

基于生物特性可信接入协议的可信计算移动终端的应用研究

徐军^{1,2}

(1. 华北科技学院安全培训部, 河北 廊坊 065201;

2. 中国煤矿安全技术培训中心, 河北 廊坊 065201)

摘要: 在分析 TPM 可信平台的基础上讨论了安全生产监测平台的架构, 提出了基于可信移动平台的双 ARM+DSP 处理器的硬件架构, 以及用户接入过程的生物认证和用户终端硬件特性认证的注册协议, 并分析了其性能。实验结果表明, 新协议时间开销增加很小, 在 TPM 中更新指纹模板, 有效地增加了指纹的识别率。

关键词: 移动通信; 无线传感网络; 可信计算

中图分类号: TP311.5

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00143

Trusted computing mobile terminal application research based on biometric trusted access protocol

XU Jun^{1,2}

(1. Safety Training Department of North China Institute of Science and Technology, Langfang 065201, China;

2. National Safety Training Center of Coal Mines, Langfang 065201, China)

Abstract: The architecture of safety production monitoring platform was discussed based on the discussion of the TPM trusted platform, the hardware architecture based on trusted mobile platform of ARM + DSP dual core processor was proposed, the user access to the process of biometric authentication and user terminal hardware authentication properties of registration protocol were proposed, and its performance was analyzed. The experimental results show that the new protocol has a small increase in the time overhead, and the fingerprint template is updated in TPM, which effectively increases the recognition rate.

Key words: mobile communication, wireless sensor network, trusted computing

1 引言

无线通信网络在各行业应用的拓展带来了数据输入端的不确定性, 从而使网络本身所面临的安全性问题日趋严重。虽然从网络本身的基础设施建立来说, 各类无线通信系统在标准建立时已经考虑了网络安全体系结构, 但始终存在各种各样的问题, 包括系统内部的安全体系和应用系统的安全架构, 并且在不同行业应用方面也存在业务的需求和安全性要求。就安全生产监测网络系

统来说, 现有的信息安全隔离体系已不能完全满足安全生产监测网络各类无线传感网络采集终端、其他无线终端安全接入需求以及视频终端安全接入等信息安全问题。

无线网络本身目前主要存在以下安全问题:

- 1) 无线网络的干扰攻击;
- 2) 无线网络的被窃听;
- 3) 无线网络终端的硬件性能(如 CPU 性能、存储器、电池性能等)使其不能进行复杂度高的安全保护计算;
- 4) 无线网络终端易丢失, 从而被人冒用;
- 5) 无线网络终端的移动性及无线网络的异

构性,要求网络端进行的漫游、切换、信任管理的复杂性所带来的安全问题;6) 无线或有线链路上的安全威胁;7) 接入网和核心网的安全威胁;8) 无线终端操作系统的安全威胁;9) 其他无线网络的安全威胁,如利益相关单位的无线网络终端监测数据造假,瓦斯、水质等地质灾害数据的防抵赖与金融诈骗的防抵赖。

2 无线网络终端安全研究的现状

1) 无线传感网络的访问控制研究

无线传感网络的访问控制是近年来的研究热点,已经有较多的访问控制协议^[1~4]。但其主要关注点在传感网络的访问控制模块,没有考虑用户的身份隐私保护。Zhang 等^[5]提出了一种隐私保护的访问控制协议,采用盲签名技术来实现隐私保护,试图解决此问题。

2) 无线网络可信终端研究

1999年,Compaq、HP、Microsoft、IBM和Intel成立了TCPA(trusted computing platform alliance),提出了可信计算的思想,用于保护计算终端的安全。该组织2003年更名为TCG(Trusted Computing Group),将其标准的应用范围进行拓展,推广到移动电话及PDA等平台。2004年10月,TCG又制定了可信移动平台的硬件体系、软件体系以及协议3个技术标准草案,

用于解决移动终端的安全问题^[6~11]。另外,国内学者郑宇^[12]提出了基于可信移动平台和PKI相结合的4G安全体系和抽象的安全框架。

3) 安全生产监测监控系统安全性研究

安全生产监测监控系统目前主要是基于物联网技术的安全生产动态信息监管系统的构建,采用信息感知技术自动收集和识别位置、状态和环境等信息,通过无线传感器网络、移动通信网、互联网和专用网等多种途径,将传感器采集的动态数据传输至存储设备,并通过对海量数据的过滤、机器分析与数据挖掘,结合地理信息系统,形成可用信息^[13],文献^[14]研究了无线传感网在医疗、车辆、电网的安全性研究。但目前安全生产监测监控系统采集前端的安全性研究不深入。安全生产监测监控系统安全性除网络系统安全性外还要防止数据造假和抵赖。

3 基于TPM的安全生产监测网络体系结构

图1的安全生产监测系统结构考虑了各种环境下被监测对象的不同传感器类型来监测数据,通过信息融合来判断被监测目标的当前状态。在安全生产监测系统中,传感层主要通过针对不同生产监测环境采用不同类型的传感器获得或感知被监测对象的当前状态,通过有线或无线接口将采集到的数据传送到无线网络或有线网络。传输

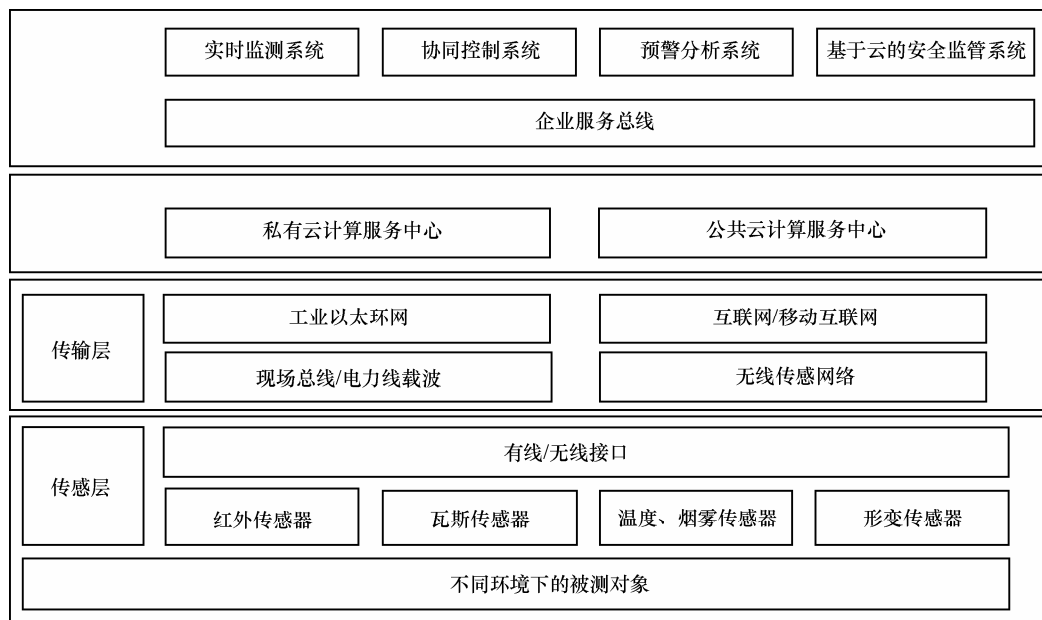


图1 安全生产监测系统

层中使用移动通信网络和无线传感网络,无线传感网络的终端主要在于不同类型的传感器,其采集的数据可以通过移动通信网络终端传输原始采集数据,也可以将传感器采集的数据进行数据分析后进行数据传输。私有云计算服务中心则是国家层面的安监管理部门负责组织管理,完成安全生产重要监测数据和分析数据的生成与分析使用。公共云计算服务中心则由安全生产管理部门和云计算技术设备厂商共同组织管理公共的基础信息和基础设施。

在图1的安全生产监测系统体系结构中,本文着重研究移动通信终端的安全性。图2则为安全生产监测系统可信移动终端设计,采用双ARM结构、主处理器运行操作系统以及其他应用,负责整个系统的控制与指挥。从处理器主要负责无线通信基带处理功能,完成数字基带和模拟基带的处理功能,包括无线接入的语音信号和模拟信号的调制解调、信道编解码和无线Modem控制等功能。

4 基于生物特性可信接入协议

UE的状态分为空闲状态和连接状态。开机后UE在空闲模式下,可以通过非接入层的信息单元IMSI、P-TMSI、TMSI等来区分不同的UE。

本文可以使核心网保留空闲模式下的UE信息。UE可以通过RRC连接建立,从空闲模式转移到连接模式(CELL-FACH或CELL-DCH)。而RRC连接释放后UE从连接模式到空闲模式。图3为空闲模式和连接模式的UE状态。

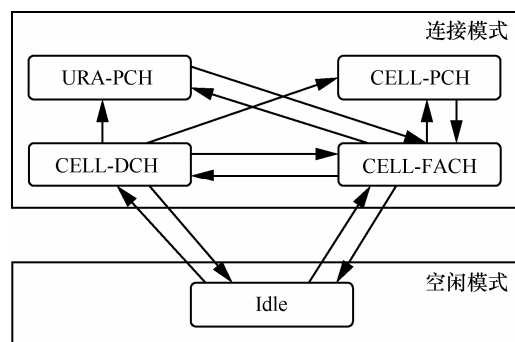


图3 UE状态跃迁示意

将指纹与虹膜信息与非接入层的UE的IMSI、P-TMSI、TMSI等标识紧密结合,提高了认证的安全强度,本文方案提供UE在空闲模式下在线证书验证功能,减少了数字签名和校验次数,提高了协议执行效率。USIM卡除完成密码运算外,还负责存储用户的数字证书和敏感信息,如认证参数、指纹/虹膜模板、指纹/虹膜匹配算法。

4.1 可信接入过程描述

1) 用户开机。判断是否有USIM,如有,则

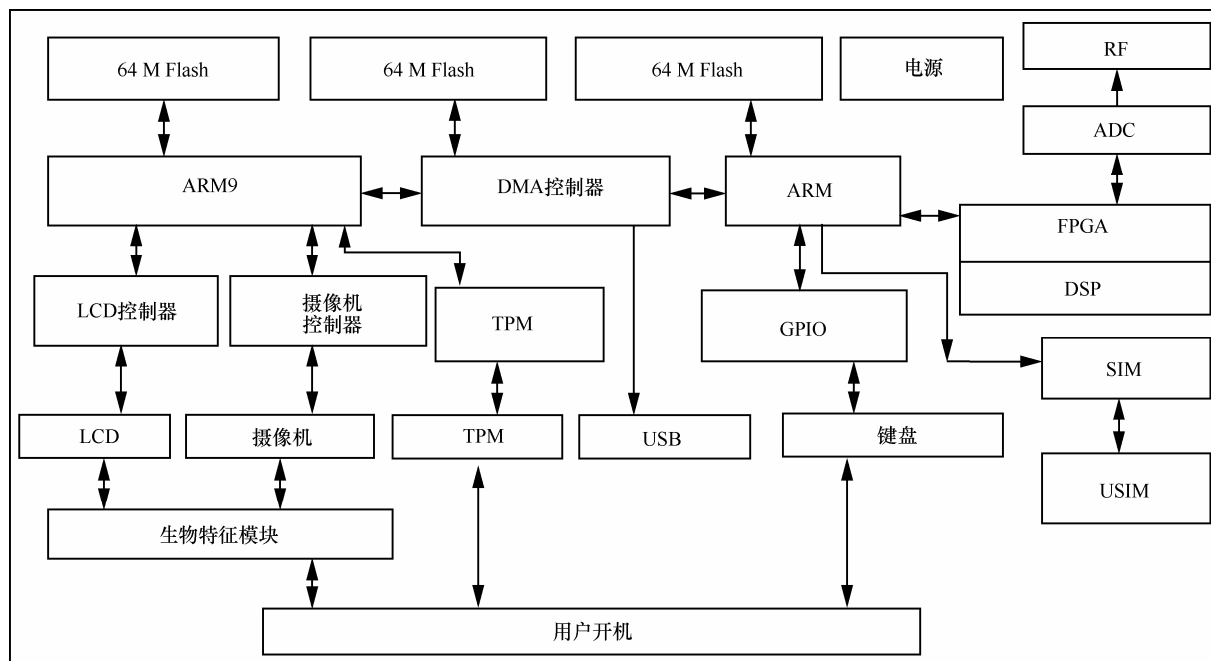


图2 可信移动终端安全体系结构

USIM 向 TPM 请求验证合法性, 转第 2) 步; 否则通知电源模块关机, 协议结束。

2) TPM 验证各部件的完整性。如果验证不通过, 通过 LCD 报警, 通知电源模块关机, 协议结束; 如果验证通过, TPM 验证指纹/虹膜的完整性。完整性未通过, 则协议结束, 关机; 完整性验证通过, 则向 USIM 报告 TPM 可用, 查询 TPM 中的指纹/虹膜并匹配生物信息。如在 TPM 中有指纹/虹膜信息, 并匹配成功, 则在 TPM 安全边界内完成 USIM 和用户的认证; 如未匹配成功, LCD 报警, 通知电源模块关机; 如在 TPM 中没有指纹/虹膜信息, 则属于新机主, 转第 3) 步, 进行新机主注册流程。

3) 移动终端开机完成后为空闲模式状态, 先选择用户和运营商确定的公共陆地移动(通信)网络 PLMN, 选择并驻留在满足条件的小区, 同时移动终端监测系统消息广播中该小区的邻小区, 选择所有小区中信号强度最好的小区驻留。移动终端通过发起位置登记过程或附着过程来通知网络侧自己的状态。这样移动终端可以接收 PLMN 广播的系统信息, 可以在小区内发起随机接入过程, 可以接收网络的寻呼, 可以接收小区广播业务。由于移动终端的移动性质, 需要进行小区重选过程来适应当前小区和邻小区信号强度不断变化的特性。当 UE 进行重选小区后, 要读取该小区的系统信息广播, 在这个小区属于另外一个位置区 LA 或路由区 RA, UE 发起位置更新过程。如果位置更新或附着不成功, UE 就要进行 PLMN 重选。

在空闲模式下, 移动终端和网络侧的联系是在移动终端和核心网中进行的。通过 NAS 消息, 利用保留信息域将机主的生物信息特征点传输到核心网络, 主要利用 3GPP 标准的两条消息 (CM SERVICE REQUEST 和 AUTHENTICATION REQUEST) 的保留信息域来传输生物信息特性模板。

4.2 可信移动终端信息流描述及性能分析

在 TPM 中存储私钥 SK_{TPM} 、证书 $Cert_{TPM}$ 与生物特征模块共享的密钥 K_{BT} 。

1) 用户开机后存在 USIM 时, USIM 和 TPM 之间的信息交互通过 USIM 向基带处理器中的

ARM 发送随机数 R_1 、 $IMSI$ 。基带处理器中的 ARM 通过 DMA 将 R_1 、 $IMSI$ 转发给应用处理器中的 ARM9。ARM9 通知 TPM 启动用户认证流程, 并向生物特征模块发送随机数 R_2 、 ID_{TPM} 。

2) 生物特征模块计算自身生物特征点 SR 的散列值 $H(SR)$, 并以 K_{BT} 为密钥加密 R_2 得到 $K_C = E(K_{BT}, R_2)$ 。以 K_C 为密钥计算 ID_{TPM} 和 $H(SR)$ 级联信息的生物特征模块的证书 $MAC_{BI} = MAC(K_C, ID_{TPM} \parallel H(SR))$ 。并将计算好的生物特征模块的证书传给 TPM。

3) TPM 利用 R_2 、 ID_{TPM} 、预存储的生物特征点以及共享密钥 K_{BT} 计算生物特征模块证书, 如果与收的证书一致, 则生物特征模块完整性成立。

4) TPM 利用自己的私钥 P_{TPM} 、随机数 R_1 、 $IMSI$ 以及产生的随机数 R_3 进行签名, 并将签名 $Sig_{TPM} = Sig(P_{TPM}, R_1 \parallel R_3 \parallel IMSI)$ 及 R_3 写入 RAM 中。

5) 主处理器 ARM9 通知基带处理器 ARM 从 RAM 中读取 TPM 的签名 Sig_{TPM} 及随机数 R_3 。

6) USIM 通过非接入层消息 CM SERVICE REQUEST 和 AUTHENTICATION REQUEST 向核心网传送证书 MAC_{USER} , K_{AU} 为网络共享密钥, 其中 $MAC_{USER} = MAC(K_{AU}, IMSI \parallel R_1 \parallel R_3 \parallel SR)$ 。

7) 核心网收到证书后, 恢复 SR 并根据 SR 通过生物特征匹配算法验证证书的合法性。

8) 根据 UE 的状态, 由于用户需要, 可以使移动终端由空闲模式进入连接模式。

由信息流分析得到, 不在本协议增加空中接口和网络之间的非接入层和接入层信令, 由此依然能满足不同厂商的协议兼容性, 时间开销在核心网中需要增加生物特征识别过程, 在用户终端中需要在基带处理器和主处理器中增加密码算法。第 5 节就生物特性模型采用指纹算法时进行具体实现过程描述, 采用虹膜方法也类似。

5 指纹识别算法

5.1 指纹识别技术研究现状

指纹识别技术包括图像获取、指纹增强、指

纹分割、指纹特征提取、指纹匹配、指纹分类与索引, 指纹识别中的安全、图像相似度计算。其中, 指纹特征提取和指纹匹配为关键技术, 指纹特征提取主要包括纹路方向计算技术、纹路频率计算技术、奇异点提取技术、纹路提取与细化技术、节点提取与过滤技术、纹数计算技术等; 指纹匹配包括参考节点对齐。纹路方向计算是指纹识别的前提, 采用基于像素之间的灰度关系或基于方向场模型全局地估计指纹图像各部分的方向。在图像分割过程、增强过程及纹路提取过程中需要通过纹路频率计算获取频率特征。可以采用傅里叶分析法, 经过傅里叶变换后得到具有 2 个峰值的频谱图像, 通过两峰值的长度计算出纹路频率。核心点和三角点统一称为奇异点。核心点和三角点在指纹分类、索引和匹配中起重要作用^[15]。指纹分割能够简化图像结构, 提高图像处理速度。指纹增强通过计算图像每个区域的局部特征(如方向和频率), 通过滤波器进行滤波来提高纹路结构的清晰度。

纹路提取和细化。一般的纹路提取方法是对增强后的指纹图像进行灰度二值化得到纹路图像。另一种纹路检测方法是基于指纹灰度图像进行纹路跟踪, 纹路跟踪法的缺点是难以处理大的断纹, 同时对于低质量图像效果不佳。纹路细化的目的是为了便于节点的检测。

节点提取和过滤。经过纹路二值化和纹路细化后可以在细化图像中检测节点的特征信息, 如端点和分叉点的特征信息。通过计算图像质量能够剔除低质量的指纹图像。指纹图像质量的计算方法有基于方向性区域和非方向性区域比例的方法、基于 Gabor 滤波器的方法等。

指纹匹配。Lee^[16]提出了基于 GBF 的提取具有核心点的图像局部区域的方向和频率来进行指纹匹配。指纹图像可以用节点集合来表示, 指纹中的节点是指纹路的端点和分叉点, 节点通常包含坐标、类型、方向等基本属性。Jain^[17]采用的对齐方法是分别从模板指纹的节点集合和输入指纹的节点集合中选取一个参考节点, 然后将两组节点对齐, 使参考节点对在坐标和方向上完全对齐。最后用约束窗口从对齐后的两组节点中寻找匹配节点对。两组节点对齐后, 离参考节点较远

的匹配节点对的位置差异和方向差异比离参考节点较近的匹配节点对的位置差异和方向差异要大。指纹采集时是将三维空间映射到二维平面上, 当按压的压力方向不垂直于采集面, 获取的图像就会产生非线性形变。为减少非线性形变对指纹匹配的影响, 采用 TPS (thin plane-spline) 处理非线性形变^[18-23]。首先从模板图像和待匹配图像中提取两组细节点, 进行匹配后得到一组候选点对, 通过这两组点对之间的形变 TPS 模型来求出形变参数。指纹识别的安全技术。指纹识别系统受到的攻击有: 1) 伪造指纹攻击; 2) 拒绝服务攻击; 3) 特洛伊木马攻击; 4) 重复使用攻击。在网络环境下的指纹应用中, 指纹特征被非法窃取。

5.2 特征点提取

特征点的提取包括图像分割、图像增强及图像细化几个步骤^[24]。以块为单位进行指纹分割, 将图像 I 分割成大小为 $w \times w$ (15×15) 的互不重叠的块, 图像 $I(m \times n)$ 共分成 $\frac{m}{w} \times \frac{n}{w}$ 块, 每一图像块

用 $W^1(i, j) \left(0 \leq i < \frac{m}{w}, 0 \leq j < \frac{n}{w} \right)$ 表示。 $O(W^1(i, j))$

表示 $W^1(i, j)$ 的平均纹路方向。 $O^1(x, y)$ 表示像素 (x, y) 的平均纹路方向。纹路方向的计算方法可以分为两大类型: 基于像素灰度关系的方法和基于方向场模型的方法。基于方向场模型的方法无依赖于核心点和三角点的准确检测, 而核心点和三角点的准确检测又依赖纹路方向的正确计算。方向场模型利用的是启发式知识, 根据奇异点位置可以预测全局纹路的大致走势, 这样预测出来的纹路并不能代表纹路的真实方向, 而且具有相同奇异点位置的 2 幅指纹图像完全可能拥有明显不同的纹路方向场。图像块纹路方向的计算采用基于梯度矢量的方法, 以像素 (i, j) 为中心, 以 w 为边长的方形区域的纹路方向 $O(W^1(i, j))$ 的计算方法如下。其中, $\langle G_x(u, v), G_y(u, v) \rangle$ 为像素 (u, v) 的梯度, 梯度的计算采用 Sobel 算子, 式(6)将方向规约到 $(0, \pi)$ 。

$$G_x(u, v) = \frac{\partial I(u, v)}{\partial u} \quad (1)$$

$$G_y(u, v) = \frac{\partial I(u, v)}{\partial v} \quad (2)$$

$$V_x = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (G_x^2(u,v) - G_y^2(u,v)) \quad (3)$$

$$V_y = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2G_x(u,v)G_y(u,v) \quad (4)$$

$$\theta^l(i,j) = \tan^{-1} \frac{V_y}{V_x} \quad (5)$$

$$O^l(i,j) = \begin{cases} \frac{\pi}{4}, & V_x = 0, V_y < 0 \\ \frac{3\pi}{4}, & V_x = 0, V_y \geq 0 \\ \theta^l(i,j) + \frac{\pi}{2}, & V_x > 0 \\ \theta^l(i,j), & V_x < 0, V_y \leq 0 \\ \theta^l(i,j) + \pi, & V_x < 0, V_y > 0 \end{cases} \quad (6)$$

$$O(W^l(k,l)) = O^l\left(kw + \frac{w}{2}, lw + \frac{w}{2}\right) \quad (7)$$

5.3 形变校正

在每次指纹采集时, 由于按压力度不一样, 指尖方向(Y方向)和垂直于指尖方向(X方向)的形变力度不一样。Glasbey 等^[25]于 1994 年针对多轨迹凝胶电泳中由于不同凝胶部分的蛋白质不均一流动性产生的失真, 提出了“笑脸”形变模型。本文假设手指按压Y方向的扩散特性为类似于凝胶的收缩速度特性, 其不同于凝胶之处在于凝胶属于收缩特性, 而指纹按压则属于扩散特性。设 m_{clm} 为图像的列数, 则指纹按压形变模型可表示为

$$U = \alpha X, \quad V = 100\beta \left[\frac{4}{n_{clm}^2} \left(Y - \frac{m_{clm}}{2} \right)^2 + 1 \right] Y$$

其中, $\alpha-1 \gg \beta-1$, 表示指纹按压时, 其指尖方向的变形远小于垂直于指尖方向的变形。

TPS 假设薄板只发生弯曲形变, 通过一些特定的数据点在具有最小线性弯曲能量的条件下进行插值。TPS 插值函数 $f(x,y)$ 满足以下最小化弯曲能量函数的条件

$$I_f = \iint_{R^2} \left(\left(\frac{\partial^2 f}{\partial x^2} \right)^2 + 2 \left(\frac{\partial^2 f}{\partial x \partial y} \right)^2 + \left(\frac{\partial^2 f}{\partial y^2} \right)^2 \right) dx dy \quad (8)$$

该函数的解为

$$f(x,y) = a_1 + a_x x + a_y y + \sum_{i=1}^m w_i U(\| (x_i, y_i) - (x, y) \|) \quad (9)$$

式(9)中 $U(r) = r^2 \log r^2$ 为核函数, 是双协调方程的基础解。权 w_i 与垂直作用于薄板上点 (x_i, y_i) 的集中力成正比。TPS 的系数 $\mathbf{a}$ 和 $\mathbf{w}$ 为以下线性方程式(10)的解。

$$\begin{bmatrix} \mathbf{K} & \mathbf{P} \\ \mathbf{P}^T & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{w} \\ \mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{f} \\ \mathbf{0} \end{bmatrix} \quad (10)$$

即 $\begin{bmatrix} \mathbf{w} \\ \mathbf{a} \end{bmatrix} = \begin{bmatrix} \mathbf{K} & \mathbf{P} \\ \mathbf{P}^T & \mathbf{0} \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{f} \\ \mathbf{0} \end{bmatrix}$, 由此可得所有未知参

数, 式中 $K_{ij} = U(\| (x_i, y_i) - (x_j, y_j) \|)$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, m$, $\mathbf{P}$ 的第 i 行为 $\mathbf{P}_i = (1, x_i, y_i)$, $\mathbf{w}$ 和 $\mathbf{f}$ 分别是 w_i 和 f_i 构成的列向量, $\mathbf{w} = (w_1, w_2, \dots, w_m)$, $\mathbf{a} = (a_1, a_x, a_y)^T$ 。

5.4 特征点匹配

从 RAM 中保留的模板特征点(坐标、类型、方向)和待匹配的特征点中寻找匹配节点对。先在模板指纹节点集合和输入指纹节点集合寻找多对参考节点, 然后将两组节点根据多对参考节点对齐进行节点排序, 以加快匹配速度。为了使 2 个指纹各区域的对齐程度相对均衡, 多参考节点选择尽量分布在指纹的各个区域。提取的每个节点信息如下。

1) 节点的坐标 (x, y) 。

2) 节点的方向 r , $0 \leq r < 2\pi$ 。

3) 局部相对方向 $D = \langle D_\alpha, D_\beta \rangle$, 其中 $D_\alpha = \{\alpha_i\}_{i=-N}^N$, $D_\beta = \{\beta_i\}_{i=-N}^N$, $\alpha_0 = 0, \beta_0 = 0$, α_i 和 β_i 分别为相对此节点的其他 2 个方向的累积方向值。

4) 排序数 $\Delta = \frac{\sum_{i=-N}^N \frac{i}{|i|} \alpha_i}{2N}$, $i \neq 0$ 。

若 $\Delta > 0$ 则称该节点为右手节点, 否则为左手节点。直观地说, 左手节点具有以下性质: 若将左手四指指向节点方向, 拇指朝上, 则该节点所在纹线的渐近中心位于手心一侧。右手节点也具有类似性质。将从指纹图像 I 中抽取的所有节点按照 Δ 排成递增序, 得到 $M(I) = \{< x_1^l, y_1^l, \gamma_1^l, D_1^l, \Delta_1^l >, \dots, < x_p^l, y_p^l, \gamma_p^l, D_p^l, \Delta_p^l >\}$, 其中, p 为节点数,

$\Delta_1^l \leq \Delta_2^l \leq \dots \leq \Delta_p^l$, $D_i^l = \langle D_\alpha^l, D_\beta^l \rangle$, $D_\alpha^l = \{\alpha_k^l | k=-N\}$, $D_\beta^l = \{\beta_k^l | k=-N\}$ 。节点模式的匹配过程通常包含节点对齐、节点配对和匹配分数计算 3 个过程。假设 T 和 Q 分别为模板指纹和输入指纹, 其节点集合分别为 $M(T) = \{\langle x_i^T, y_i^T, \gamma_i^T, D_i^T, \Delta_i^T \rangle | 1 \leq i \leq p\}$ 和 $M(Q) = \{\langle x_i^Q, y_i^Q, \gamma_i^Q, D_i^Q, \Delta_i^Q \rangle | 1 \leq i \leq q\}$, 节点模式匹配是为了从模板节点集合和输入节点集合中寻找对应节点对。可以通过以下步骤获取多参考点。对 $M(T)$ 和 $M(Q)$ 进行旋转和平移粗对齐。计算以 $\langle x_k^T, y_k^T, \gamma_k^T \rangle$ 为参考节点时 $M(T)$ 的极坐标形式为

$$M_k^P(T) = \{\langle r_i^T, \varphi_i^T, \psi_i^T, D_i^T, \Delta_i^T \rangle | 1 \leq i \leq p\}$$

其中, γ_i^T 和 φ_i^T 分别为极半径和极角, $\psi_i^T = \gamma_i^T - \gamma_k^T$ 。

类似地, 可以得到 $M_k^P(Q) = \{\langle r_i^Q, \varphi_i^Q, \psi_i^Q, D_i^Q, \Delta_i^Q \rangle | 1 \leq i \leq q\}$ 。

记 $C[u][v]$ 为 $M_u^P(T)$ 和 $M_v^P(Q)$ 的匹配节点对数, 采用一对参考节点将两组节点对齐, 然后用约束窗口检测匹配节点。在计算 $C[u][v]$ 时, 若 $|\Delta_u^T - \Delta_v^Q| > \tau_1$ 或 $|D_u^T - D_v^Q| > \tau_2$ (τ_1, τ_2 为阈值), 其中 $|D_u^T - D_v^Q| = \sum_{k=-N}^N (|\alpha_k^u - \alpha_k^v| + |\beta_k^u - \beta_k^v|)$, 则 $C[u][v] = 0$, 否则再匹配两组节点。令 $c = C[r_1][r_2] = \max\{C[u][v] | 1 \leq u \leq p, 1 \leq v \leq q\}$, 则将 $\langle x_{r_1}^T, y_{r_1}^T, \gamma_{r_1}^T \rangle$ 和 $\langle x_{r_2}^Q, y_{r_2}^Q, \gamma_{r_2}^Q \rangle$ 分别作为 T 和 Q 的参考节点时可以得到最大匹配节点对数 c 。假设此时得到的匹配节点集合分别为 $\{\langle x_{m_i}^T, y_{m_i}^T, \gamma_{m_i}^T, D_{m_i}^T, \Delta_{m_i}^T \rangle | 1 \leq i \leq c\}$ 和 $\{\langle x_{n_j}^Q, y_{n_j}^Q, \gamma_{n_j}^Q, D_{n_j}^Q, \Delta_{n_j}^Q \rangle | 1 \leq j \leq c\}$, 它们就是要求的多对参考节点, 其中 $\langle x_{n_j}^Q, y_{n_j}^Q, \gamma_{n_j}^Q, D_{n_j}^Q, \Delta_{n_j}^Q \rangle$ 和 $\langle x_{m_i}^T, y_{m_i}^T, \gamma_{m_i}^T, D_{m_i}^T, \Delta_{m_i}^T \rangle$ 为匹配节点对, 在 $M_{r_1}^P(T)$ 和 $M_{r_2}^P(Q)$ 为匹配节点对。

基于多参考节点对齐的基本思想就是将 $\{\langle x_{m_i}^T, y_{m_i}^T, \gamma_{m_i}^T \rangle | 1 \leq i \leq c\}$ 和 $\{\langle x_{n_j}^Q, y_{n_j}^Q, \gamma_{n_j}^Q \rangle | 1 \leq j \leq c\}$ 进行整体对齐, 为方便平移和旋转, 将其转换为极坐标表示, 分别为 $\{\langle r_{m_i}^T, \varphi_{m_i}^T, \psi_{m_i}^T \rangle | 1 \leq i \leq c\}$ 和 $\{\langle r_{n_j}^Q, \varphi_{n_j}^Q, \psi_{n_j}^Q \rangle | 1 \leq j \leq c\}$ 。在极坐标表示的对齐过程可以分解为对 $\{\langle x_{n_j}^Q, y_{n_j}^Q, \gamma_{n_j}^Q \rangle | 1 \leq j \leq c\}$ 的旋转和平移, 即要计算旋转参数和平移参数。

1) 计算 $\{\langle r_{m_i}^T, \varphi_{m_i}^T, \psi_{m_i}^T \rangle | 1 \leq i \leq c\}$ 和 $\{\langle r_{n_j}^Q, \varphi_{n_j}^Q, \psi_{n_j}^Q \rangle | 1 \leq j \leq c\}$ 方向差异 $\Delta_\psi = \frac{\sum_{i=1}^c (\psi_{n_j}^Q - \psi_{m_i}^T)}{c}$, 将

$\{\langle r_{n_j}^Q, \varphi_{n_j}^Q, \psi_{n_j}^Q \rangle | 1 \leq j \leq c\}$ 旋转 $-\Delta_\psi$, 得到 $\{\langle r_{n_j}^Q, \varphi_{n_j}^Q - \Delta_\psi, \psi_{n_j}^Q - \Delta_\psi \rangle | 1 \leq j \leq c\}$, 再计算其与 $\{\langle r_{m_i}^T, \varphi_{m_i}^T, \psi_{m_i}^T \rangle | 1 \leq i \leq c\}$ 的位置差异。

$$\Delta_x = \frac{\sum_{i=1}^c (r_{n_j}^Q \cos(\varphi_{n_j}^Q - \Delta_\psi) - r_{m_i}^T \cos(\varphi_{m_i}^T))}{c}$$

$$\Delta_y = \frac{\sum_{i=1}^c (r_{n_j}^Q \sin(\varphi_{n_j}^Q - \Delta_\psi) - r_{m_i}^T \sin(\varphi_{m_i}^T))}{c}$$

然后平移 $(-\Delta_x, -\Delta_y)$, 得到 $\{\langle r_{sn_j}^Q, \varphi_{sn_j}^Q, \psi_{sn_j}^Q \rangle | 1 \leq j \leq c\}$ 。对 $M_{r_2}^P(Q)$ 所有节点集合执行旋转 $-\Delta_\psi$, 再平移 $(-\Delta_x, -\Delta_y)$, 得到 $M_{sr_2}^P(Q)$, 则 $M_{r_1}^P(T)$ 和 $M_{sr_2}^P(Q)$ 进行了对齐。接下来就要对 $M_{r_1}^P(T)$ 和 $M_{sr_2}^P(Q)$ 在直角坐标系中进行节点匹配, $M_{r_1}^P(T)$ 和 $M_{sr_2}^P(Q)$ 在直角坐标系中表示为 $M_{r_1}^C(T) = \{\langle X_i^T, Y_i^T, \psi_i^T, D_i^T, \Delta_i^T \rangle | 1 \leq i \leq p\}$ 和 $M_{r_2}^C(Q) = \{\langle X_i^Q, Y_i^Q, \psi_i^Q, D_i^Q, \Delta_i^Q \rangle | 1 \leq i \leq q\}$ 。则 T 和 Q 最终匹配的节点数 $N = \sum_{i=1}^p \sum_{j=1}^q p(i, j)$, 其中 $p(i, j) = \begin{cases} 1, & |X_i^T - X_j^Q| \leq \xi_x, |Y_i^T - Y_j^Q| \leq \xi_y, |\psi_i^T - \psi_j^Q| \leq \xi_\psi \\ 0, & \text{其他} \end{cases}$ 其中, ξ_x, ξ_y, ξ_ψ 为阈值。

指纹匹配算法根据检测指纹特征点和模板特征点的相似程度决定是否属于同一个手指的指纹。 $M(T) = \{\langle x_i^T, y_i^T, \gamma_i^T, D_i^T, \Delta_i^T \rangle | 1 \leq i \leq p\}$ 和 $M(Q) = \{\langle x_i^Q, y_i^Q, \gamma_i^Q, D_i^Q, \Delta_i^Q \rangle | 1 \leq i \leq q\}$ 的相似度为

$$S_{TQ} = \frac{\sum \exp \left(-\frac{\rho \sum_{k=-N}^N (|\alpha_k^u - \alpha_k^v| + |\beta_k^u - \beta_k^v|)}{2\pi N} \right)}{N_T + N_Q - N_P}$$

其中, ρ 为常数, 实验中取 10, N 为采样点的数量参数, 2 个指纹对齐之后, 有一个重叠的公共区域 C , N_T 为 T 位于 C 中的节点数量, N_Q 为

Q 位于 C 中的节点数量。 S_{TQ} 越大, T 和 Q 越相似。

5.5 模板中特征点更新

通过上面利用多参考点的特征点匹配, 如果成功, 需要修改模板中的特征点的信息。利用均值改正。在 RAM 中存储的 $M(T)$ 为一个六元组, sum_i 为模板中该节点信息已经更新过的次数。

$M(T)$ ($M(T) = \{<x_i^T, y_i^T, \gamma_i^T, D_i^T, \Delta_i^T, sum_i> | 1 \leq i \leq p\}$) 待匹配的输入指纹为 $M(Q) = \{<x_i^Q, y_i^Q, \gamma_i^Q, D_i^Q, \Delta_i^Q> | 1 \leq i \leq q\}$, 如果匹配的结果为同一个手指指纹, 则将每个节点特征信息和输入指纹的信息进行简单加权。

$$x_i^T = \frac{x_i^T sum_i + x_i^Q}{sum_i + 1}, \quad y_i^T = \frac{y_i^T sum_i + y_i^Q}{sum_i + 1},$$

$$\gamma_i^T = \frac{\gamma_i^T sum_i + \gamma_i^Q}{sum_i + 1}, \quad D_i^T = \frac{D_i^T sum_i + D_i^Q}{sum_i + 1}, \quad \Delta_i^T =$$

$$\frac{\Delta_i^T sum_i + \Delta_i^Q}{sum_i + 1}, \quad sum_i = sum_i + 1, \text{ 然后将新的 } M(T)$$

存入 RAM 中。

5.6 基于指纹识别的安全接入协议

结合 3GPP 标准, 安全接入协议可以描述如下。

1) 首次提取指纹, 在 ARM 中运行指纹算法, 获得 $M(T)$, 并将特征点模板存入 RAM 中, 默认通过指纹验证, 以后以此认证模板为用户终端的拥有者。

2) UE 通知核心网, 并将 $M(T)$ 信息传送给核心网, UE 拥有者的指纹信息在核心网中注册完成。

3) 对于已经注册过指纹信息的手机, 开机后需要输入指纹, 提取特征点, 形成指纹特征点信息集合 $M(Q)$, 然后从 RAM 中提取 $M(T)$, 对比待匹配特征模板与认证模板获得形变程度

系数 β 和图像的列数 m_{clm} , 得到形变模型中未知参数。

4) 获取两模板中 m 对相应标记点坐标 i_{pts} 和 o_{pts} , 利用形变模型对坐标 i_{pts} 进行变换得到 $s_{i_{pts}}$ 。

5) 利用标记点坐标 $s_{i_{pts}}$ 和 o_{pts} , 通过公式

$$\begin{bmatrix} w \\ a \end{bmatrix} = \begin{bmatrix} K & P \\ P^T & 0 \end{bmatrix}^{-1} \begin{bmatrix} f \\ 0 \end{bmatrix} \text{ 获得 TPS 形变模型的未知}$$

参数 w_i ($i=1, 2, \dots, m$)、 a_1 、 a_x 、 a_y 。

6) 匹配 $M(T)$ 和 $M(Q)$, 若匹配成功, 则为合法使用者。否则 UE 状态不变, 仍处于空闲模式, 协议结束。

7) 匹配成功时, 利用 3.5 节的方法修改 $M(T)$ 。

8) 将 $M(T)$ 存入 RAM 中, 并将 $M(T)$ 信息传送给核心网。

6 实验结果

本文提出的基于生物特性的可信移动终端及接入协议, 采用在 TPM 中保留生物特性特征模板, 在核心网侧也保留相应的密钥, 可以防止移动终端丢失而被人冒用。实验环境由 3 块单板组成, 分别执行 UE、NODEB、RNC/CN 的功能。后台工作站由 PC 机构成, 用于进行信令监测。信令监测过程如图 5~图 7 所示。

在指纹算法中, 为提高指纹特征模板的顽健性, 本文提出了基于 TPS 模型的符合移动终端用户使用需要验证特点的指纹匹配算法, 在两方面进行了改进。一是在非线性形变的处理中, 借助凝胶的“笑脸”形变模型, 提出了指纹按压形变模型, 先经过指纹按压形变模型进行校正,

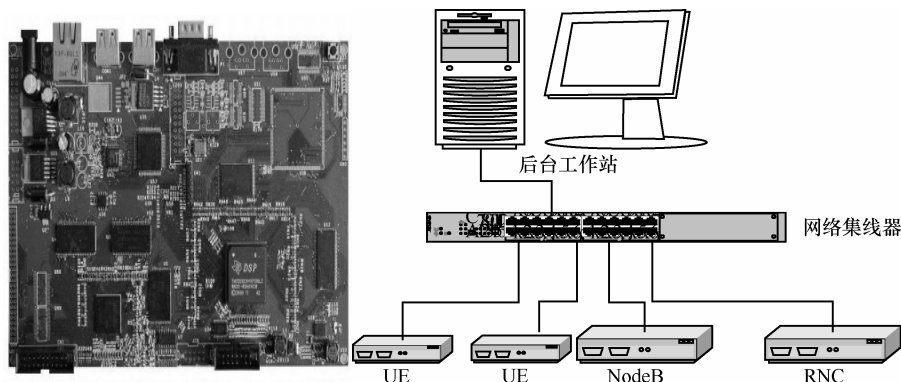


图4 实验环境

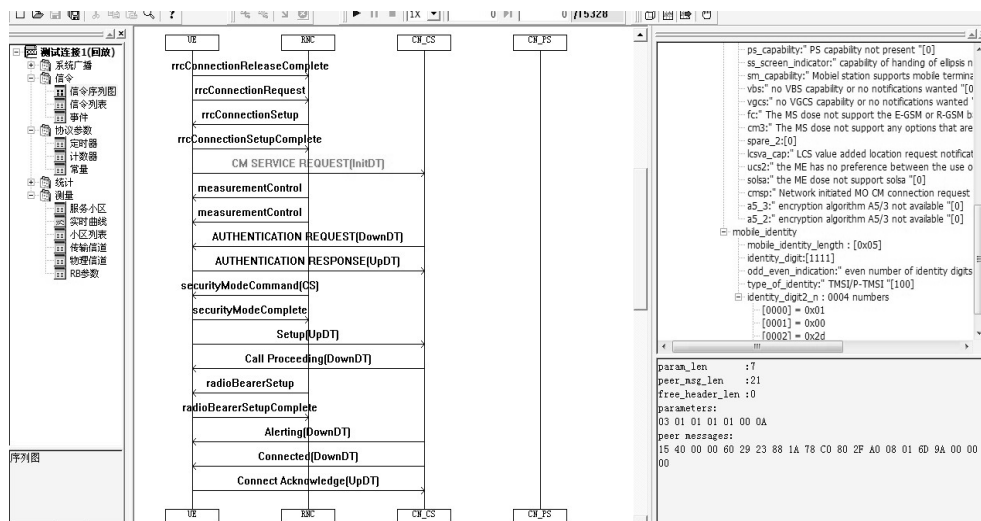


图5 UE侧CM SERVICE REQUEST

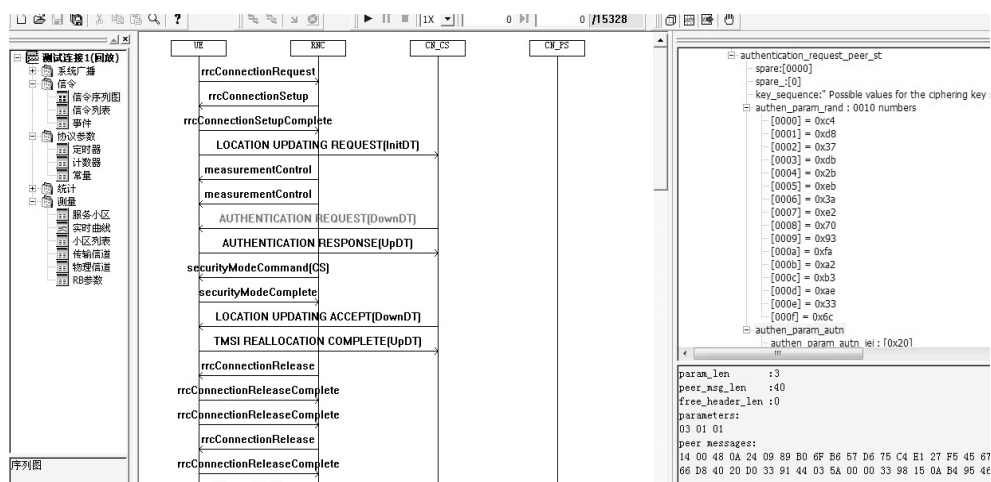


图6 UE侧AUTHENTICATION REQUEST

编号	1. 链路ID	1. 协议	1. 消息	2. 协议	2. 消息	3. 协议	3. 消息	4. 协议	4. 消息	5. 协议	5. 消息
6020	2. 18	3. FP	DATA								
6021	2. 18	3. FP	DATA	RRC_DC...	initialDirectTransfer	NAS_MM	CM SERVICE REQUEST				
6022	2. 17	3. FP	DATA								
6023	2. 17	3. FP	DATA								
6024	2. 17	3. FP	DATA								
6025	2. 17	3. FP	DATA	RRC_DC...	downlinkDirectTransfer	NAS_MM	AUTHENTICATION REQUEST				
6026	2. 17	3. FP	DATA								
6027	2. 18	3. FP	DATA	RRC_DC...	uplinkDirectTransfer	NAS_MM	AUTHENTICATION RESPONSE				
6034	2. 18	3. FP	DATA								
6035	2. 18	3. FP	DATA								
6036	2. 17	3. FP	DATA								
6039	2. 17	3. FP	DATA								

BITMASK	IE名	值	注释
0000----	service type	1	Mobile originating call establishment or packet mode connection establishment
----0000	Ciphering key sequence num	0	
----0000	CSM	0	
-----0	spare	0	
	Mobile station classmark	2	
	IE Length	3	
011----	RF power capability	7	All other values are reserved
---0----	AS/1 algorithm supported	1	encryption algorithm AS/1 not available
---0----	ES IND	0	'Controlled Early Classmark Sending option' is not implemented in the MS
---00---	Revision level	2	Used by mobile stations supporting R99 or later versions of the protocol
---00---	spare	0	
0-----	Frequency Capability	1	The MS does support the E-GSM or R-GSM (For definition of frequency bands s
-1-----	VGCS notification receipt	1	VGCS capability and notifications wanted
---0----	VBS notification receipt	1	VBS capability and notifications wanted
---0----	SM capability	1	Mobile station supports mobile terminated point to point SMS
---10--	SS Screening Indicator	0	default value of phase 1
---0----	PS capability	1	PS capability present
---0----	spare	0	
0-----	AS/2 algorithm supported	1	encryption algorithm AS/2 available
0-----	AS/3 algorithm supported	1	encryption algorithm AS/3 available
---1----	CM Service Present	1	'Network initiated MO CM connection request' supported for at least one CM s

HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	15	40	00	00	60	29	21	88	1a	7a	7a	78	2f	a0	c0	a8
10	00	82	00	00	40											

图7 CN侧鉴权流程

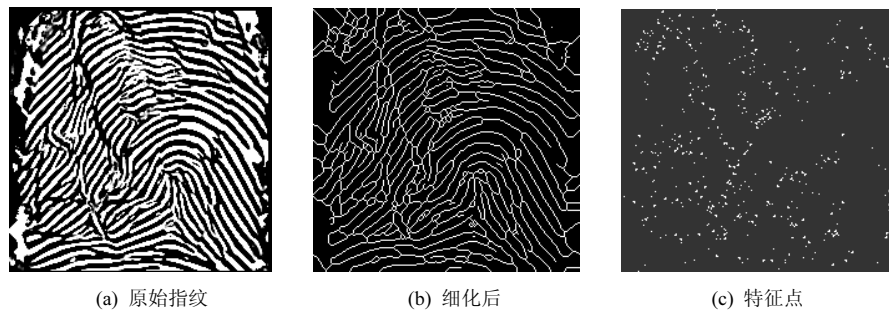


图 8 指纹算法实验

然后再进行 TPS 插值。二是考虑到移动通信终端使用的特点，通过阈值来控制匹配的精度，并将匹配成功的指纹信息加入到特征模板中，这样随着验证的次数增多，指纹模板越来越能够减少指纹采集误差的影响。指纹算法实验如图 8 所示。在 FVC2004 中选取 100 个指纹，并对该 100 个指纹通过方向场模型生成新的指纹图像（首先根据奇异点位置生成方向场，然后用滤波器生成指纹纹路）。表 1 说明随着模板更新次数越多，识别率提升明显，经过 500 次的更新，识别率提高了 1.59%。

表 1 指纹算法的识别率	
次数	准确率
1	93.46%
10	93.82%
100	94.78%
500	95.05%

7 结束语

本文利用双 ARM 硬件结构，通过指纹识别和 TPM 结合的方法获得较为可信的安全终端。在指纹采集过程中采用 TPS 变形模型对指纹进行校正，并对本次指纹识别的结果与先前保存在 TPM 中的指纹模板进行优化，并将优化后的模板替代之前存储在 TPM 中的模板，从而提升指纹识别率。

参考文献：

[1] WANG H, SHENG B, LI Q. Elliptic curve cryptography-based access control in sensor networks[J]. International Journal of Security and Networks, 2006, 1(3/4): 127-137.

[2] HE D, GAO Y, CHAN S, et al. An enhanced two-factor user authentication scheme in wireless sensor networks[J]. Ad Hoc and Sensor Wireless Networks, 2010,10(4):361-371.

[3] SONG H, ZHU S, ZHANG W, et al. Least privilege and privilege deprivation: toward tolerating mobile sink compromises in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2008: 4(4).

[4] WANG H, LI Q. Distributed user access control in sensor networks[J]. Lecture Notes in Computer Science, 2006(4026): 305-320.

[5] ZHANG R, ZHANG Y, REN K. DP2AC: distributed privacy-preserving access control in sensor networks[C]//The IEEE Infocom. 2009: 1251-1259.

[6] Trusted mobile platform hardware architecture description[EB/OL]. http://www.trusted-mobile.org/TMP_HWAD_rev1_00.pdf.

[7] Trusted mobile platform software architecture description[EB/OL]. http://www.trusted-mobile.org/TMP_SWAD_rev1_00.pdf.

[8] Trusted mobile platform protocol specification document[EB/OL]. http://www.trusted-mobile.org/TMP_Protocol_rev1_00.pdf.

[9] TPM main part 2: TPM structures[EB/OL].http://www.trusted-computinggroup.org/downloads/tpmwmmainrev62_Part2_TPM_Structures.

[10] Infineon technologies. Infineon technologies TPM[EB/OL]. <http://www.national.com/pf/pc/PC21100.html>

[11] A trusted biometric system[EB/OL]. <http://www.hpl.hp.com/techreports/2002/2002-HPL-185.pdf>.

[12] 郑宇. 4G 无线网络安全若干关键技术研究[D]. 成都: 西南交通大学, 2006.

ZHENG Y. Some key technologies used in 4G wireless network security research[D]. Chengdu: Southwest Jiaotong University, 2006.

[13] 张磊. 基于物联网的安全生产动态监管系统的设计与实现[D]. 厦门: 厦门大学, 2012.

ZHANG L. Dynamic production safety supervision system based on Internet of things in the research and design[D]. Xiamen University, 2012.

- [14] 何道敬. 无线网络安全的关键技术研究[D]. 杭州: 浙江大学, 2012.
- HE D J. The key technology of wireless network security research[D]. Hangzhou: Zhejiang University, 2012.
- [15] BAZEN A M, GEREZ S H. Systematic methods for the computation of the directional fields and singular points of fingerprints[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(7): 905-929.
- [16] LEE C J, WANG S D. Fingerprint feature extraction by principal gabor basis function[J]. Pattern Recognition, 2001, 34: 2245-2248.
- [17] JAIN A K, HONG L, PANKANTI S, et al. An identity authentication system using finger print[J]. Proceedings of the IEEE, 1997, 85(9): 1365-1388.
- [18] ROSS A, DASS S, JAIN A. A deformable model for fingerprint matching[J]. Pattern Recognition, 2005, 38: 95-103.
- [19] CAPPELLI R, MAIO D, MALTONI D. Modeling plastic distortion in fingerprint images[C]//Advances in Pattern Recognition — ICAPR 2001. 2001:371-378.
- [20] BAZEN A M, GEREZ S H. An intrinsic coordinate system for fingerprint matching[J]. Lecture Notes in Computer Science, 2001, 2091: 198-204.
- [21] SENIOR A, BOLLE R. Improved fingerprint matching by distortion removal[J]. IEICE Transaction Information and System, Special Issue on Biometrics, 2001,(7): 825-831.
- [22] BAZEN A M, GEREZ S H. Elastic minutiae matching by means of thin-plate spline models [C]//The International Conference on Pattern Recognition, 2002: 985-988.
- [23] ROSS A, DASS S C, JAIN A K. Estimating fingerprint deformation[C]//The International Conference on Biometric Authentication. 2004:2490255.
- [24] 祝恩. 低质量指纹图像的特征提取与识别技术的研究[D]. 湖南: 国防科技大学, 2005.
- ZHU E. Low quality fingerprint image feature extraction and recognition technology research[D]. Hunan: National University of Defense Technology, 2005.
- [25] GLASBEY C A, WRIGHT F. An algorithm for unwarping multi-track electrophoretic gels[J]. Electrophoresis, 1994, 15(1): 143-148.

作者简介:



徐军(1970-), 男, 湖南邵阳人, 博士, 华北科技学院高级工程师, 主要研究方向为移动通信系统、嵌入式系统、数字图像处理。

收录声明

本刊对发表的文章,拥有出版电子版、网络版版权,并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Chinese Journal of Network and Information Security has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果,无一稿多投;论文内容不涉及国家机密;未曾以任何形式用任何文种在国内外公开发表过;论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题,论文作者将承担全部责任。

The authors of *Chinese Journal of Network and Information Security* guarantee that their submitted article is original and contains nothing confidential. The said article is only submitted to *Chinese Journal of Network and Information Security*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

网络 Chinese Journal of
信息安全学报 Network and Information Security

读者信箱:
cjin@bjxintong.com.cn
官方微信:



2017年2月15日出版

定价: 30.00元

ISSN 2096-109X

