人脸采集器故障，不能成功捕捉图像；
b) 像质障碍：捕捉的人脸图像质量不适于生成人脸模板或生成人脸样本；
c) 超时断开：终端操作超时断开；
d) 数据库故障：人脸数据库故障且在规定尝试次数内未能消除；
e) 尝试超次：对人脸验证与人脸辨识，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。

6.2.6.9.3 失败处理

人脸识别失败的处理符合以下要求：

a) 制定识别失败返回值表；
b) 在出现识别失败情况时，返回对应的错误代码或错误值；
c) 针对识别失败记录事件日志；
d) 制定明确的识别失败处理策略，进行警告与报警；
e) 针对不同识别失败原因进行相应处理。

6.2.6.10 警告与报警

系统的警告与报警应满足以下要求：

a) 进行人脸验证时，如用户不是所给身份标识信息或其他用户身份信息的持有者，或用户已被删除，或在进行人脸辨识时，已存贮的人脸模板中无用户的候选者，应给出警告信息；
b) 检测出伪造识别图像、识别数据，或复制、非授权保存图像、数据，或非活体人脸，或非授权数据库操作时应给出报警信息。

7 性能要求

7.1 基本级要求

7.1.1 人脸注册

系统人脸注册失败率应不大于1%。

7.1.2 人脸验证

当错误接受率为0.1%时，错误拒绝率应不大于5%。

7.1.3 活体检测防范能力

7.1.3.1 攻击类型

系统应对以下攻击类型具备防御措施：

——活体检测基础级（静态攻击），能够对以下攻击手段进行防范：打印的普通人脸照片、纸质高清人脸照片、移动终端屏幕重放的人脸照片、纸质面具。

7.1.3.2 正常通过率

系统活体检测正常通过率应不小于95%。

7.1.3.3 攻击拒绝率

系统活体检测攻击拒绝率应不小于99%。

7.2 增强级要求

7.2.1 人脸注册

系统人脸注册失败率应不大于0.1%。

7.2.2 人脸验证

当错误接受率为0.01%时，错误拒绝率应不大于5%。

7.2.3 活体检测防范能力

7.2.3.1 攻击类型

系统应对以下攻击类型具备防御措施：

——活体检测基础级（静态攻击），能够对以下攻击手段进行防范：打印的普通人脸照片、纸质高清人脸照片、移动终端屏幕重放的人脸照片、纸质面具。

——活体检测增强级（合成动态攻击），能够对以下攻击手段进行防范：人脸视频（包含活体动作）、人脸CG合成、3D假体面具。

7.2.3.2 正常通过率

系统活体检测正常通过率应不小于99%。

7.2.3.3 攻击拒绝率

系统活体检测攻击拒绝率应不小于99%。

8 安全功能要求

8.1 基本级要求

8.1.1 安全审计

8.1.1.1 安全审计数据产生

安全审计功能应按以下要求产生审计数据：

a) ：

1) ；

2) ；

3) 、 、 ；

4) ；

5) ；

6) ；

7) 、 、 ；

8) ；

9) ；

10) 。

b) ： 、 、 、 ，

。

、 。

。

c) ， （ ， ）。

8.1.1.2 安全审计查阅

， ：

a) 。

b) 。

8.1.1.3 安全审计事件选择

：

、 、 、 。

8.1.1.4 安全审计事件存储

， ：

a) ： ， ；

b) ： ，

；

c) ： ， ，

、 ， 。

8.1.1.5 审计日志保护

。

。

。

， 。

8.1.2 用户数据保护

8.1.2.1 访问控制

， 、 ， 、 、

度的访问控制机制。

系统中有两类主体：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。

系统中的客体是指主体所能操作的对象，包括作为图像处理、数据存储的对象和为用户服务的进程。前者主要包括：已登记人脸模板、人脸采集样本、识别结果；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。

8.1.2.2 数据存储安全

本项功能应：

a) 具备对人脸等个人信息数据加密存储能力，满足数据保密性保护要求；

b) 利用存储访问控制模块实施人脸数据用户身份标识与鉴别策略、数据访问控制策略，并实现相关安全控制措施，防止非授权的访问用户人脸数据。

8.1.2.3 数据传输安全

应采用满足数据传输安全策略相应的安全控制措施，如数据加密等，对人脸识别数据的传输进行保护。

8.1.3 个人信息保护

应对用户人脸模板等公民个人隐私信息进行保护，包括但不限于以下功能：

a) 无关联保护，应防止通过应用程序或数据库关联到存储的人脸模板数据；

b) 机密性保护，应防止非授权用户对人脸模板数据的访问；

c) 残余信息保护，要求系统安全功能有能力确保，对于安全控制范围内的某个已定义的客体进行资源的配给或回收时，剩余信息是不可用的。

8.1.4 时间戳

系统的安全功能应能为自身的应用提供可靠的时间戳。

8.1.5 备份与恢复

系统应具有备份和恢复功能，在系统运行中出现致使信息丢失的故障时，能进行信息恢复；在系统运行中出现致使系统无法运行的故障时，能进行系统恢复。

8.1.6 安全管理

系统应提供系统管理员、安全管理员和审计管理员的角色定义。

系统管理员：安装、配置、维护系统；建立和管理用户账户；执行系统的备份和恢复。

安全管理员：维护用户属性定义；管理秘密信息质量量度；维护人脸算法参数设置、识别决策策略。

审计管理员：配置审计参数；查看和维护审计日志。

系统应具备使主体与角色相关联的能力，并保证一个身份不应同时具备多个角色的权限。一个人不应同时拥有多个角色，系统应在系统设计时对角色的管理进行相关限制。

本级系统角色的安全功能管理应按表1中的配置对授权的角色修改安全功能的能力进行限制。

1

	/
	；
	、 ， （ 、 、 ） 、 （ ）。 、 ， 、

8.2

8.2.1

8.2.1.1

：

a) ：

1) ；

2) ；

3) 、 、 ；

4) ；

5) ；

6) ；

7) 、 、 ；

8) ；

9) ；

10) 。

b) ， ： 、 、 、 ，

。

、 。

。

c) ， （ ， ）。

8.2.1.2

， ：

a) 。

b) 。

8.2.1.3

：

、 、 、 。

8.2.1.4

， ：

a） ： ， ；

b） ： ，

；

c） ： ， ，

、 ， 。

8.2.1.5

。

。

。

， 。

8.2.2

8.2.2.1

， 、 ， 、 、

。 / 、 、 。

： ， 、 ；

。

， 、

。 ： 、 ； ：

、 、 、 。

8.2.2.2

：

a） ， ；

b） 、 ，

， ；

c） 。

8.2.2.3

：

a） ， 、 、 ；

b） ；

c） ；

d） ， 。

8.2.3

，：

a) ，。

b) ，。

c) ，，

，。

d) ，：

—— ，、、。

—— ，。

—— ，。

—— ，。

8.2.4

。

8.2.5

，，

。。

。、

。。

8.2.6

、。

：、、；；。

：；；、。

：；。

，。

，。

2 。

2

	/
	；
	、，（、、）、（）。 、，、

9 安全保障要求

9.1 基本级要求

应具备 GB/T 18336.3—2015 中 EAL 3 级能力。

9.2 增强级要求

应具备 GB/T 18336.3—2015 中 EAL 4 级能力。

附 录 A
（资料性附录）
远程人脸识别系统基本级和增强级对应关系

A.1 系统功能要求

系统功能要求见表 A.1。

表 A.1 系统功能要求

功能要求		基本级要求	增强级要求
用户标识		*	*
人脸图像采集与处理		*	* *
人脸图像质量判断		*	*
活体检测		*	* *
人脸数据注册管理		*	*
用户鉴别	鉴别时机	*	*
	人脸验证	*	* *
	人脸辨识	*	* *
	一次性鉴别机制	*	*
	多机制鉴别		*
	防伪造	*	* *
	决策反馈保护	*	*
	秘密的规范	*	*
	鉴别失败	*	* *
	警告与报警	*	*
“*”表示具有该要求；“* *”表示功能要素要求的提高。			

A.2 系统性能要求

系统性能要求见表 A.2。

表 A.2 系统性能要求

功能要求	基本级要求	增强级要求
人脸注册	*	*
人脸验证	*	* *
活体检测防范能力	*	* *
“*”表示具有该要求；“* *”表示性能要素要求的提高。		

A.3 系统安全功能要求

系统安全功能要求见表 A.3。

表 A.3 系统安全功能要求

安全功能要求		基本级要求	增强级要求
安全审计	审计日志产生	*	*
	审计日志查阅	*	*
	审计事件选择	*	*
	审计事件存储	*	*
	审计日志保护	*	*
用户数据保护	访问控制	*	* *
	数据存储安全	*	* *
	数据传输安全	*	* *
个人信息保护		*	* *
时间戳		*	*
备份恢复		*	* *
系统管理		*	*
“*”表示具有该要求;“* *”表示性能要素要求的提高。			

A.4 系统安全保障要求

系统安全保障要求见表 A.4。

表 A.4 系统安全保障要求

安全保障要求	基本级要求	增强级要求
GB/T 18336.3—2015 中 EAL 3	*	—
GB/T 18336.3—2015 中 EAL 4	—	*
“*”表示具有该要求。		

附 录 B
（资料性附录）
远程人脸识别系统安全描述

B.1 受保护资产

B.1.1 描述目的

、 ，

。

B.1.2 用户数据类

B.1.2.1 概述

， 。

B.1.2.2 系统配置数据

、 、 。

B.1.2.3 人脸图像数据

。

B.1.2.4 人脸处理数据

， 、 、 。

B.1.2.5 输入数据

， 。 。

B.1.2.6 传输数据

：

a) ；
b) ；
c) ；
d) 。

B.1.3 安全功能数据类

B.1.3.1 概述

，

。

B.1.3.2 安全功能受保护数据

， 。

注：，

，。

示例：、、、

。

B.1.3.3 安全功能保密数据

，。

注：，

。

示例：、、、、。

B.2 安全威胁分析

B.2.1 概述

，，

，，，

，。，，

。

B.2.2 人脸识别系统安全威胁分析

、、：

、、、（），（

、）。：

a）

，。

，、。

，

，，，，、、

。，，

。

b）

，。

。

c）

，、、，

。、。

（、）。

d）

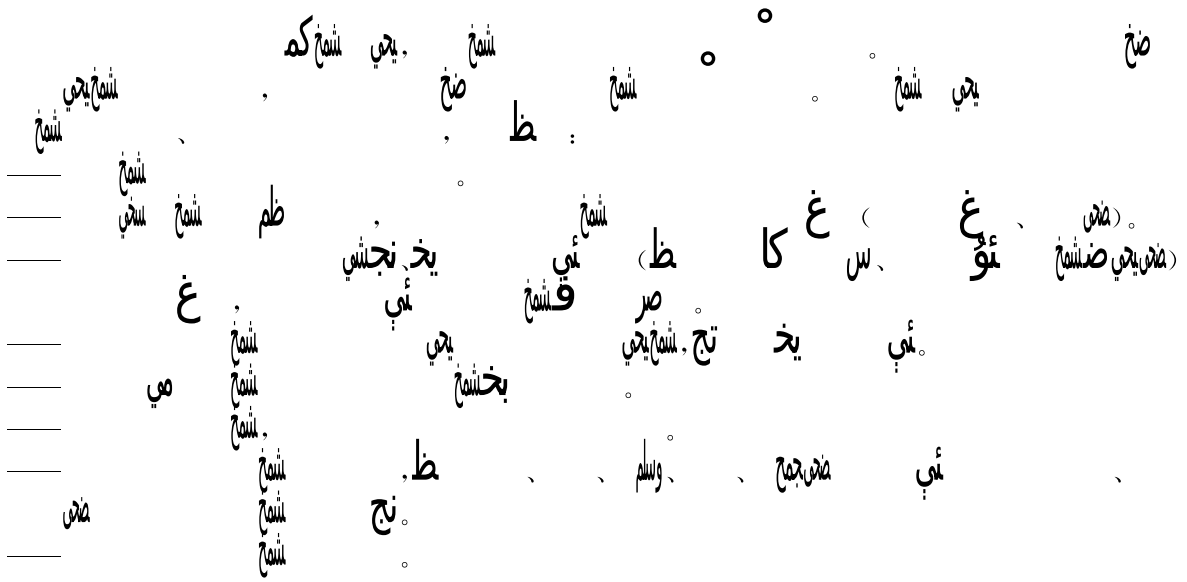
，、/、，。

B.2.3 人脸识别技术安全性分析

，。

，，，

B.3　安全假设

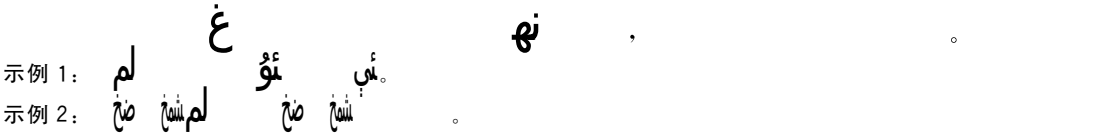


B.4　安全目的

B.4.1　概述

B.4.2　针对评估对象的安全目的

B.4.2.1　防止系统配置数据和人脸处理数据未授权的泄露和更改



B.4.2.2　防止输入数据和传输数据的伪造、抵赖和未授权更改

B.4.2.3　防止受保护数据和保密数据伪造和未授权的更改

B.4.2.4　防止安全功能保密数据泄露

。

B.4.2.5　产生安全日志

，　　、

。

B.4.2.6　防止旁路攻击

，　　。

B.4.2.7　密码模块和密码算法安全

，　　、

。

B.4.2.8　防伪造攻击

。

B.4.2.9　防重放攻击

，　　。

B.4.2.10　防遗留信息攻击

。

B.4.2.11　人脸特征参考模板安全保护

、　　、　　。

B.4.3　针对评估对象运行环境的安全目的

。

。

参 考 文 献

[1] GB 17859—1999 计算机信息系统 安全保护等级划分准则
[2] GB/T 18336(所有部分) 信息技术 安全技术 信息技术安全评估准则
[3] GB/T 20273—2019 信息安全技术 数据库管理系统安全技术要求
[4] GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范
[5] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求
[6] GB/T 27912—2011 金融服务 生物特征识别 安全框架
[7] GB/T 31504—2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范
[8] GB/T 33767.5—2018 信息技术 生物特征样本质量 第5部分:人脸图像数据
[9] GB/T 35273—2017 信息安全技术 个人信息安全规范
[10] GA/T 1212—2014 安防人脸识别应用 防假体攻击测试方法
[11] ISO/IEC 30107-1:2016 Information technology—Biometric presentation attack detection—Part 1: Framework