智能手机中指纹技术的安全性分析

臧亚丽

中国科学院自动化研究所,北京 100190

近两年,配备指纹识别功能的智能手机逐渐成为了市场的主流产品。指纹手机的功能除了屏幕解锁,也推广至各类手机App内的认证和移动支付等,但对于指纹识别安全性的质疑和争议从未停止。本文分析指纹识别系统和其在智能手机中应用的安全性。

自2013年9月美国苹果公司发布了搭载Touch ID的指纹手机iPhone 5S以来,国内外各大主流手机生产厂商都陆续推出了带有指纹识别功能的手机产品。一时间,指纹识别功能俨然成了主流智能手机的标配,而指纹手机也引起了大众的普遍关注。在Touch ID问世之前,指纹识别就已经不是陌生的技术,而指纹手机也并非苹果公司首创。2005年,中国科学院自动化研究所和波导公司等就曾联合发布了国内首款指纹识别手机。而在2011年前后,摩托罗拉、东芝等也先后在其手机新产品中加入指纹芯片。在苹果之前,没有一家公司成功推广其指纹手机,这其中有技术成熟度、市场成熟度等多方面的原因,但不可否认的是,苹果公司在指纹功能的易用性和安全性上的设计是其产品成功的重要助力。易用性自不必说,HOME键手指一按解锁的简单快捷已经深入人心;安全性一方面表现在指纹识别准确率的提升,使得非法指纹通过系统验证的可能性更加微乎其微,更重要的是对于手机采集的指纹信息的保护和对于假指纹抵御的考量。2014年Apple Pay的发布及其业务于2016年在国内上线,使指纹功能的安全性成为不仅关系到手机安全本身,同时关系到金融安全的大问题。再次引发对指纹手机安全性的质疑和争议。那么,目前指纹手机的安全性究竟如何?Touch ID的"安全性的提升"是相对于以前的指纹技术和指纹手机而言,而相对于密码、图形等传统认证手段,指纹认证的安全性有本质提升么?指纹的应用对于智能手机的信息安全和移动支付的金融安全,究竟是救赎者还是破坏者?本文围绕上述问题加以阐述。

1 指纹如何实现身份识别

指纹是手指末端皮肤表面凹凸的纹路。通过计算机技术处理后,指纹就表现为深浅不一的灰度纹理图像,如图1所示。这些纹线的形状、长度、末梢点、分叉点等属性都可以作为指纹匹配的特征,用于计算指纹图像之间的相似度,其中末梢点和分叉点统称为指纹细节点,是目前公认最常用、最有效的指纹特征。由于人类胎儿时期指纹成长的随机性,全世界范围内也很难找到两枚完全一样的指纹。而指纹一旦形成,几乎终生不会改变。我们称这两个特性为唯一性和持久性,这是任何一种身份认证手段的必要属性。除此之外,指纹具有易被用户接受、系统成本低、易用性高、认证精度高等多种优势,都是促成指纹广泛应用的重要原因。

一个完整的指纹识别系统如图2所示。系统通过采集指纹图像、指纹图像增强和特征提取后,将指纹特征作为模板进行存储,被存储的指纹即成为系统的合法用户;用户请求系统认证时,同样需要经过采集、增强和特征提取的处理,然后将提取到的特征与系统中存储的模板特征进行比对,计算出两组指纹特征的相似度分数;如果该分数超过一定的阈值,就认为输入指纹和模板特

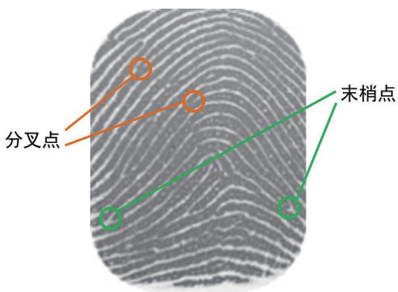

图1 表现为灰度纹理图像的指纹及其分叉点和末梢点

收稿日期:2016-04-28

作者简介:臧亚丽,助理研究员,研究方向为生物特征识别、指纹识别与指纹加密,电子信箱:yali.zang@ia.ac.cn

引用格式:臧亚丽. 智能手机中指纹技术的安全性分析[J]. 科技导报,2016, 34(9): 59-62; doi:10.3981/j.issn.1000-7857.2016.09.008

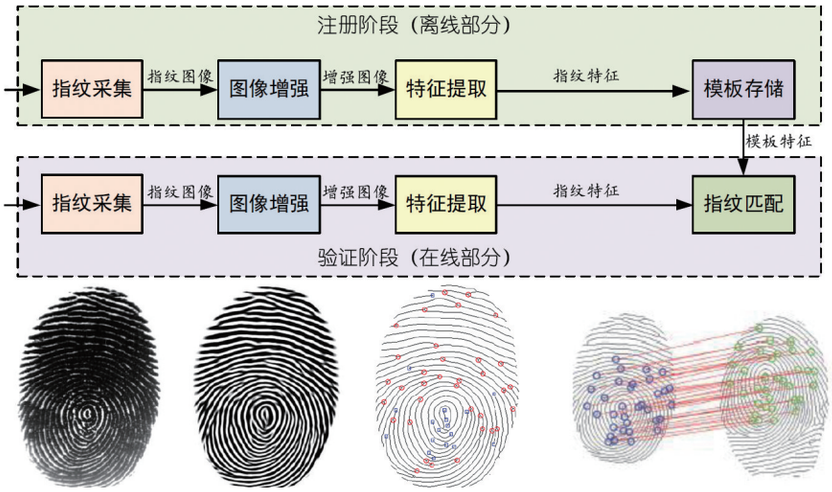

图2　指纹识别系统流程

征来源于同一个用户，通过认证，否则认证失败。

虽然指纹具有唯一性，但是在指纹识别系统对指纹进行采集和处理的过程中，每个阶段都可能有信息损失，所以指纹识别系统达不到100%的认证精度，这其中最简单直接的损失就是采集面积的不完整。一般用于评价一个指纹识别系统性能的好坏，最常见的指标就是误识率和拒识率。拒识率是指合法用户被系统拒绝的概率，也称错误不识别率、拒真率等；而误识率是指非法用户被系统接受的概率，也称错误识别率、认假率等。这两个指标是相互矛盾的，即对于一个特定的系统，误识率的下降必然带来拒识率的上升，但可以通过系统内部算法的不断优化来实现两个指标的同步改善。就目前的技术水平而言，对于采集面积相对完整的指纹图像，系统性能在误识率小于10^{-6}的前提下，拒识率可以控制在1%甚至更低。这个性能表示当用非法用户的指纹对一个合法用户进行认证攻击时，平均需要10万种尝试才会有一次成功通过系统认证；而该合法用户指纹的每一百次正常输入中，最多只有一次被系统拒绝而需要重新输入。不过，在当前指纹手机中的应用情境下，由于采集面积非常小，系统性能会有一定程度的下降。但应用于智能手机的指纹识别系统仍然有较高的性能要求，如误识率小于2×10^{-6}及拒识率小于3%。

由此可见，指纹作为一种身份认证的手段，其识别的准确率是完全可以适用于大多数的应用情景之下的。尤其是智能手机这种单机用户最多只有10余人的情况，即使因采集面积小导致了性能下降而使得拒识率略有提升，但出现误识的概率仍然是微乎其微的。

2　指纹识别系统安全性分析

指纹识别系统之所以有广泛的应用，主要在于其带给用户的两大优势：方便与安全。方便性主要体现在不像ID卡或U-Key一样需要随身携带，也不像密码一样需要记忆；而安全性则体现在不会丢失、也无需担心被猜到或暴力破解。但是应用指纹技术后系统的安全性真的就比使用传统密码或图形等加密手段有本质上的提升么？答案是否定的。

密码的不安全性主要在于它容易被别人破解，同样的，指纹也存在被复制的威胁，如假指纹。当然，制作高质量的假指纹比窃取或破解密码要困难很多，但并非完全不可能。在2013年iPhone 5S上市后的3天内，就有欧洲的黑客组织声称可以通过玻璃杯上的指纹残留制作假指纹来通过Touch ID的检测。在实际生活中，由于双手的频繁使用，在物体表面留下指纹的概率非常高，但是采集这种指纹并制作出假指纹仍然需要一定的专业知识和技术，而且当前的指纹采集设备大都具备一定的抗假指纹能力，这就对假指纹制作的质量和材料提出了更多的要求。也有人说，密码是虚拟的存在，而指纹就实实在在地裸露在手指表面，因此指纹要比密码容易获取，但换一个角度思考，密码可以通过偷窥或监控录入过程来获知，而指纹即使在被监视的状态下录入也不会泄露任何信息。而且从获取到指纹的痕迹或照片到实际攻击系统成功，中间还有很多的步骤，如制作假指纹的工艺和材料等。图3展示了一些通过物体表面残留痕迹采集到的指纹图像和直接拍照得到的指纹图像。可以发现，通过物体表现采集到的指纹图像质量往往很差，而拍照得到的指纹图像由于角度、光线的影响和分辨率的限制，其清晰性和完整性和较难保证。在手指主人不配合的情况下，想要窃取其指纹并制作高质量的假指纹是非常具有挑战性的。因此，就被复制的难度而言，指纹比密码等传统认证手段要安全得多。

而在其他方面，指纹却面临着密码不会带来的威胁。密码一旦被别人破解，用户可以选择更换密码，不论密码被破解带来的损失有多少，更换密码后系统又重新变得安全了。有很多的系

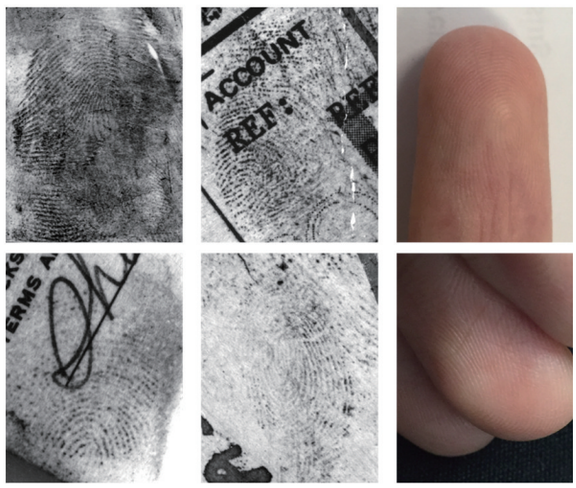

图3　物体表面残留指纹和拍照得到的指纹

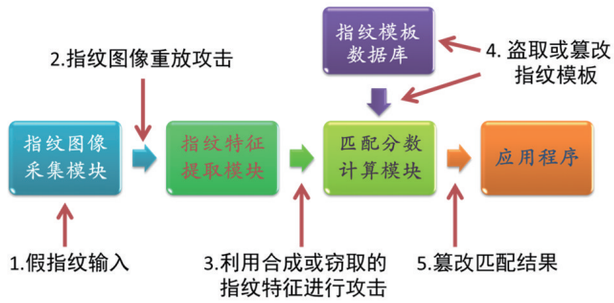

图4　指纹识别系统面临的几种攻击威胁

统要认证也因此有大量不同的密码。攻击者很难通过一个破解的密码而得知用户其他系统的密码,更无法通过密码相同就确定两个系统的用户是同一个人。以上可以概括为密码的可撤销性和无关联性,这两种属性对于有丢失可能的身份认证凭据非常重要。

如果指纹是这些系统的认证手段,则攻击者的以上困惑就很容易解决了:成功复制到用户指纹后,用户可以用来修改指纹的次数是极其有限的,因为指纹永久不变而每个人通常只有十指;通过一枚成功复制的指纹,该用户的很多系统都可以成功攻破,因为这些系统使用的指纹不过是这1/10;使用了相似指纹进行认证的系统基本也可以确认是同一个用户,这为追踪用户行为提供了更多的便利。由此可见,由于指纹不具有可撤销性和无关联性,如果不能解决这一弊端,指纹在身份认证中的应用毫无疑问将是一场灾难。

指纹识别系统面临多种攻击威胁,图4列举了其中常见的几种。在这些攻击威胁中,重放攻击、盗取或篡改模板以及篡改匹配结果是常规加密系统面临的共同问题;而假指纹攻击、利用盗取的模板攻击系统是指纹有别于密码系统的攻击类型。虽然各指纹识别产品和方案供应商都在宣称系统存储的只是指纹特征而不是指纹图像,而且经过了加密,但是这种加密是可逆的,而且有多项研究表明通过指纹细节点特征可以恢复出原始指纹图像,而利用恢复的指纹图像攻击系统的成功率可以超过95%。因此,传统的加密手段对于保护指纹信息的安全性收效甚微。

在安全指纹识别的研究领域,安全的指纹识别技术主要包括两个方面:假指纹的检测和指纹模板的保护。假指纹检测主要研究如何抵御通过系统外部获取指纹信息并在输入端使用伪造指纹攻击系统的行为;而指纹模板保护主要研究在系统内部信息传输和存储过程中被盗取的指纹模板不会泄露原始指纹信息,以抵御被窃取模板对系统的攻击,同时为指纹模板增加可撤销和无关联的属性。假指纹检测技术的应用根据系统设计的不同需要增加一定的软硬件配置,也会增加相应的成本等。假设一个指纹识别的应用系统,我们希望它有非常高的安全等级,以至于愿意花费一个稍微昂贵一些的价钱并且可以容忍它不那么小巧的体积,那么集当前假指纹检测技术之大成,可以使这个系统很好地抵御各类假指纹的攻击。所以,假指纹从来不是指纹识别系统安全性的最大威胁。如前所述,不具可撤销性和无关联性才是指纹识别技术应用和发展过程中终将爆发的隐患,而指纹模板保护技术就是为解决这一问题而出现的。

指纹模板保护,简言之就是一种对指纹模板进行加密的技术,使加密后的模板具有不可逆、可撤销、无关联3种属性。它不同于传统密码学中加密的概念,因为密码学要求精确匹配,而指纹模板信息本质是模糊的。换言之,指纹由于采集过程中手指放置位置不同和发生形变等原因,不同次采集提取到的特征很难完全一致,经过不可逆加密后还会损失一定量的信息,在这种情况下如何保证加密模板可以匹配是指纹模板保护的重要研究内容之一。而之所以可以实现可撤销性和无关联性,是因为在加密过程中会添加随机信息。当加密模板存在泄露的可能时,只需重新采集指纹图像,系统会换一组随机信息生成新的加密模板,就像更改密码一样方便。由于随机信息的不同,新加密模板与之前的模板不可匹配,不同系统中的加密模板之间也不可匹配。由此可见,应用模板保护技术后指纹的安全性会有质的飞跃。不幸的是,受限于当前的技术水平,指纹模板保护在加密过程中造成的性能损失以及需要对原有系统进行的大量改造是目前很多应用系统难以接受的,所以还没有实现大范围的推广应用。但是从指纹应用的长期安全性考虑,指纹模板保护一定是未来指纹系统的必要组成部分。

3　智能手机中的指纹安全

智能手机对于指纹识别技术是一个稍微有些特别的应用场景:指纹识别在单机环境下进行,即手指的注册只在本手机有效;指纹信息不会存储在网上,也不会通过网络共享到其他的手机。在这样的环境下,不需要担心信息传输可能带来的指纹信息安全隐患,也无需担心服务器端或者云端泄露指纹信息的可能,而只需要考虑它在本机的存储是否安全。而事实上,目前的指纹手机大都是采取了安全区(secure chip)的策略,即指纹信息保存在特定的硬件区域,不提供对外的接口,除了特定的程序,理论上任何人用任何手段都无法存取该区域存储的内容。另一方面,同一个手机中用户很少,注册的手指数量通常不超过10个,因此在识别的过程中,误识的可能非常小。可以说,相比于大规模系统的在线认证,智能手机的终端认证更适合指纹识别技术发挥其优势。

针对假指纹检测,智能手机中普遍采用的电容式采集模块本身就可以对不具导电性的假指纹材质有拒识作用,也有部分厂商采用超声检测等技术抵御假指纹。但是受限于智能手机中可接受的芯片体积和硬件成本,假指纹抵御的问题在目前的手机中并没有得到完美解决。针对指纹模板保护,安全区不失为一个好的策略,但是有一个前提,即手机和指纹模块的提供商确实地履行承诺,不通过网络等途径收集和存

储用户的指纹。此外,安全区的安全性也并非绝对的,与芯片供应商的工艺品质和攻击者的技术水平都有一定的关系。整体来说,由于智能手机应用环境的特殊性,指纹手机的安全性较之传统指纹应用系统是有所提升的。受硬件等限制,假指纹检测技术和指纹模板保护技术都没有得到有效的应用,因此指纹的安全性问题并没有得到根本的解决,较之智能手机中的传统认证方式,其安全性也没有本质的提高。

智能手机也给指纹技术的应用带来了新的挑战:小面积。由于智能手机的轻薄化趋势,必然要求被集成的指纹采集模块极其小巧。一般应用于的指纹识别所采集的指纹图像面积通常在300×300像素以上,而智能手机集成的指纹芯片上,这个尺寸一般只有100×100像素左右。小面积带来的第一个难题是提取到的细节点数量少,甚至提取不到细节点,因此无法使用完全依赖细节点的匹配方法;另一个问题是两幅指纹之间的重叠面积小,甚至没有重叠部分,不能完成匹配。图5展示了指纹面积变小带来的重叠面积变化。如何在面积尽可能小的前提下保持指纹匹配的优秀性能是指纹在智能手机中应用的主要问题之一。

此外,目前的指纹手机产品的设计和使用中还可能存在以下两种安全隐患。

1)在注册指纹模板的时候,同一个手指需要采集10次左右,形成多个模板;但是由于小面积指纹的特殊性,这多个模板之间很难做同一性验证,即同一个账号下的指纹模板可能不是来源于同一个手指,这是不安全的。

2)在识别时,有些手机没有限制识别次数,即认证失败后可以无限制地再次认证。这增加了手机被假匹配和假指纹攻击的成功率。

以上两种问题不属于指纹技术本身的缺陷,而是手机产品设计过程中需要不断完善的方面。指纹技术和指纹手机发展至现阶段,相信仍有待解决的问题,但这并不妨碍指纹手机成为当前移动市场的主流产品。安全无绝对,指纹以其带来的便捷性赢得了消费者的青睐,相信其安全性随着技术的发展进步也会不断有突破。

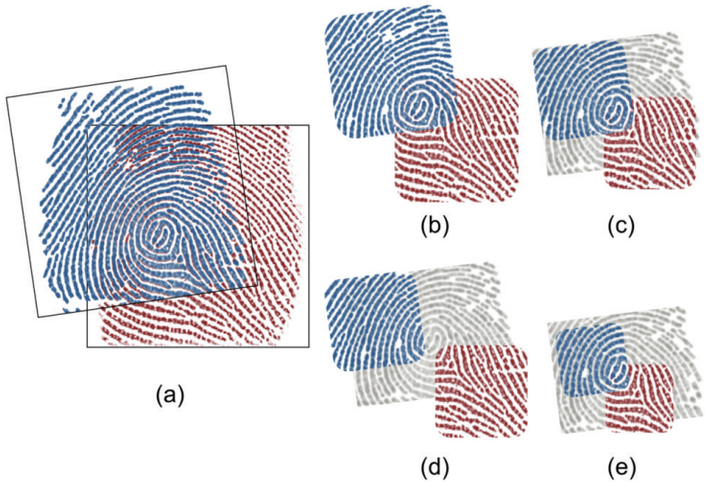

图5 小面积对指纹匹配带来的挑战:(a)中两幅指纹的尺寸约为300×300像素,传统指纹系统的图像尺寸通常在此之上,任意位置的两幅图像都有一定程度的重叠面积;(b)为(a)中两幅指纹裁剪后约为160×160像素的图像,是目前较为主流的指纹手机采集的指纹大小,重叠面积较难保证;(c)和(d)中指纹的尺寸约为120×120,不在同一个采集中心的指纹图像很难保证有效地重叠面积;(e)中指纹的尺寸约为88×88,是苹果公司Touch ID采集的指纹大小,也是目前已知的投入应用的采集面积最小的指纹芯片。灰色图案作为指纹图像相对位置的参考

4 指纹手机仍是发展趋势

尽管指纹手机没有带来信息安全的质的飞跃,但其带来的便捷性是毋庸置疑的。正因如此,仅仅两年时间指纹手机就占有了稳定的用户市场。在指纹手机广泛应用的刺激下,也在指纹安全争议的推动下,应用其他生物特征的智能手机产品也应运而生。2015年3月,日本富士通推出了通过虹膜解锁的概念手机;同月,马云在德国知名展会演示了手机"刷脸"支付的新技术;2016年1月,由中国科学院参与研发的中国首款量产虹膜识别手机问世。但是假生物特征的攻击威胁和生物特征模板保护是所有生物特征识别技术面临的共同问题,没有哪一种生物特征的安全性相对其他生物特征有本质上的突破。指纹、虹膜和人脸是生物特征识别的三大主力军。其中虹膜可达到的识别精度最高,抗假性相对最好,但是虹膜采集模块的成本很高,采集受光线和佩戴眼镜等因素的影响较大;而人脸由于可通过手机内置摄像头直接拍照采集,因此成本最低,但是人脸可达到的识别精度相对较低,抗假性也更差,人脸特征随着时间变化而发生的改变较为明显,而且对于双胞胎等长相相似的人群很难正确匹配。相比之下,指纹在唯一性、匹配精度、应用成本、用户接受度等多方面都有出色的表现,因此适用于更多的应用情景。

生物特征识别技术是身份认证的必然趋势。随着大众安全意识的提高、软硬件技术的不断发展,生物特征识别技术的应用会越来越广泛。智能手机已经成为个人信息、亲友关系、移动金融等各种安全隐私信息的集中存储地,每天解锁和使用频率可达几百次甚至上千次,因此身份认证的便捷性和安全性变得越来越重要。尽管目前的指纹手机还不够完美,但指纹有着密码等传统认证手段和其他生物特征技术无法超越的优势,因此在可预见的未来,指纹手机会越来越普遍,指纹识别也会成为智能手机中最常见的认证方式。

(责任编辑 刘志远)