

Biometrics



1 简介

2 其余机制

3 理论和实践

4 口令泄漏

- 身份认证
- 认证因子
- 文本口令
- 优缺点

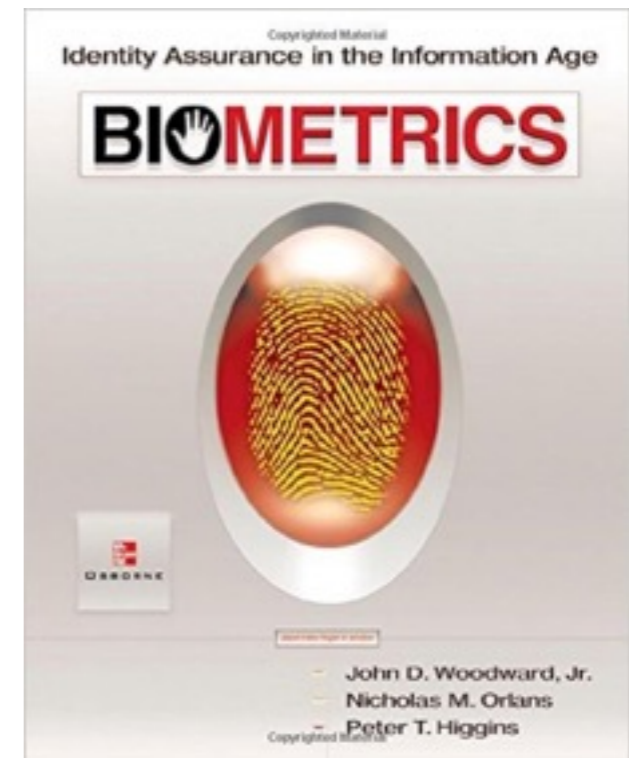
- PKI
- Biometrics
- OTP、管理
- OpenID、OAuth

- 口令建议
- 口令强度
- 智能分类
- 主动认证等

- HoneyWord
- SAuth
- ErsatzPass
- PolyPassHash

本次课程内容

- 生物学认证简介
- 生物学认证系统
- 生物学认证类型
- 生物学认证挑战



生物学认证简介

身体作为口令

定义

- 根据生理和行为特征来识别或验证一个有生命个体的自动方法

● 指纹

● 虹膜

● 静脉

● 手型

● 视网膜

● 脸部热成像

● 脸型

● 耳朵

● DNA

生理

VS

行为

识别 vs 验证

有生命

自动

● 语音

● 击键

● 足部运动

● 签名

● 滑动

● 操作行为

● 步态

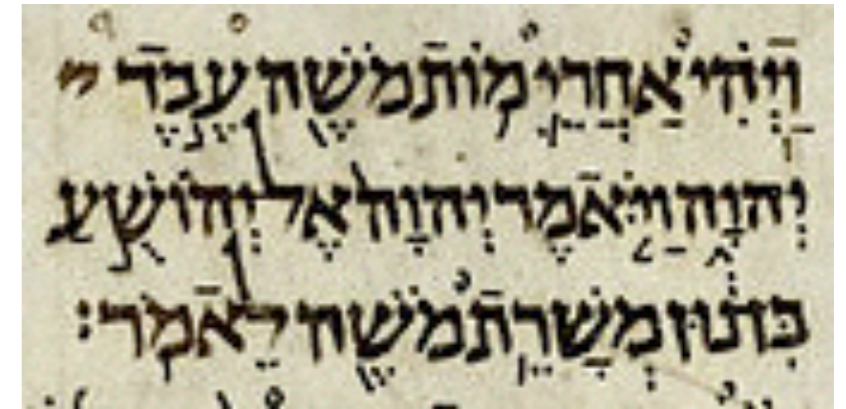
● 握手

● 脑电波

Gilead then cut Ephraim off from the fords of the Jordan, and whenever Ephraimite fugitives said, 'Let me cross,' the men of Gilead would ask, 'Are you an Ephraimite?' If he said, 'No,' they then said, 'Very well, say "Shibboleth" (שבלת).' If anyone said, "Sibboleth" (סבלת), because he could not pronounce it, then they would seize him and kill him by the fords of the Jordan. Forty-two thousand Ephraimites fell on this occasion.

—Judges 12:5-6, NJB

《士师记》 (The Book of Judges)



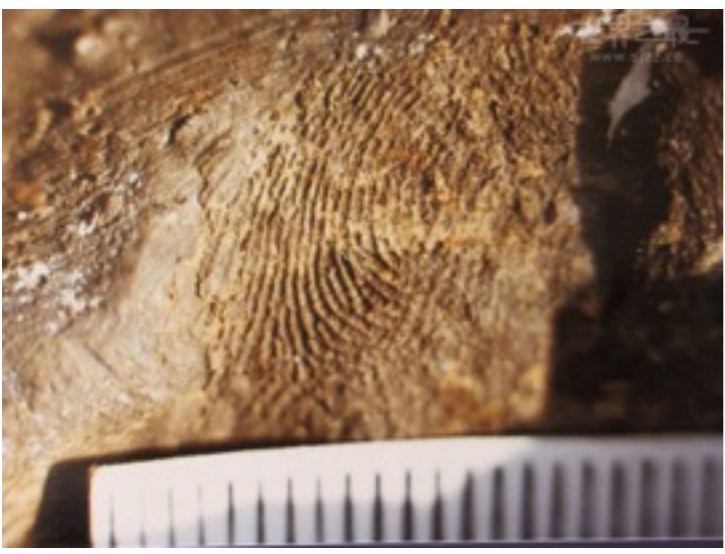
45000厄弗雷姆人



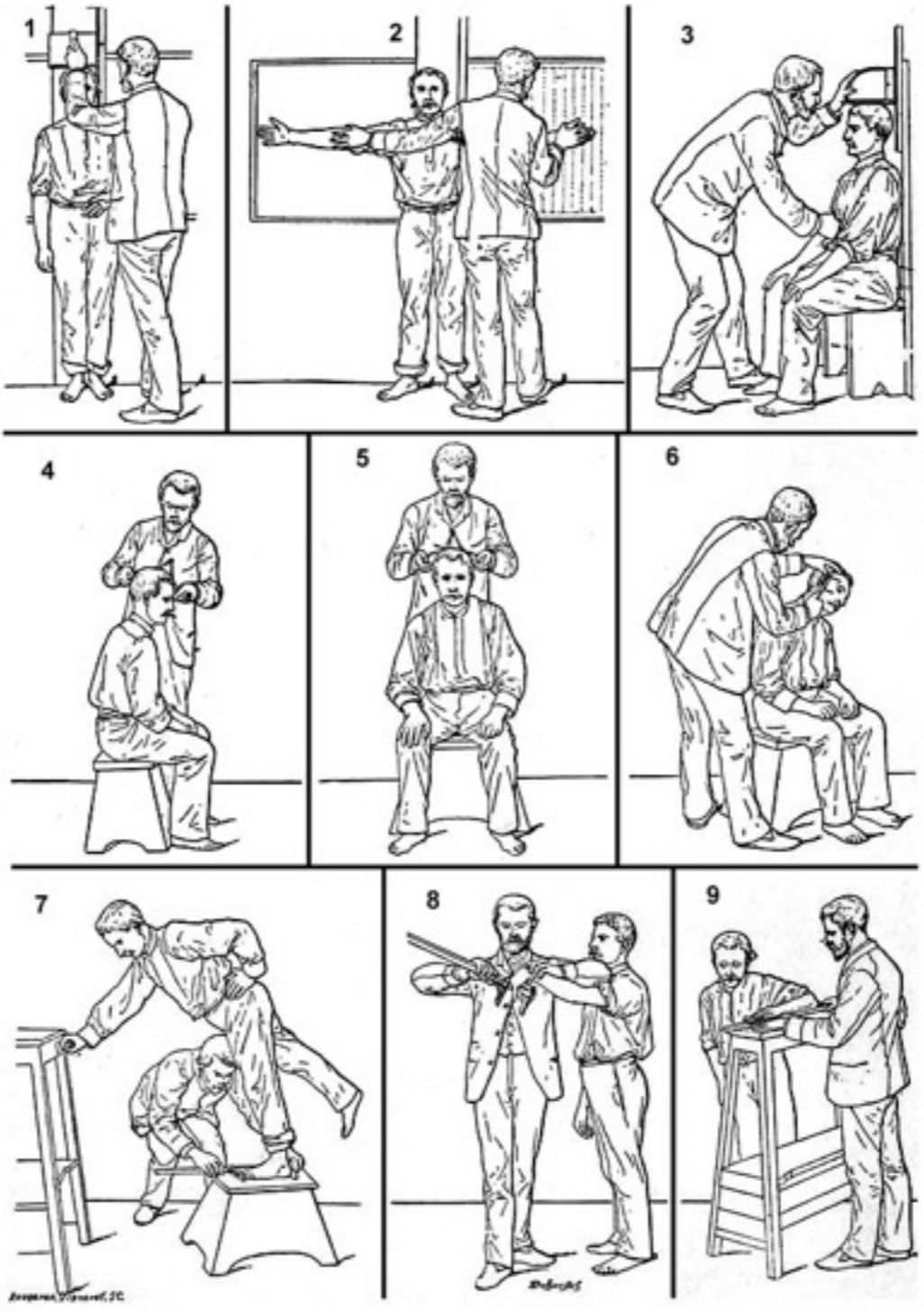
<http://shibboleth.internet2.edu/>

Biometrics Introduction

历史

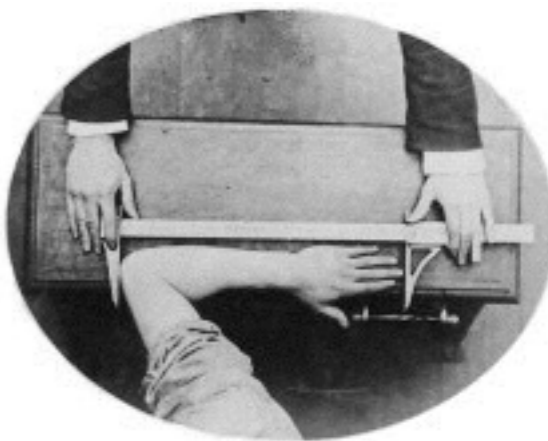


7000年前 半坡遗址



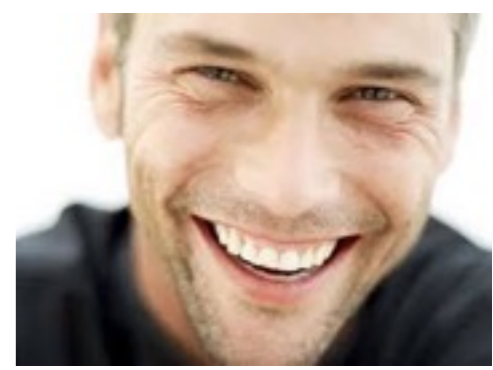
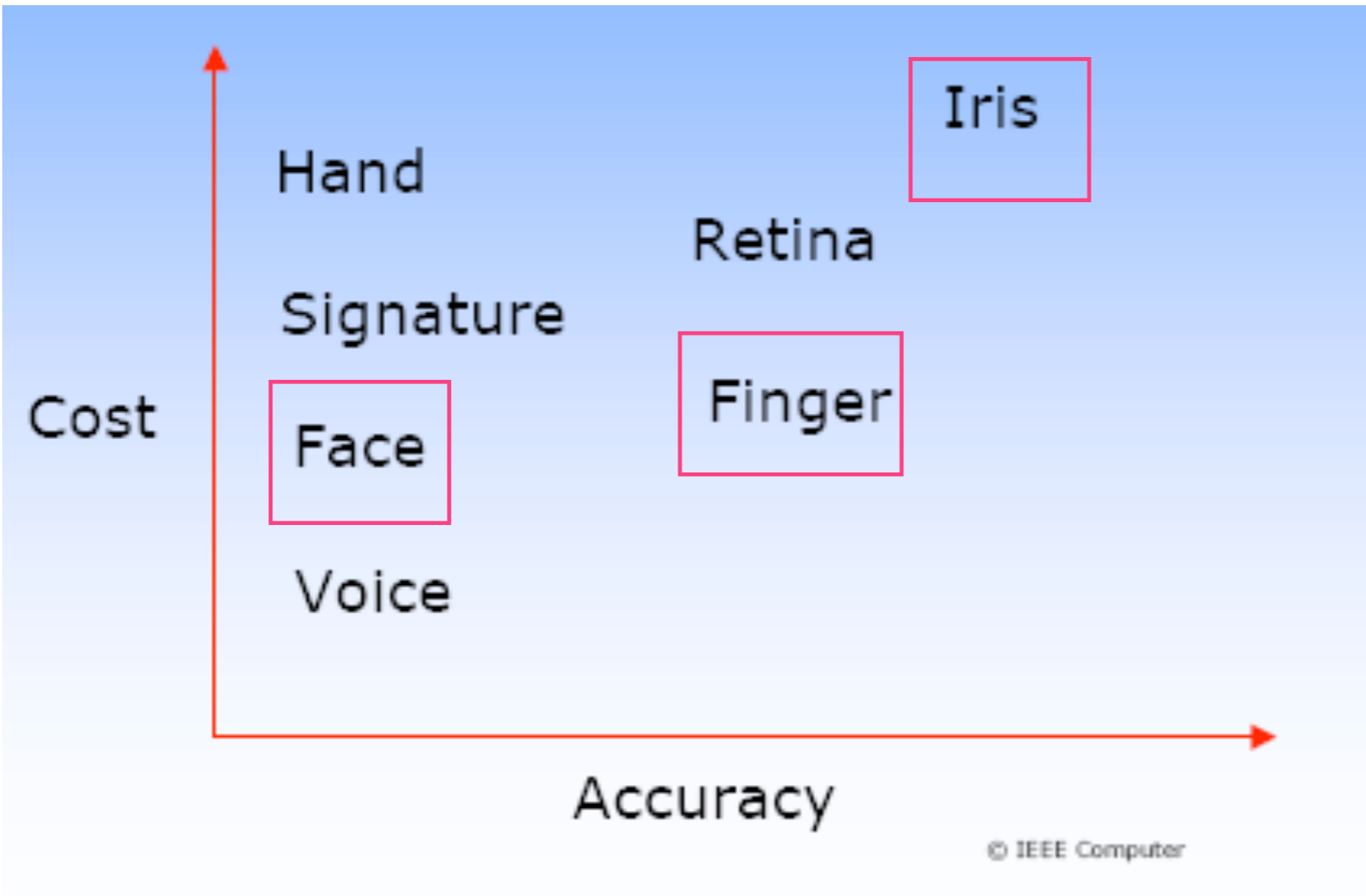
- 1. Height.
- 2. Reach.
- 3. Trunk
- 4. Length of head.
- 5. Width of head.
- 6. Right ear.
- 7. left foot.
- 8. Left middle finger.
- 9. Left forearm.

1882 Bertillion系统



1880 Nature Henry Faulds





1963: 指纹 1963: 语音 1966: 脸型 1971: 手型 1987: 虹膜

2003: US-Visit

物理访问控制



出入境



金融支付



背景调查



- 身份证件
- 军事应用
- 社会公益
- 考勤
- 赌场
- 计算机和网络
- 智能手机
- 个性化

优缺点

优点

- 安全
- 方便
- 难于欺骗，不容易改变、丢失、复制
- 唯一性标识
- 被动标识

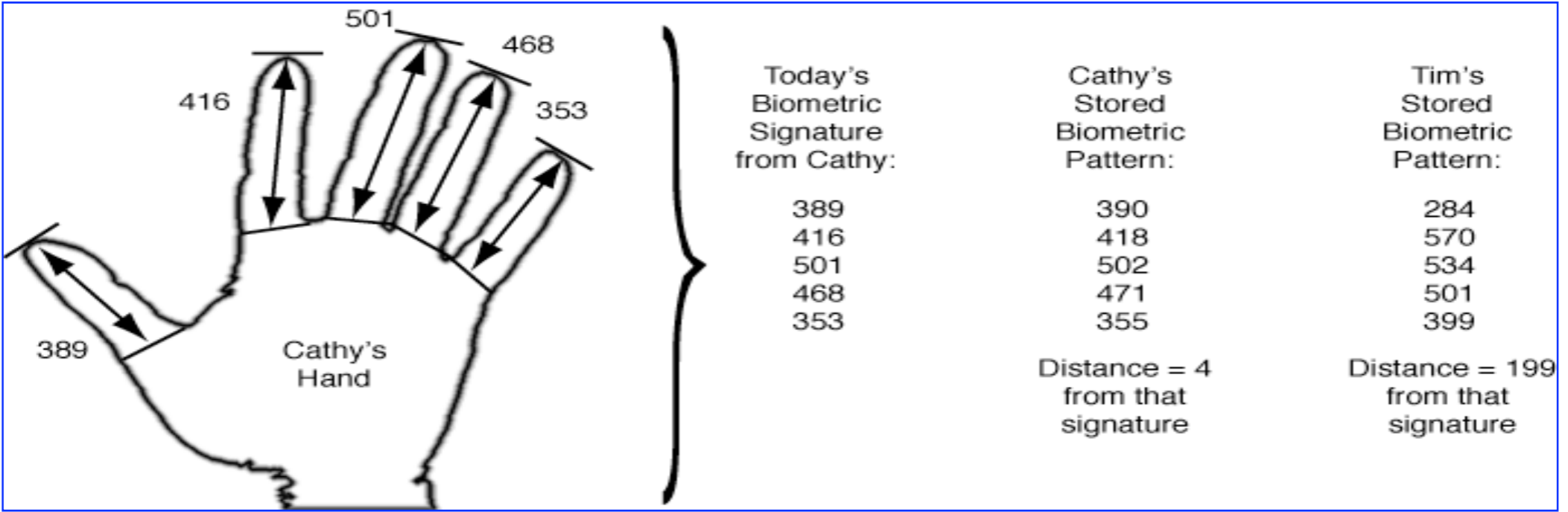
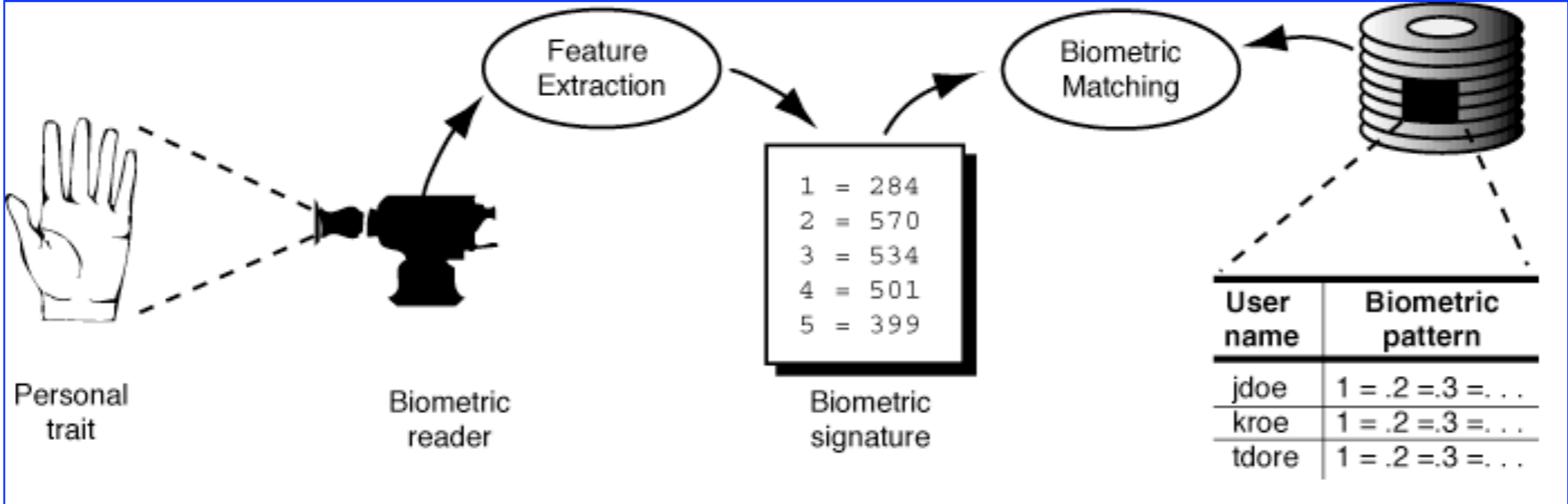
缺点

- 准确性
- 难于作废
- 存在适配问题
- 可能侵犯隐私
- 系统存在被攻击的危险

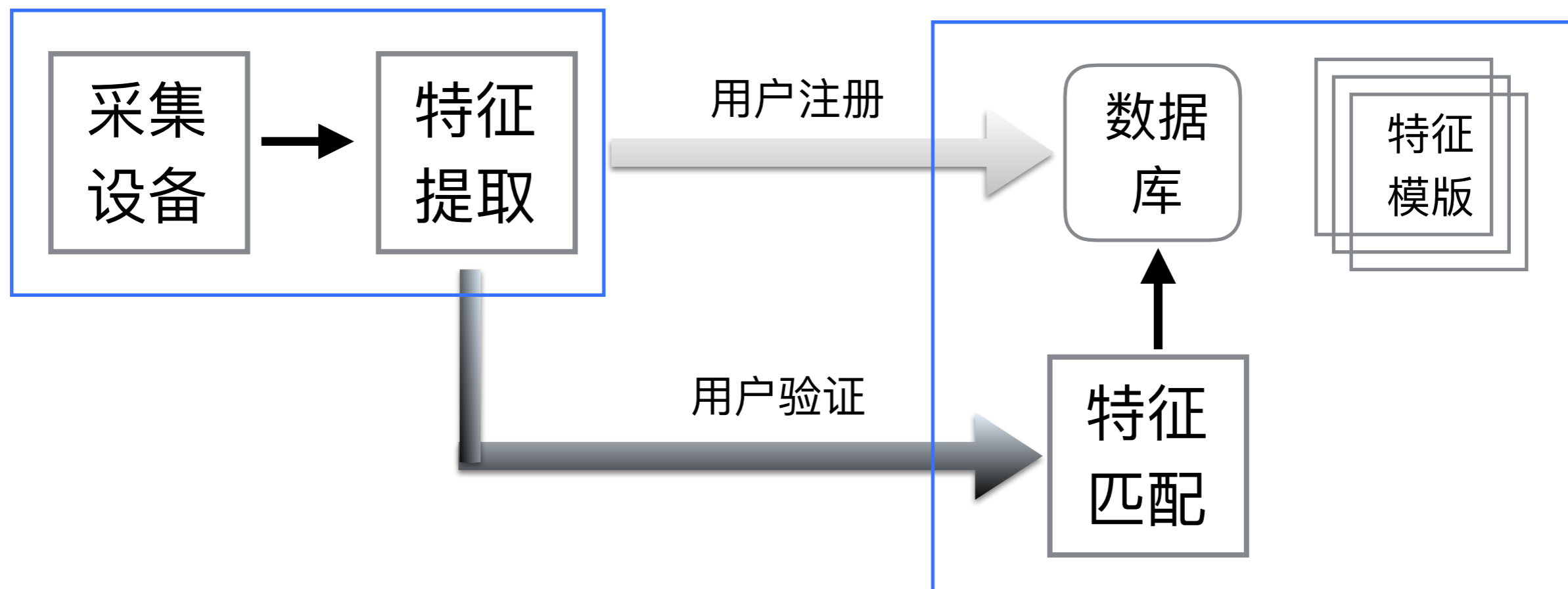




生物学认证系统



构成



- 健壮性 (持久性)
 - * 能够在相当长时间内反复表现出来，并让生物认证系统成功进行自动测量的性质
- 独特性 (唯一性)
 - * 人与人之间存在足够大的差异，并且这种差异能够被测量出来
 - * 所有的生物特征都包括三种因素
 - ➔ 遗传因素：天生
 - ➔ 表现因素：胚胎发育的早起形成
 - ➔ 行为因素：后天学习的行为，可以改变和重新学习

- 模板生成

- ✧ 单个和多个生物特征样本

- ✧ 生物特征类型、用户和环境因素、性能要求

- ✧ 指纹

- ➔ 手指放在扫描仪上的角度和位置

- ➔ 手指上伤痕、残留物、障碍物

- ➔ 扫描仪的灰尘和残留物

- 注册分数：反应注册质量

- 强制 vs 自愿

- 动态阈值 vs 静态阈值

多重注册

注册失败率
允许的次數

需要的附加信息

注册数据的存储位置

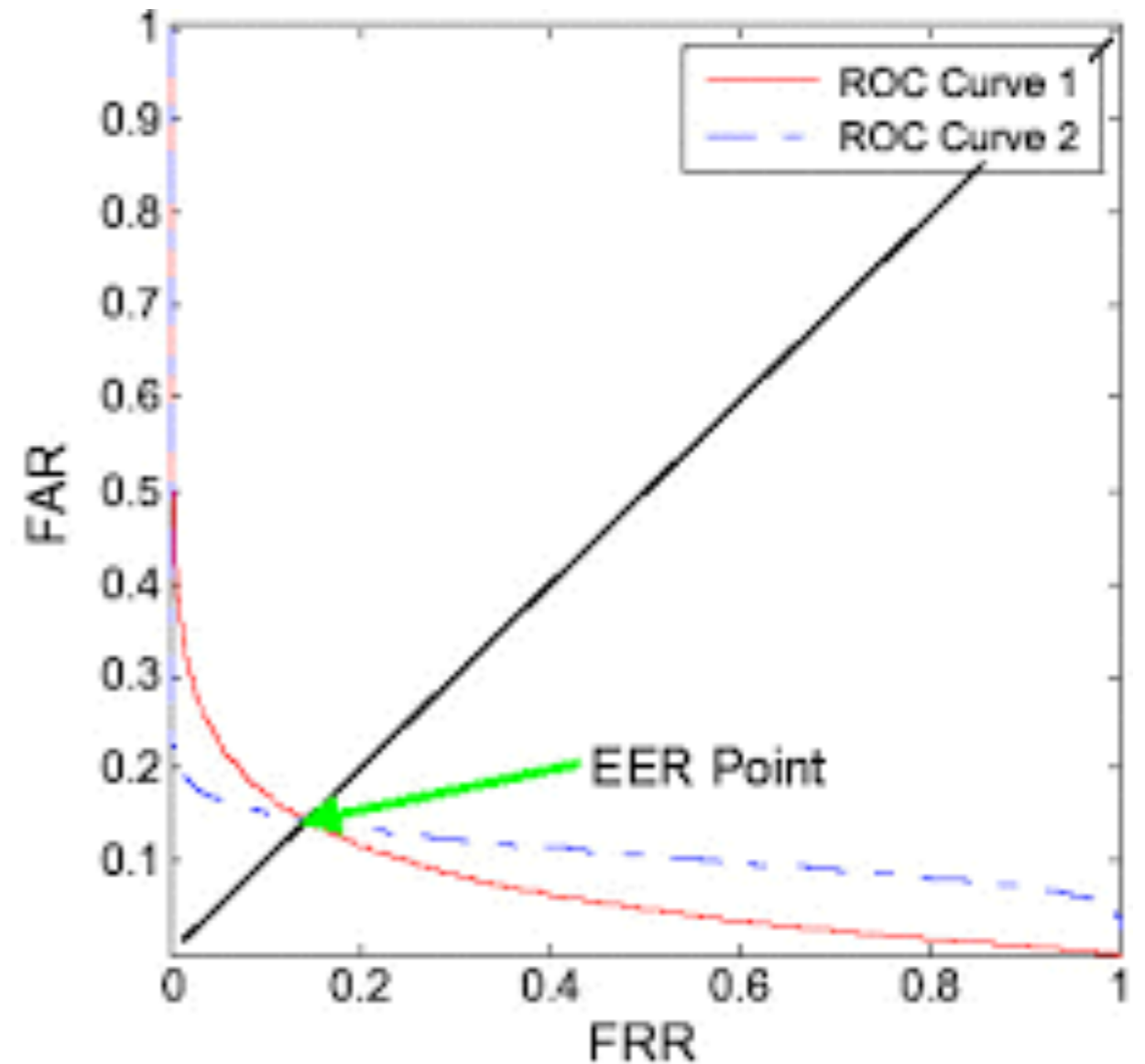
是否需要多方法的注册

- 模板：通过原始数据提取出来的生物特征的总和
- 模板的老化和漂移
- 模板更新
- 模板存储
 - * 空间
 - * 方式：本地、网络、便携设备
- 模板安全

所有生物认证系统的有效性是以模版数据库的质量和完备性为基础的，因为每一次匹配均需要将获得的数据和存储的参考模版相比较

- 验证：一对一匹配、肯定性匹配
- 识别：一对多匹配、否定性匹配
- 合作 vs 非合作
- 活体检测
 - * 热传感器测量体热
 - * 测量身体运动或者其它特征
 - * 费用和性能
 - * 不要以为生物学认证设备会做活体检测

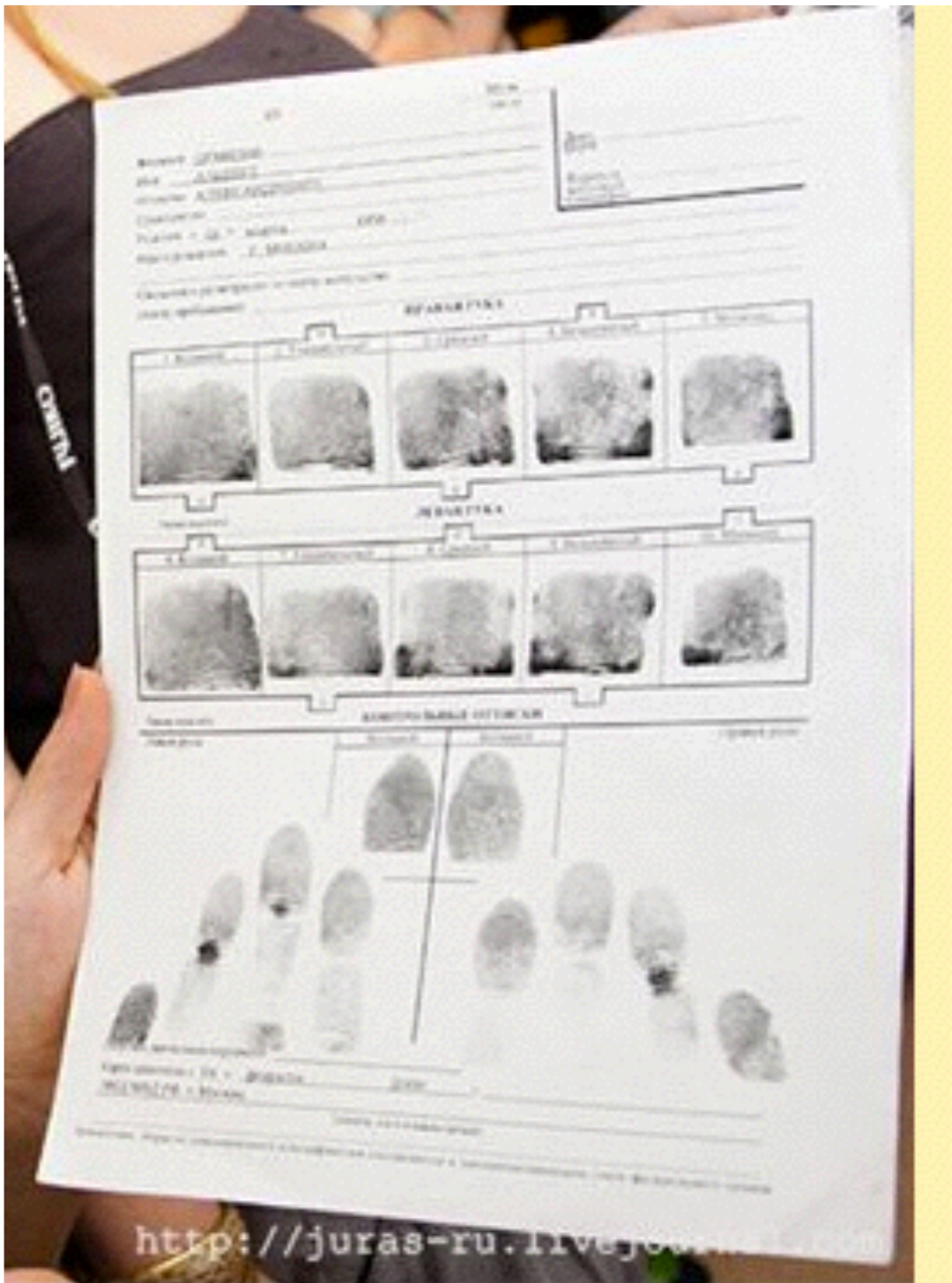
- FAR: False Acceptance Rate
- FRR: False Rejection Rate
- ERR: Equal Error Rate
- ROC: Receiver Operating Characteristic
- AUC: Area Under the Curve of ROC



生物学认证类型

Types of Biometrics

指纹



指纹

分离纹



箕形纹



螺形纹



棒形纹



交叉纹



分离纹



弧形纹



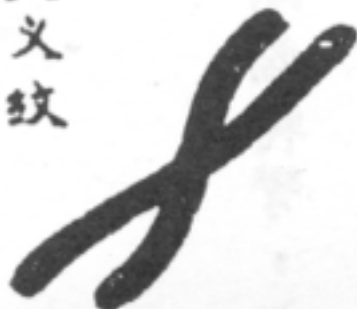
环形纹



三角纹



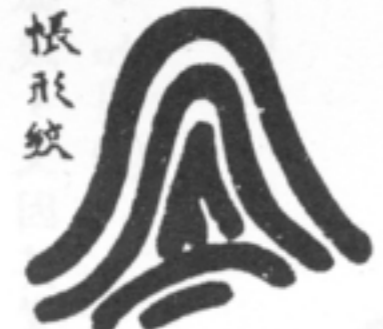
交叉纹



分离纹



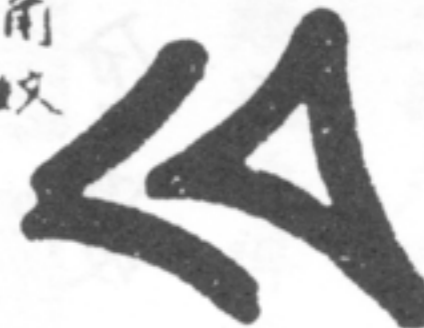
帐形纹



接合纹



三角纹



指纹

环
弧
螺旋



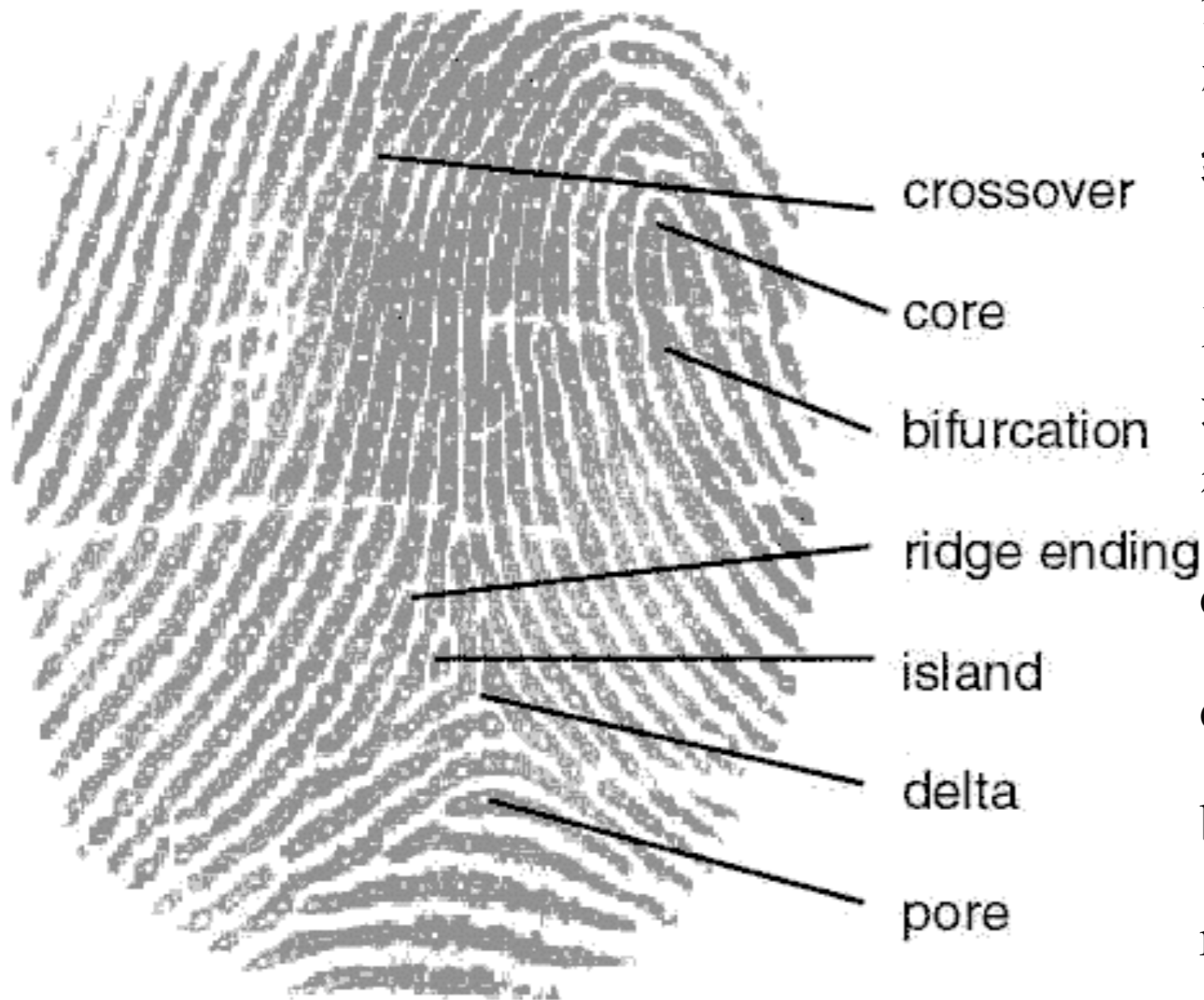
末梢
分叉
园点
组合

总体形状

突起细节和路径

单个突起细节

指纹



亨利系统将一个指纹的图形划分为：左环，右环，拱，涡和棚状拱。环型占了将近2/3的指纹图象，涡占1/3，可能存在5-10%的拱，这种指纹图形分类方法在大规模刑侦上有着广泛运用，但在生物识别认证方面很少有运用。

crossover 交叉

core 核

bifurcation 分岔

ridge ending 脊断点

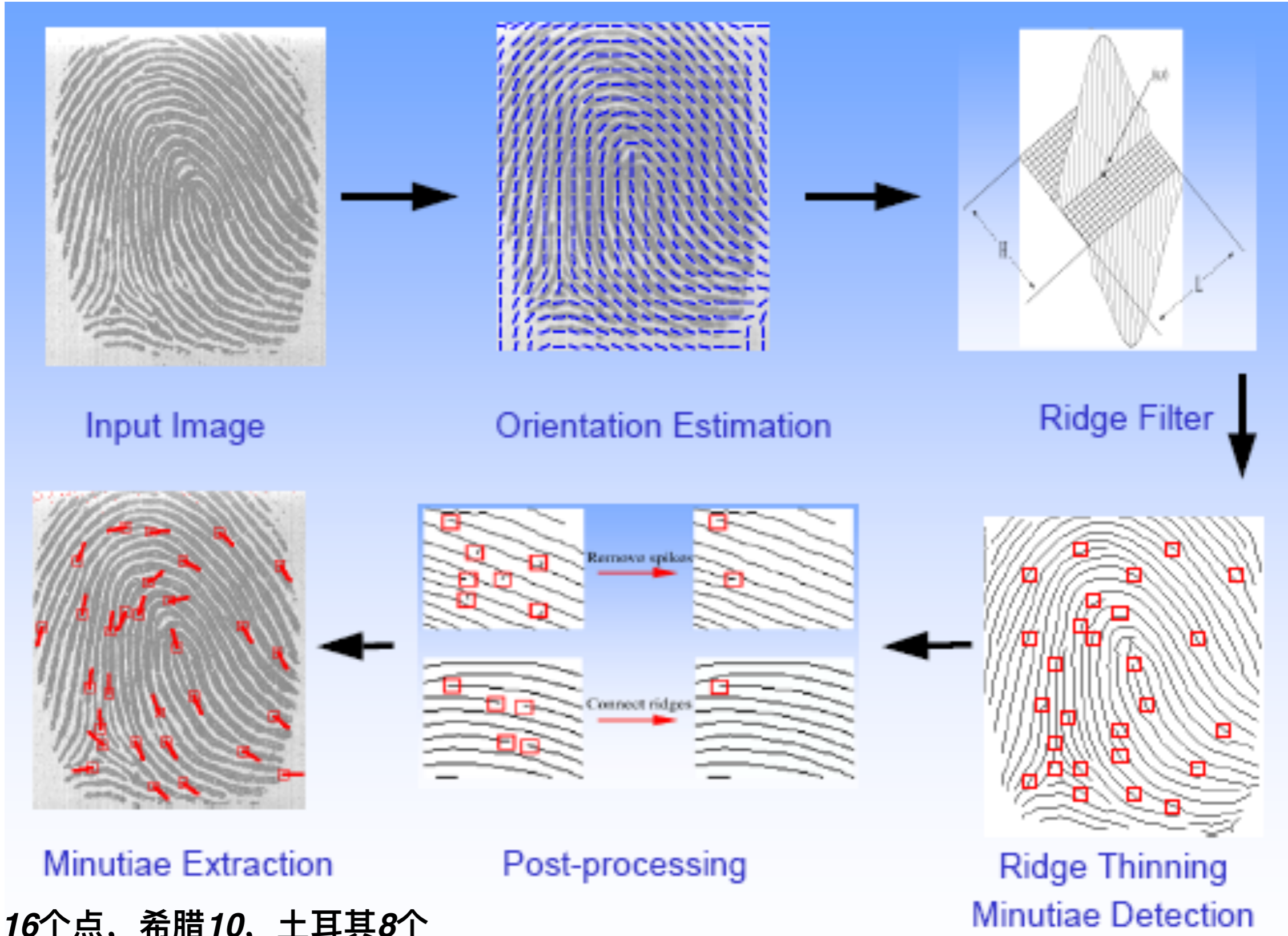
island 岛型区域

delta 三角形区域 pore 孔

Figure 1

<http://www.biocn.com/serv-finger.htm>

指纹



英国 16 个点, 希腊 10, 土耳其 8 个

Types of Biometrics

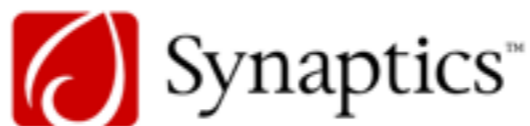
手机上指纹的历史

西门子

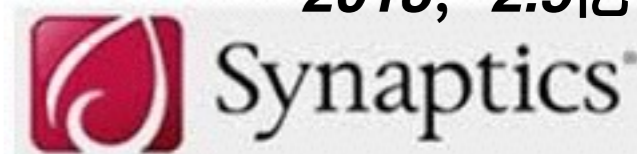
1998

背部

刮擦式



2013, 2.5亿



FINGERPRINTS



2012, 3.7亿

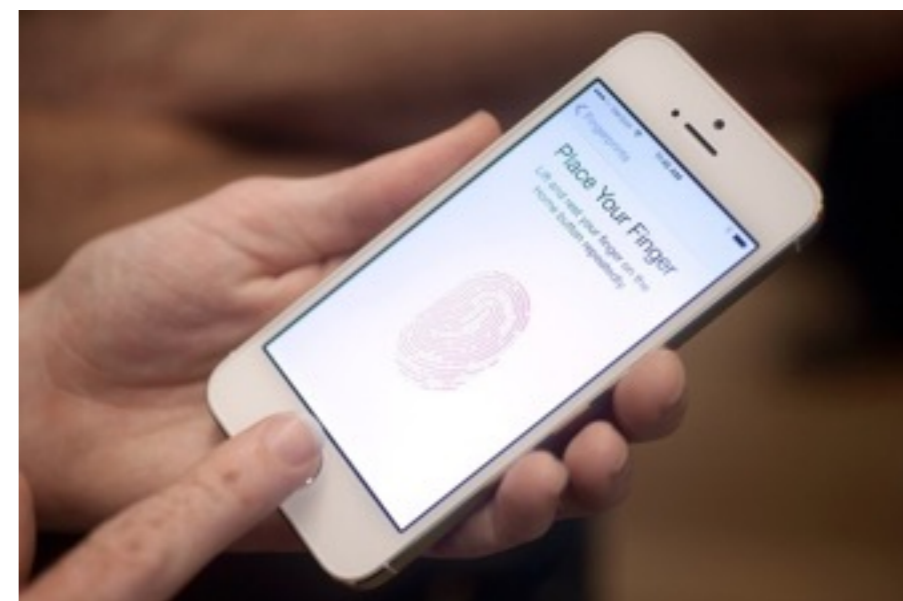
SAGEM
MC 959

2000



光学 vs 电容

前置 vs 后置



富士通

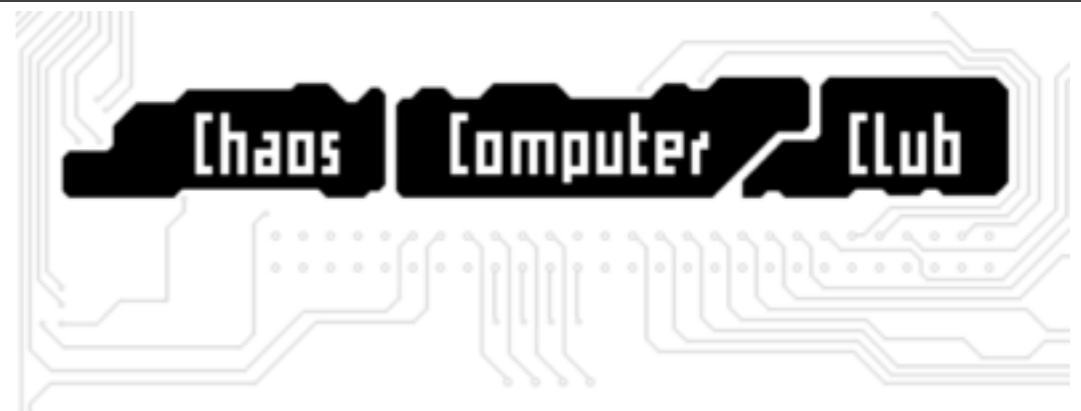
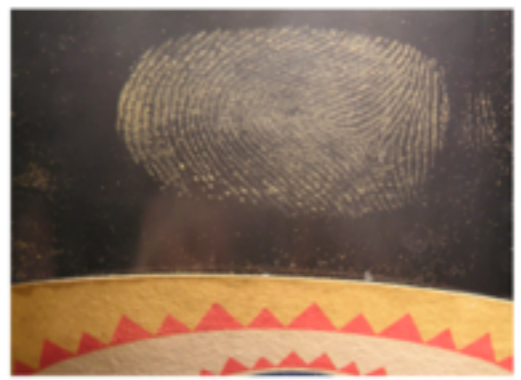
2003



Moto
MB 860

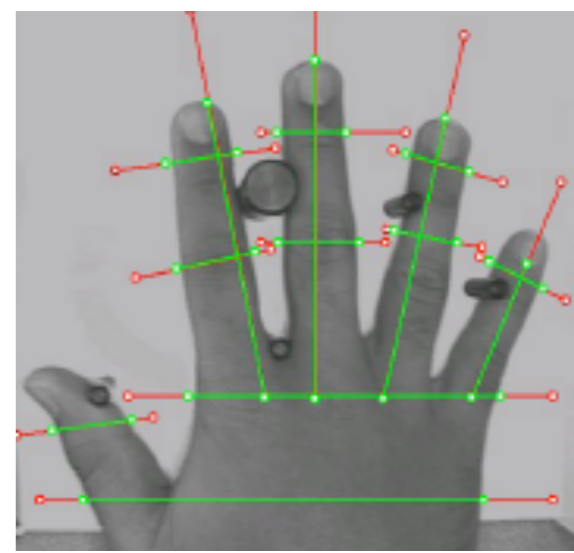
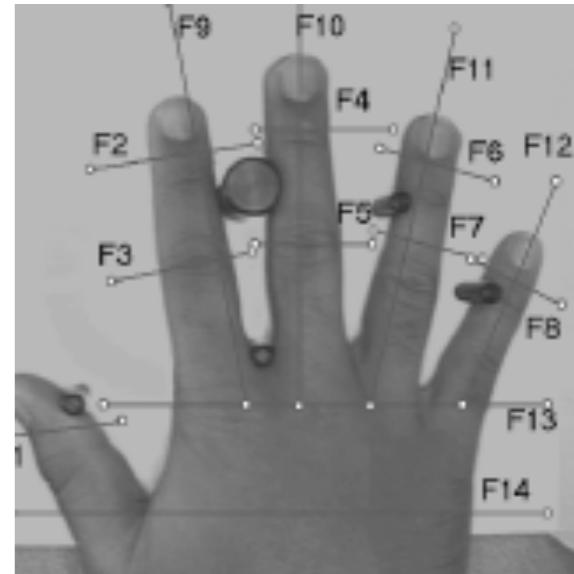
Types of Biometrics

攻击指纹



手型

手指：
长度
宽度
厚度
表面区域



访问控制
资源使用
打卡

尺寸
结合掌纹
AirAuth

美国INS
佐治亚大学
奥兰多迪斯尼乐园



脸型

识别和验证身份
监视和监控
视频搜索和索引应用



光线
遮盖

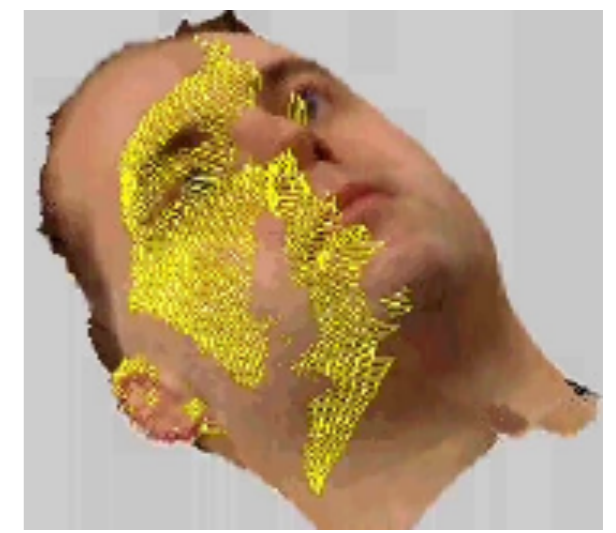
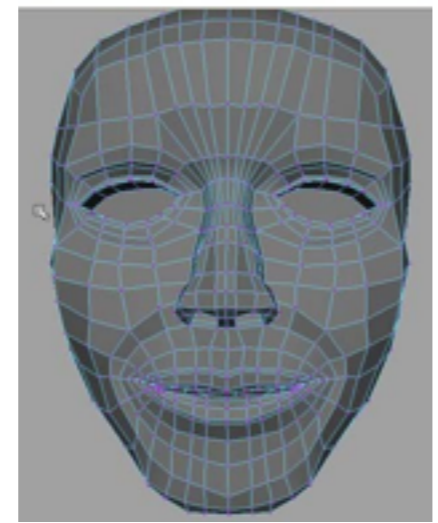


神经网络、特性脸型、局部特征分析

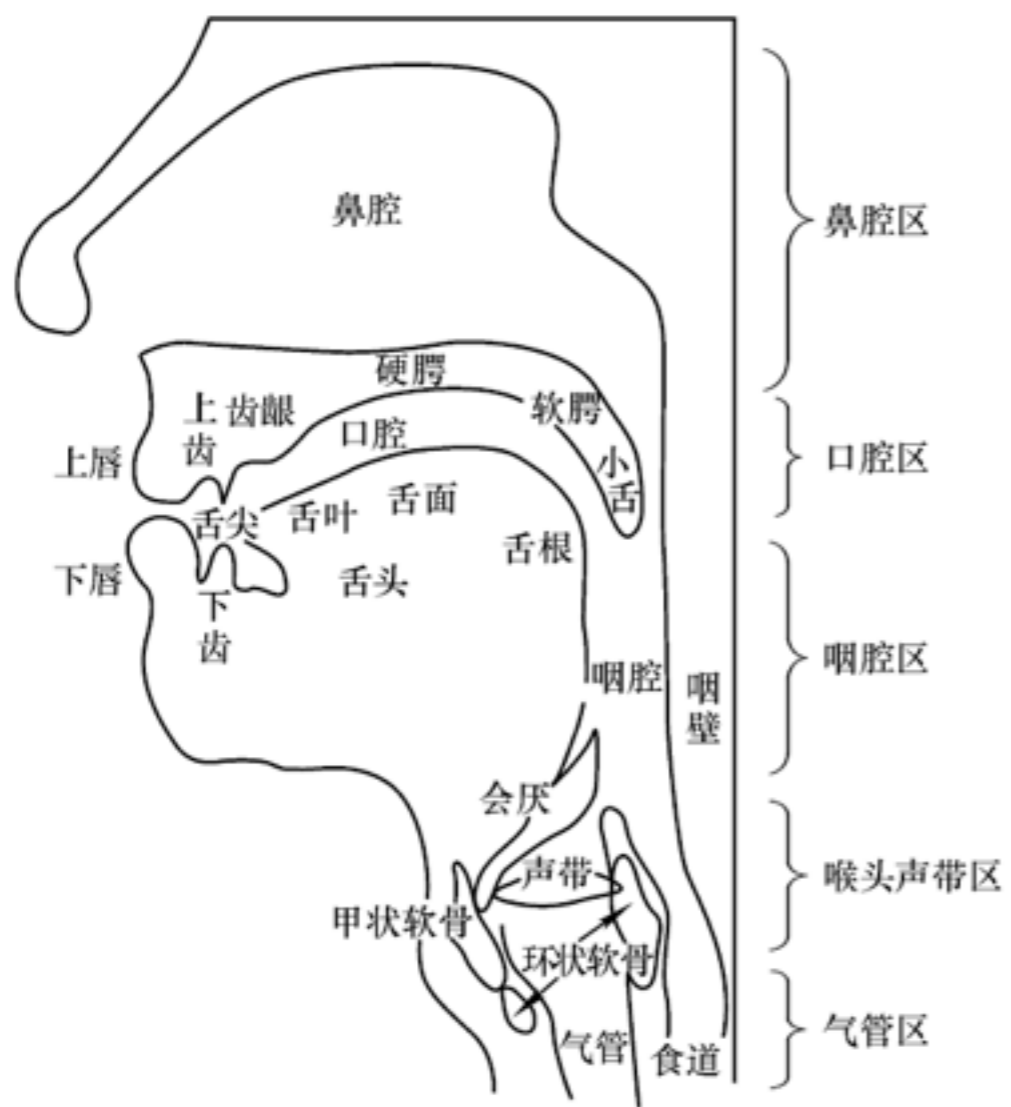


1996年，政府脸型识别实验 (FERET)
样本小于100个字节，好的大约为86个字节

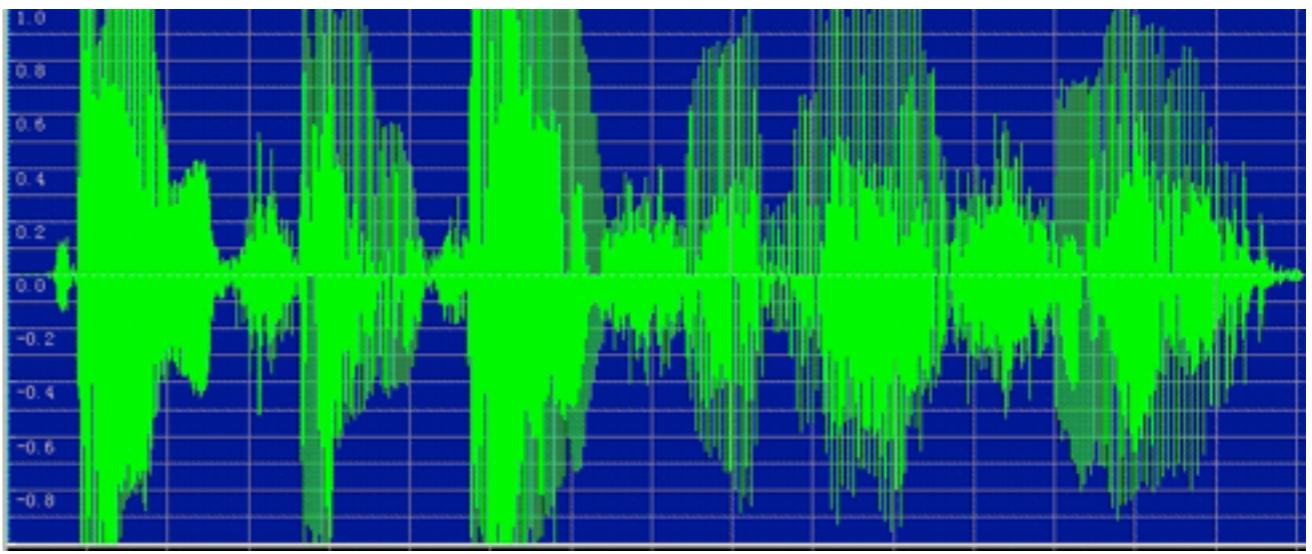
安全
剧场



语音



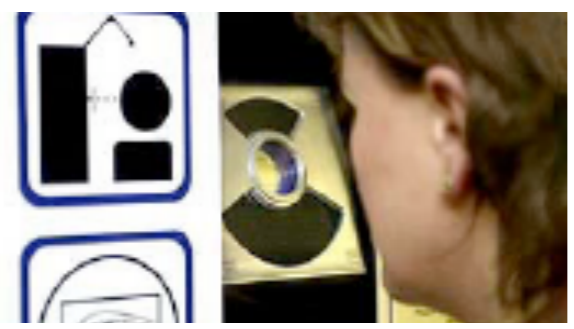
发音器官纵侧面示意图



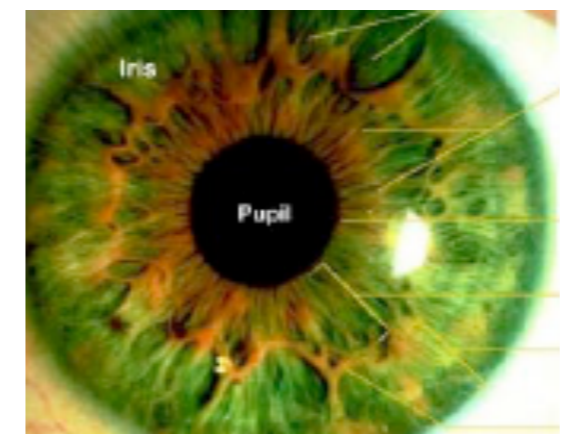
嘈杂环境、没有电话、不够健壮



结合了生理和行为两种成分
 语音识别 vs 发音者识别
 有约束识别 vs 无约束识别



眼镜
时间



虹膜编码
256字节



签名

- 最古老的方式
- 唯一、高效、难于伪造
- 注册验证简单方便
- 错报率高
- 容易被哄骗



- 伪造责任归属
- 卡上签名
- PIN & 电子令牌
- 电子签章

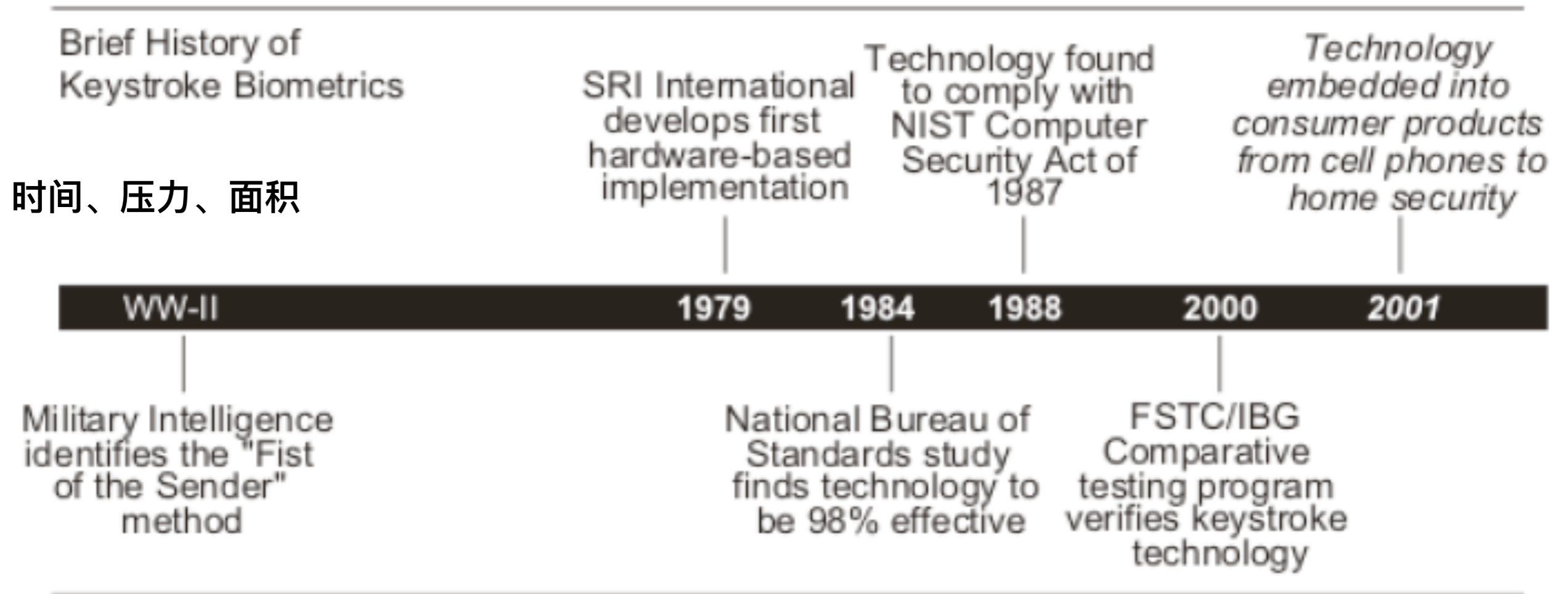
静态 vs 动态



□ ePadLink

- 分析速度、压力、加速度、节奏
- 存储小于1K，每秒40
- 灵活性好
- 能扩展到PDA、PC和网络

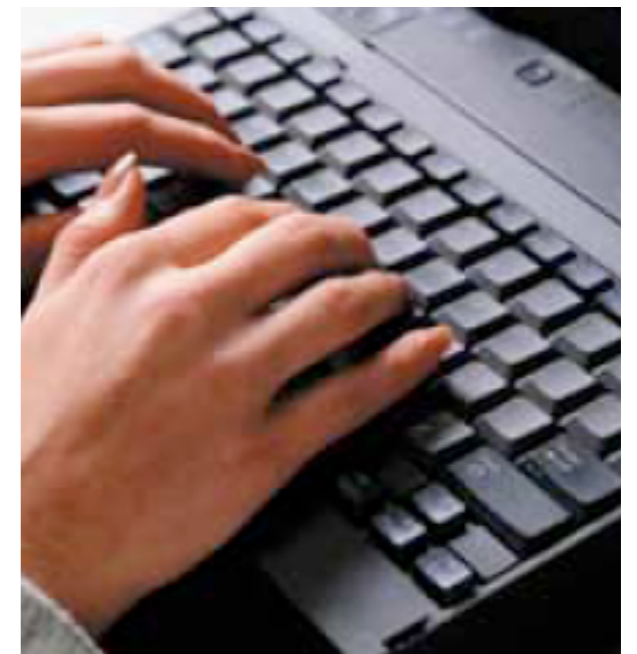
<http://www.epadlink.com/>



击键监控潜在的威胁已经超过了它的合理性
最自然的应用是“固化”口令
错误率过高，口令太短不行

作者识别
剽窃检测

<http://www.biopassword.com/>



其他



汗毛孔



身体气味



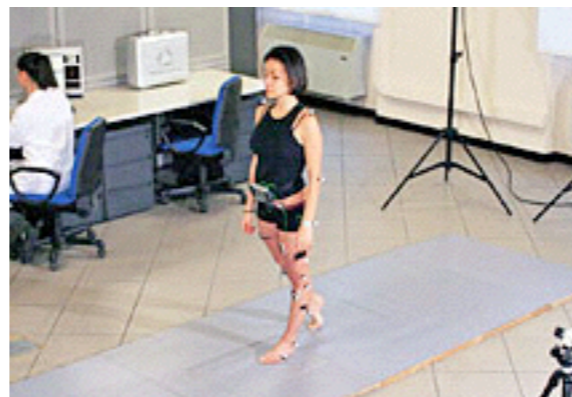
脚印



握手



和计算机或者智能手机的交互



步态



脑电波分析

生物学认证挑战

如果一个系统是人制作的
那么它也能被人击败

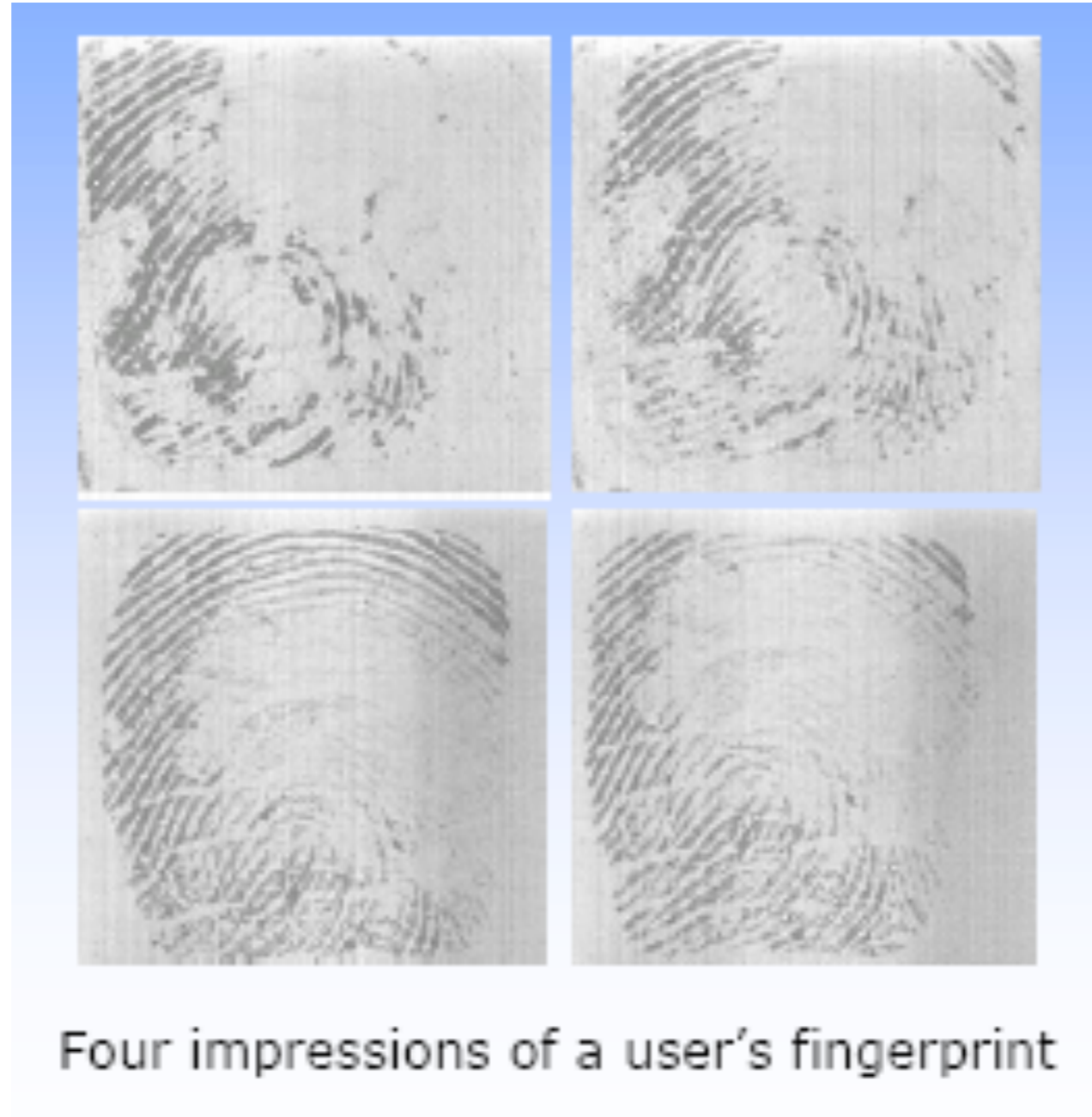


生日悖论

Biometrics Challenge

持久性







Put the plastic into hot water to soften it.

It takes around 10 minutes.



Press a live finger against it.



The mold



Pour the liquid into the mold.

It takes around 10 minutes.



Put it into a refrigerator to cool.

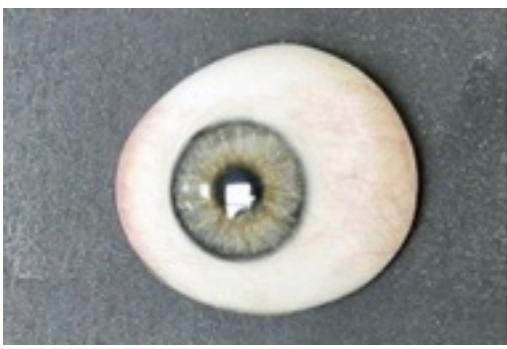
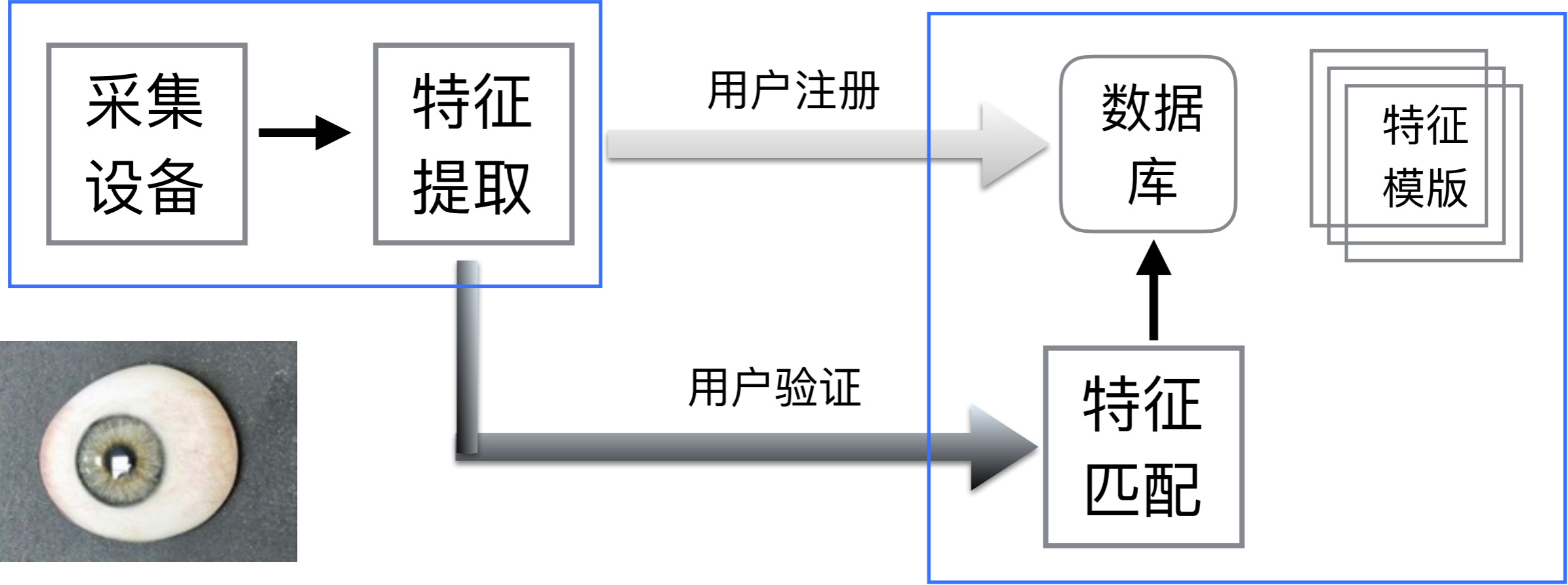


The gummy finger

攻击

错误注册
共谋

胁迫
职权滥用



物理攻击
模仿攻击

重放攻击
爬山攻击
中间人攻击

木马攻击

模版攻击

*Biometrics
Challenge*

欺骗



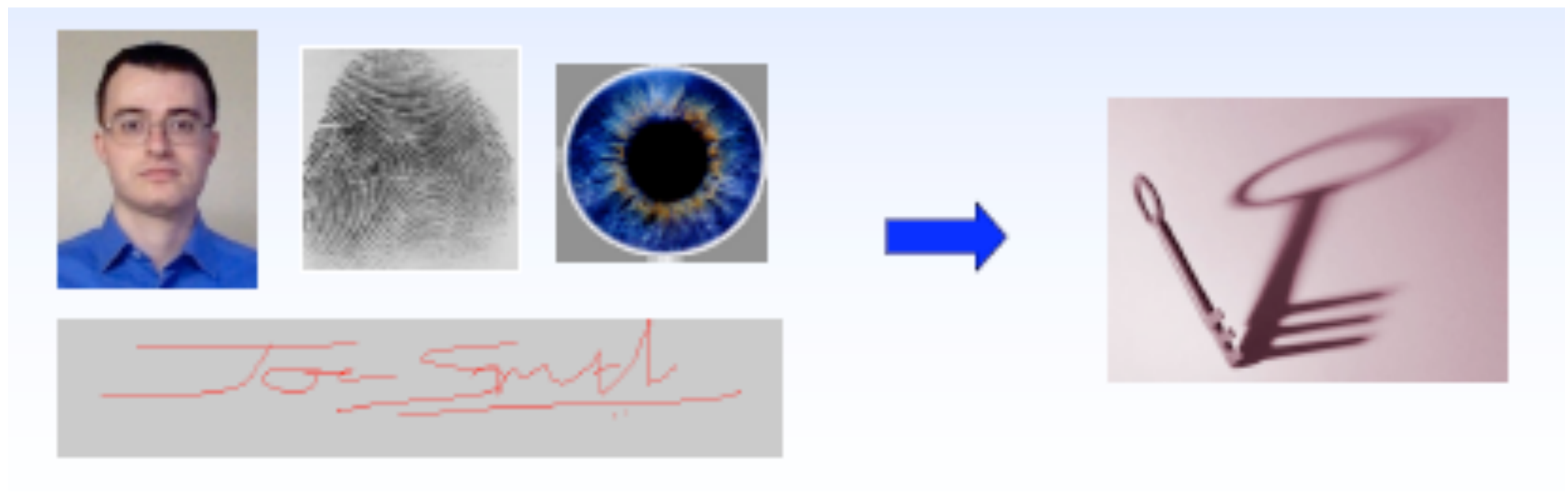
- 用户数据获取接口
- 有人监督 vs 无人监督
- 只能降低，不能根除
- 联合采用其余认证技术
- 现有技术
 - ✳ 活体内部固有特性
 - ✳ 分析活体自然产生的特点
 - ✳ 测试身体对外部刺激的反应

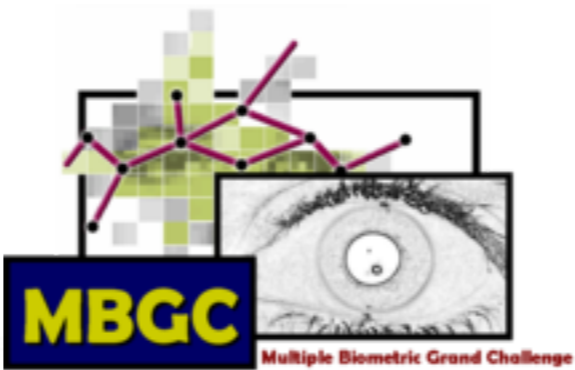


- 老大哥问题
- 匿名权和自由
- 公共安全 vs 公民自由
- 提高了保密性、检验身份、访问控制
- 单一化 vs 多样化
- 未经允许不能泄露

Biometrics Challenge

BioKey





- 你的物理特征
- 你的行为特征
- 你被感知的位置
- 你使用的硬件和软件
- 你的家庭和好友
- 你在网络上的行为
-

Defines
You!



Jon Crowcroft

September 24 at 3:38pm · London, United Kingdom · 🌐

smart phones, smart cars, smart homes, smart cities, smart lights, smart meters, smart clothes, stupid stupid stupid stupid people.

提问时间！

课后作业

```
graph LR; A[阅读教材] --> B[阅读论文]; B --> C[思考]; C --> D[撰写报告];
```

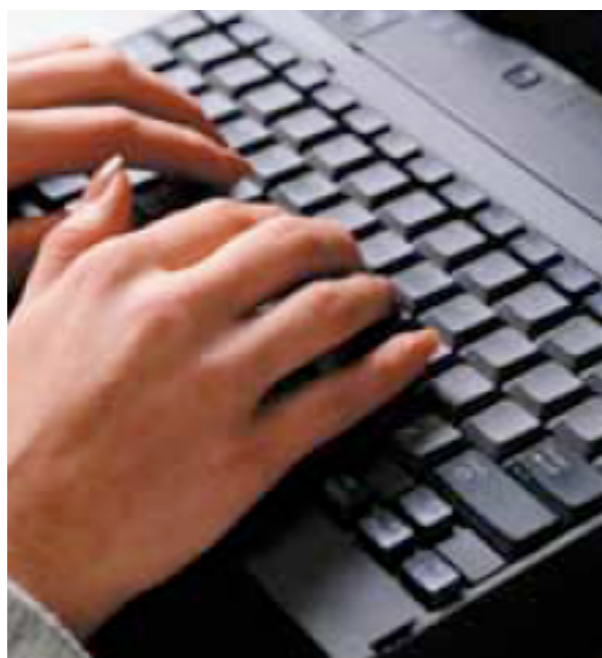
阅读教材

阅读论文

思考

撰写报告

完成一个Demo



击键认证、*Keystroke*

提交文档、PPT和代码

- 1、算法描述
- 2、实现效果
- 3、存在问题
- 4、主要收获
- 5、改进空间

11月8日晚上
12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

<https://huipingsun.github.io>