

智能化的安卓手势密码取证关键技术

裘佳浩¹, 邱卫东¹, 王杨德¹, 查言¹, 谢宇明¹, 李岩²

(1. 上海交通大学网络空间安全学院, 上海 200240;

2. 司法鉴定科学研究院上海市司法鉴定专业技术服务平台司法部司法鉴定重点实验室, 上海 200063)

摘要: 在电子数据取证中, 如何对手机等移动设备进行屏幕解锁一直是亟待攻克的难题。将手势图形密码这种广泛应用于手机屏幕解锁以及软件访问授权的密码防护机制作为研究对象, 针对已有的手势图形密码还原技术存在的隐蔽性差、实用性低、非智能化、场景单一等弊端, 从肩膀冲浪、监控摄像、现场取证等场景中抽象出两个基本的威胁模型, 提出一种多场景下的手势图形密码侧信道攻击技术方法。该方法以监控摄像头或人工拍摄视频数据为基础, 采用智能视觉识别技术, 实时而动态地对视频中目标设备和解锁生物关键点进行识别、选择与跟踪; 随后采用空间映射和剪枝算法, 将离散的跟踪轨迹进行整合, 使用降噪算法对跟踪轨迹进行去冗余和优化, 定位出视频中绘制手势图形密码的关键转折点; 最后将精简的轨迹与手势图形密码的规则进行比对和匹配, 根据置信度对实际绘制的手势图形密码进行猜测和还原。实验结果表明, 在监控摄像场景中, 即设备屏幕可见场景下, 所提技术对手势图形密码的 10 次尝试成功率为 89%, 20 次尝试成功率为 99.3%; 在面对面拍摄场景中, 即屏幕和手部关键点被遮挡情况下, 10 次尝试成功率为 82%, 20 次尝试成功率为 89.3%; 拍摄水平距离的增加在监控摄像场景下对成功率的影响较明显, 但随着尝试次数的增加影响逐渐降低; 复杂密码在所提技术中无法起到更好的保护作用, 在 20 次尝试内, 复杂密码的破解成功率始终高于简单密码; 拍摄角度偏转在 5° 以内对破解成功率几乎没有影响。

关键词: 手势图形密码; 智能视觉识别; 电子数据取证; 侧信道攻击

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022005

Intellectualized forensic technique for Android pattern locks

QIU Jiahao¹, QIU Weidong¹, WANG Yangde¹, ZHA Yan¹, XIE Yuming¹, LI Yan²

1. School of Cyber Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

2. Key Laboratory of Forensic Science, Shanghai Forensic Service Platform, Ministry of Justice, Academy of Forensic Science, Shanghai 200063, China

Abstract: In the field of digital forensics, how to unlock mobile devices such as phones has always been an urgent problem to overcome. As a special kind of password, pattern lock is widely used in mobile phone screen unlock and

收稿日期: 2021-07-09; 修回日期: 2021-10-29

通信作者: 李岩, liyan@ssjfd.cn

基金项目: 科研院所公益研究专项 (GY2019G-2, GY2020G-6)

Foundation Item: Fundamental Research Funds for the Central Scientific Research Institutions (GY2019G-2, GY2020G-6)

引用格式: 裘佳浩, 邱卫东, 王杨德, 等. 智能化的安卓手势密码取证关键技术[J]. 网络与信息安全学报, 2022, 8(1): 118-127.

Citation Format: QIU J H, QIU W D, WANG Y D, et al. Intellectualized forensic technique for Android pattern locks[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 118-127.

software access authorization. Existing pattern lock cracking techniques have several non-negligible disadvantages, such as poor concealment, low practicability, non-intelligence and single application scenario. Two basic threat models were abstracted from shoulder surfing, surveillance camera, and real-time forensics, and a multi-scenario side channel attack on pattern locks was proposed. Based on the data of surveillance camera or manual video, intelligent vision recognition algorithms were adopted to identify, select and track the target device and biological key points in the video dynamically. Then, discrete tracking points were integrated by spatial mapping and pruning algorithm. The denoising algorithm was used to eliminate redundancy and optimize the trajectory. Through procedures above, the original trajectory was simplified into regular polylines defined by several key turning points. Finally, the simplified pattern was compared and matched with the rules of legal pattern locks to inference and retort its actual pattern. Possible candidates will be sorted in the output according to their confidences. Results show that in the surveillance camera scenario, where the device screen is always visible, the cracking success rate of our technique is 89% for 10 attempts and 99.3% for 20 attempts. In the face-to-face scenario, where the subject consciously blocks the screen and his drawing finger, the success rate was 82% after 10 attempts and 89.3% after 20 attempts. In the surveillance camera scenario, the increase of shooting horizontal distance can significantly decrease the cracking success rate. But this effect diminishes with the increase of the number of attempts. Results show that the cracking success rate of the complex password is always higher than that of the simple password during 20 attempts, which means a complex pattern lock cannot play a better protection role if the proposed technique is applied. Shooting angle deflection within 5° has little effect on the success rate of cracking.

Keywords: pattern lock, intelligent vision recognition, digital forensics, side channel attack

0 引言

随着移动互联网时代的到来和发展,手机如今已经是人人必备的互联网终端设备。由于其承载着大量个人数据以及用户隐私,以手机为代表的移动设备安全防护技术以及取证技术一直是安全领域的研究热点之一。在对手机等移动设备的取证过程中,如何对手机进行屏幕解锁是一个难题。本文希望找到一个更加快捷、隐蔽、智能的方法帮助解决这一问题。

手势图形密码是一种基于图形的密码。手势图形密码早期应用场景是安卓手机的屏幕解锁,后来扩展到软件应用内部的身份认证和访问授权。一般来说,手势图形密码是连接 3×3 网格中一系列点构成的一笔画图案。

研究表明,相对于 PIN 码或基于文本的密码,手势图形密码具有更加易于记住和回忆的特点^[1],因而其在移动设备上的使用范围较 PIN 码及文本密码更广。根据 2017 年的一项调查^[2],73% 的受访者在移动设备上选择使用手势图形密码进行屏幕解锁或者常见应用的访问授权,如 PayPal、支付宝、邮箱等。因此,如何对用手势图形密码保护的涉案

设备进行取证,是非常值得讨论和研究的课题。

近年来,研究者指出了一些手势图形密码潜在的安全威胁,提出并论证了一些破解手势图形密码的攻击方法的有效性,这些技术可以应用在对手机等涉案移动设备的取证中。常见的破解手势图形密码的技术通常是侧信道攻击,即通过解密时用户或者设备本身泄露出来的一些信息进行非侵入式地还原手势密码,如 Aviv 等^[3]提出的涂抹攻击、Zhang 等^[4]提出的无线信号攻击、Abdelrahman 等^[5]提出的热学攻击、Zhou 等^[6]提出的声学攻击等。但是大部分包括上述攻击在内的针对手势图形密码的还原方法在实际应用中面临着许多限制,存在着对攻击环境要求较高、实施攻击设备要求较高等问题。

2017 年,Ye 等提出了一种基于视频的手势图形密码破解算法^[2],攻击者在拍摄一段用户绘制手势图形密码的视频后,人工对视频进行剪辑、标注目标设备和指定绘制密码指尖,然后对指尖的轨迹进行跟踪,从而还原出手势图形密码。这种攻击方法的优势是不需要接触受害者的手机设备,拍摄过程隐蔽不会引起受害者的警觉而导致更换密码。在该研究中,作者定义了基于视频的

攻击场景,即基于摄像头视角的、关键部位可见场景。该工作严重依赖于指尖的捕捉和连续跟踪,一旦视线遮挡或者跟踪目标丢失就会导致攻击失败。除此之外,攻击过程中大量的人工干预是其难以在实际场景中应用的原因,包括视频剪辑、手动定位指尖、判断起始结束时间等。

为了探究手势图形密码存在的安全隐患,以及探讨如何将其作为电子取证中的一个突破点,本文分析并总结了多种在实际应用场景下针对手势图形密码的威胁模型。同时,结合人工智能领域前沿的计算机视觉算法,本文提出并实现了对手势图形密码更实用且更有效的破解和取证方法。通过捕捉手部其他关键点的运动轨迹,在更一般、更真实、更广泛的遮挡场景下,即无法捕获绘制手势图形密码指尖的情况下,也能实现对手势图形密码的破解。

1 相关工作

1.1 威胁场景

随着互联网的普及,手机等移动设备的使用场景越来越多,面临的攻击威胁也越来越多。在实际生活中,攻击威胁不仅来自手机内部各种恶意软件的非授权访问和数据窃取,同样来自手机外部环境中。手机等移动设备的安全性和隐私性面临着以下几个经典的威胁场景。

(1) 肩膀冲浪

肩膀冲浪攻击指的是在未经他人同意的情况下,观察他人手机等移动设备上的个人数据和隐私信息等行为^[7]。在这种场景下,观察者难以观察到实际有用的信息(文献[7]中收集的189个攻击样本,仅有13个样本包含PIN码或密码),并且容易引起被攻击者的警觉,因此被认为是低风险的^[2]。尽管如此,仍然有一些研究^[8-10]针对肩膀冲浪攻击提出了防御手段。

(2) 监控摄像

随着监控摄像在各种场合的广泛分布和清晰度的日益提升,其对个人隐私的威胁也在逐步增加。针对监控摄像和个人隐私之间的矛盾^[11-13],部分学者提出了一些解决方案^[14-15],但是监控摄像存在的威胁仍然不能忽视。

(3) 现场取证

现场取证行为通常是隐蔽的,指的是攻击者

在受害者不知情的情况下,通过设备对用户行为进行记录,进而分析获得敏感数据的行为。不同于肩膀冲浪容易引起察觉,这一类攻击通常有专业工具的辅助,并且能够在远距离的情况下实施攻击。前人的工作证明可以通过智能手表等可穿戴设备实现密码窃取等攻击^[16-18],可以在5 m甚至8 m的距离下通过视频取证的方式进行现场取证^[19]。

1.2 基于视频的密码破解与取证技术

近年来,计算机视觉算法的发展使针对手机等移动设备的视频取证技术得到进步,安全从业人员也提出了许多基于视频的破解移动设备身份认证机制的取证方法。

在文献[20-22]中,研究者提出了基于视频破解手机PIN码的方法,在此基础上,文献[23-25]将破解的密码从数字PIN码扩展到基于文本的密码。但是这些取证技术都是在成功捕获手机屏幕的基础上进行的,一旦拍摄视角受限,或者用户在键入密码时有意识遮挡屏幕,取证就容易失败。

与本文的研究十分相似的是Shukla等在文献[19]中提出的针对文本密码的破解技术。他们的方法可以在较远距离的情况下,不引人注目地拍摄一段5~10 s用户输入密码的视频片段,在不需要捕获手机屏幕的情况下破解用户文本密码。与Ye等在文献[2]中的研究对应,Shukla等对基于视频的攻击场景进行扩展,提出了关键部位遮挡情况下,面对面拍摄视频的攻击场景。

1.3 手势图形密码破解

在Android 6.0以前的版本中,系统会根据用户设置的密码类型生成对应的key文件,将手势图形密码按照点线顺序转为序号,计算SHA-1散列值并存储为gesture.key文件。取证人员可以采用两种方法破解或者绕过手势图形密码:使用root权限删除或者替换gesture.key、提前计算包含所有手势图形密码哈希值的彩虹表进行碰撞。在Android 6.0之后的版本中,Google引入了Gatekeeper等一系列安全机制,上述方法在新的系统中几乎很难生效。

研究者提出了从其他角度破解手势图形密码的思路。2010年,Aviv等^[3]尝试用手机屏幕上的油性残留物来破解手势图形密码。这种攻击方法需要在理想化的环境下进行,手机设备在解锁前

和解锁后必然都有其他手指活动的痕迹。2016年, Zhang等^[4]提出绘制手势图形密码期间无线信号的差异可以重建手势图形密码,但是需要访问目标设备连接的路由器并进行复杂配置才能攻击,而且受环境中其他移动物体的影响较大,很难真正在实际场景中应用。2017年, Abdelrahman等^[5]将热成像设备引入手势图形密码的破解中,取得了不错的效果。但是热成像需要专业的设备近距离拍摄用户解锁后的屏幕,成功率随着时间的推移下降。而他们的攻击对于有重叠线段的手势图形密码来说无计可施,成功率仅为16.67%。Zhou等^[6]发现声音信号也会受到手势图形密码绘制过程的影响,因此提出了一种声学攻击方法,但是这种方法甚至需要在手机上安装特定的软件获取扬声器和麦克风权限。

2017年, Ye等^[2]提出了基于视频的侧信道攻击方法,通过拍摄一段攻击者绘制手势图形密码的视频,成功从视频片段中还原出手势图形密码,这种方法使手势图形密码在公共环境下受到的攻击威胁大大增加。该方法是目前基于视频的手势图形密码还原的最佳方案,但是这种方法仍然存在缺陷,即需要捕捉手机屏幕和手指轨迹。

2 方法设计

2.1 概述

相较于前人的工作,本文提出的破解手势图形密码的方法有以下几点贡献。

(1) 本文综合了前人在基于视频的手势图形密码侧信道攻击方案中提出的两种攻击场景(Ye2017^[2]和 Shukla2019^[19]),首次在多场景上实现了手势图形密码的破解还原,丰富了针对移动设备手势图形密码的取证技术。

(2) 本文创新性地提出了一种更简洁、更有效的、基于跟踪轨迹的启发式手势密码还原算法,实现了从跟踪轨迹到最终手势图形密码的映射。

(3) 前人提出的攻击和取证方法大多需要人工干预,本文的取证方法通过目标检测算法YOLOv3识别设备出现与否,代替人为裁剪视频寻找攻击起点;使用人体姿态识别算法OpenPose自动输出手部关键点坐标,代替人工标注视频帧中的关键点;使用启发式手势密码还原算法代替人工判定或者暴力破解,从而实现整个破解流程的自动化。实验结果表明,通过自动化处理方式在两种攻击场景下的识别成功率均可达到89%以上,与人工干预下的识别效率持平。

本文提出的手势图形密码破解方法与其他文献中提出方法的特征对比如表1所示,该方法有4个关键步骤:视频拍摄、关键点检测与跟踪、轨迹生成与优化、候选手势生成。图1展示了整个方法的工作流程。

表1 手势图形密码攻击方法的特征对比
Table 1 Features comparison of different pattern lock attacks

攻击方法	隐蔽性	实用性	鲁棒性	遮挡场景	自动化
涂抹攻击 ^[3]	×	×	×	√	×
无线信号攻击 ^[4]	√	×	×	√	×
热成像攻击 ^[5]	×	√	√	×	×
声学攻击 ^[6]	√	×	×	√	√
视频攻击(Ye) ^[2]	√	√	√	×	×
本文方法	√	√	√	√	√

2.2 视频拍摄

对用户绘制手势图形密码的过程进行视频拍摄是整个方法的基础和起点。在视频拍摄过程中,

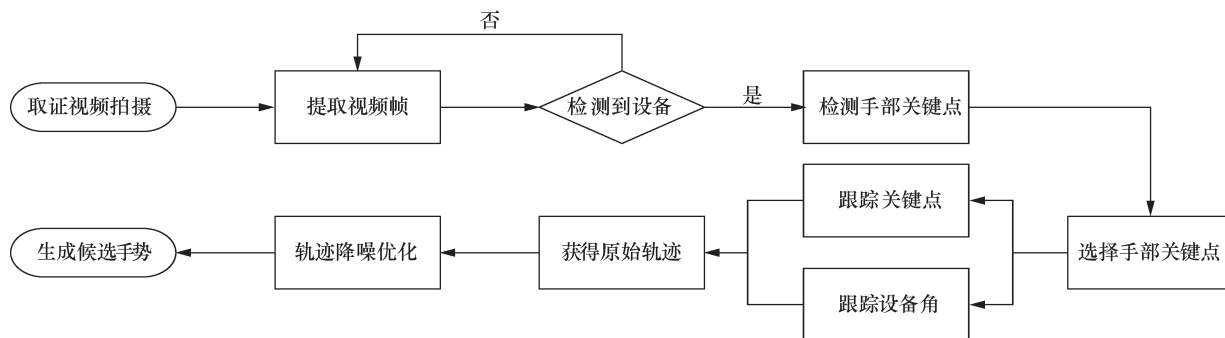


图1 方法工作流程
Figure 1 Method work flow

场景的选择和视角的选择是这一步的重点。

基于监控摄像头分布日益广泛^[26]和手机、平板等便携式设备拍摄能力日益增强的现状,本文提出的方案可以应用在两类典型的场景中。

场景 1 监控摄像

监控摄像头的数量呈逐年增长趋势,监控摄像的视角范围和清晰度也在逐渐提升。由于监控摄像头广泛存在,被摄像者不会感到特别警惕。在涉及案件调查时,执法人员在取证过程中可以调取各类监控摄像的数据。在实际场景中,监控摄像布置位置离地约 3 m,可以捕捉到手机屏幕和手指指尖。

场景 2 面对面拍摄

与场景 1 最大的区别在于,拍摄者与被拍摄者面对面,视线南向手机背部,无法直接捕捉屏幕显示内容和正在绘制手势图形密码的指尖。

2.3 关键点检测与跟踪

采集到合适的视频片段后,系统会自动选取合适的关键点进行跟踪,以还原出形变最少、噪声最小的轨迹。

2.3.1 关键点检测

目标在视频中的位置通常是随机的,每个人手持手机的高度不统一,人在监控摄像视角下站立的位置也不固定,因此从视频中检测并定位手部关键点是一个难题。本文结合人工智能领域的相关算法,通过手机检测、感兴趣区域扩展、手部关键点检测 3 个模块实现手部关键点的检测。为了防止视频帧中非绘制密码手的干扰,本文引入目标检测算法 YOLOv3^[27],训练神经网络使其能够识别并定位图像中手机的所在区域。接下来,算法对手机区域按比例适当向两边扩展放大,如式(1)~式(4),在扩展区域内捕获到的手就是绘制密码手。裁剪扩展后的手机所在区域图像,输入开源人体姿态识别算法 OpenPose^[28]中,该模型能够从图像中输出 21 个手部关键点的位置,如图 2 所示。

$$x'_0 = \max \{x_0(1 - \alpha), 0\} \quad (1)$$

$$y'_0 = \max \{y_0(1 - \alpha), 0\} \quad (2)$$

$$x'_1 = \min \{x_0(1 + \alpha), \text{ImageWidth}\} \quad (3)$$

$$y'_1 = \min \{y_1(1 + \alpha), \text{ImageHeight}\} \quad (4)$$



图 2 21 个手部关键点示意
Figure 2 21 key points of a hand

2.3.2 关键点选择

在场景 1 及以场景 1 为代表的威胁模型中,手机屏幕与绘制手势图形密码的指尖始终都是可见的。因此,在场景 1 中,算法只需要选择指尖对应的关键点序号进行跟踪即可。对于场景 2,当指尖在视频取证过程中无法被捕获时,算法选择运动轨迹和指尖同步的其他手部关键点进行跟踪。在所有手部关键点中,部分关键点在绘制手势图形密码过程中,其运动状态和指尖几乎是同步的,基于此算法选择其他可见的手部关键点进行跟踪。

2.3.3 关键点跟踪

选定需要跟踪的关键点后,本文使用 CSRT^[29]来跟踪关键点的移动,并对手机角进行同步跟踪用以校准。CSRT 适合短期跟踪场景,其跟踪精度相较于其他跟踪算法更高^[29],并且跟踪过程自动化,不需要人为干预。

2.4 轨迹生成与优化

跟踪算法能够输出目标在每一帧中的位置,将关键点的坐标通过当前帧中手机角的坐标进行校准后,逐帧绘制出来即原始轨迹。

图 3 是跟踪算法得到的原始轨迹,从图中可以看出,原始轨迹通常是包含噪声的,这些噪声可能来自于绘制密码时的冗余动作、拍摄者的抖动以及跟踪算法本身精度上的缺陷。从原始轨迹中直接得到手势图形密码是困难的,为此需要对轨迹进行优化。

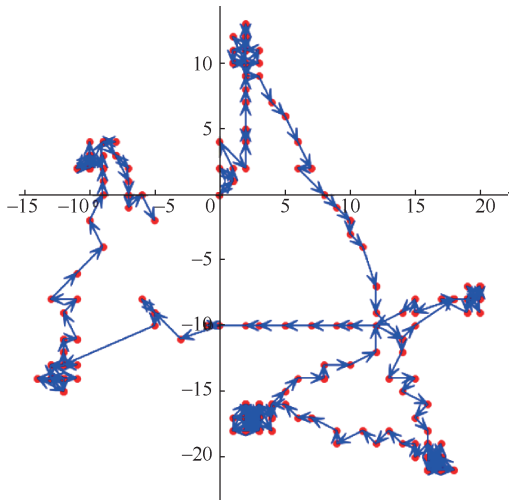


图 3 原始跟踪轨迹
Figure 3 Original trajectory from tracking

为了优化轨迹、去除噪声，本文使用 Ramer-Douglas-Peucker(RDP)算法^[30]对轨迹进行迭代拟合。RDP 算法实际上是用于减少表达一条曲线所需要用到的点的个数，并且尽可能保留曲线的原始形状。跟踪算法输出的原始轨迹实际上是由 $\text{Num}_{\text{Frame}}$ 个点构成的折线，通过将轨迹简化到由 4~9 个关键点组成的点集表达的折线，可以将其映射到手势图形密码的九宫格中。

2.5 候选手势生成

如何将优化后的关键点轨迹映射成可能的手势图形密码是本节需要解决的问题。

如图 4 所示，在所有可能的手势图形密码中，线段长度和转折点角度只能从固定的集合中取值。将图 4 中同一行列的相邻两点之间的距离定义为 1，长度可能取值集合如式(5)所示，角度集合如式(6)所示。

$$\text{DistanceSet} = \{1, \sqrt{2}, 2, \sqrt{5}, 2\sqrt{2}\} \quad (5)$$

$$\text{AngleSet} = \{18^\circ, 27^\circ, 37^\circ, 45^\circ, 53^\circ, 63^\circ, 72^\circ, 90^\circ, 117^\circ, 135^\circ\} \quad (6)$$

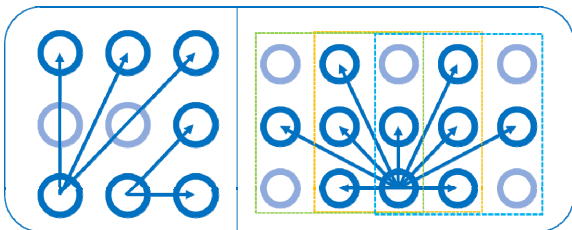


图 4 手势图形密码分段长度与转折点角度示意
Figure 4 All possible segment lengths and turning angles of pattern locks

对于角度和长度这两个轨迹特征，本文做了一系列数学工作来验证它们对于映射关系的相关性，以及两个特征之间的相关性。引入 Kendall^[31]和 Spearman^[32]两种相关系数 (R 和 ρ)，计算方法如式(7)和式(8)所示。

$$R = \frac{\sum_{i < j} \text{sgn}(x_i - x_j) \text{sgn}(y_i - y_j)}{\binom{n}{2}} \quad (7)$$

$$\rho = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}} \quad (8)$$

计算实际轨迹与标准手势图形密码指尖角度特征的相关系数、长度特征的相关系数，以及标准手势图形密码中角度与长度两个特征之间的相关系数，结果如表 2 所示。实验证明：① 两个变量都可以用作映射的有效特征；② 角度特征对于映射的相关性较长度更高；③ 两个特征之间的相关度很低，不能相互替换。

表 2 相关系数计算结果
Table 2 Results of Kendall and Spearman correlation coefficients

影响因素	Kendall	Spearman
角度	0.905 2	0.978 6
长度	0.668 6	0.810 9
角度&长度	-0.059 7	-0.086 8

因为拍摄角度以及跟踪位置的关系，优化后的轨迹实际上会产生不可避免的旋转或形变。直接将轨迹和标准的手势图形密码库对比准确率不高，因此本文把优化轨迹中的每 3 个点看成一个整体并将其向量化。同理，标准的手势图形密码库也可以拆分成 3 个点一组的标准向量库。对于连续的 3 个点 $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$ ，向量化的步骤如式(9)~式(11)。

$$\vec{a} = (x_2 - x_1, y_2 - y_1) \quad (9)$$

$$\vec{b} = (x_3 - x_2, y_3 - y_2) \quad (10)$$

$$\vec{c} = (\|\vec{a}\|, \|\vec{b}\|) \quad (11)$$

对于轨迹中的一组向量 $(\vec{a}, \vec{b}, \vec{c})$ ，与标准向量库中的标准向量 $(\vec{u}, \vec{v}, \vec{w})$ 进行比较，通过计算余弦相似度比较两对向量的相似性，计算公式为式(12)，其中 θ 是可调整的加权因子。一个轨迹可能由多

组向量构成,因此需要对各组向量计算的余弦相似度相乘,再将结果降序排列,得到最终的候选手势图形密码。

$$S = \frac{1}{2} \left(\frac{\vec{u} \cdot \vec{a}}{\|\vec{u}\| \cdot \|\vec{a}\|} + \frac{\vec{v} \cdot \vec{b}}{\|\vec{v}\| \cdot \|\vec{b}\|} \right) \times \theta + \frac{\vec{w} \cdot \vec{c}}{\|\vec{w}\| \cdot \|\vec{c}\|} \times (1 - \theta) \quad (12)$$

3 实验分析

3.1 实验设置

3.1.1 手势图形密码选择

本文从所有可能的 389 112 个手势图形密码中随机选取 150 个手势图形密码作为测试的样本,并使用文献[33]中提出的计算手势图形密码复杂度的方法来衡量密码强度 C_{SP} , 计算式如式(13)所示。

$$C_{SP} = S_p \cdot \lg L_p + I_p + O_p \quad (13)$$

对于手势图形密码 P , S_p 是连接点的个数, L_p 是手势图形密码长度, I_p 是交叉点的数量, O_p 是重叠线段的数量。根据式(13), 密码强度与上述变量都呈正相关, 并且所有合法手势图形密码中, 强度最高为 46.8。本文实验选用的 150 个手势图形密码强度分布如图 5 所示。

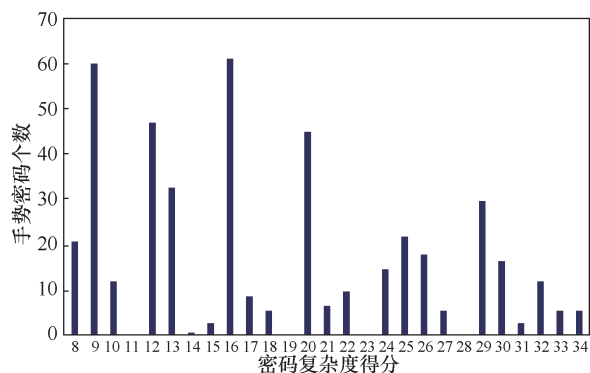


图5 样本中手势图形密码强度分布
Figure 5 Distribution of pattern complexity score

3.1.2 取证场景模拟

2.2 节中声明了应用本文取证技术的两个场景, 实验时进行如下环境模拟。

1) 监控摄像: 将录像设备固定在 2 m 高的三脚架上模拟监控摄像, 志愿者绘制手势图形密码时, 与录像设备的水平距离设置为 1 m、2 m 和 3 m。志愿者将手机放置在桌子上进行实验, 拍摄角度

为前方和左侧。

2) 面对面拍摄: 两名志愿者面对面进行实验, 一名志愿者手持拍摄设备, 另一名志愿者手持手机, 两者间隔的水平距离分别是 1 m、2 m 和 3 m, 两个设备位于同一高度。

3.2 实验效果

整体的实验效果如图 6 所示。通常情况下, 手势图形密码有 3~5 次初始尝试机会, 此后每次尝试需要等待一定的时间, 等待时间随着尝试次数的增加而增加。从 OPPO Reno 2 为例, 5 次尝试之后需要等待 30 s, 10 次尝试后需要等待 5 min, 具体数据会随系统和软件而异, 本文选取 20 次作为最大尝试次数。

在场景 1 的模拟实验中拍摄了 300 个视频样本, 包含 150 种手势图形密码。在所有样本中, 10 次尝试成功率为 89%, 20 次尝试成功率为 99.3%。

在场景 2 的模拟实验中拍摄了 150 个视频样本, 包含 150 种手势图形密码。本文选择小拇指根部作为跟踪目标, 即图 2 中的第 17 号关键点。在所有样本中, 10 次尝试成功率为 82%, 20 次成功率为 89.3%。

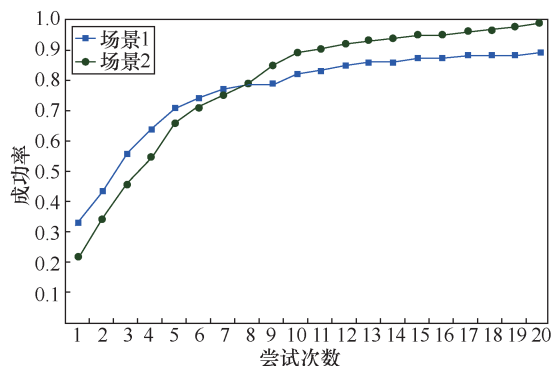


图6 不同尝试次数下的破解成功率
Figure 6 Success rate of cracking pattern locks with different number of attempts

由于 Ye 等在文献[2]中的工作不支持在无法捕捉手机屏幕和绘制密码指尖的情况下破解手势图形密码, 并且文献[2]中所用到的算法与数据集并没有公开, 因此本文的实验结果无法与其进行全面对比。在场景 1 中, Ye 等在文献[2]中所做的工作为目前在相同场景下最好的手势图形密码破解算法, 在他们的数据集中, 手势图形密码的破解成功率超过 95%; 本文提出的取证技术能够在

无须人工干预的前提下, 对于手势图形密码的 20 次破解成功率达到 99.3%, 与文献[2]中的实验结果持平。对于场景 2, Ye 等的方案不能实现手势图形密码的破解, 无法进行对比。

3.3 水平距离的影响

水平距离对成功率的影响如图 7 和图 8 所示。在两个场景中, 垂直距离都是固定不变的。场景 1 中垂直距离为 2 m, 场景 2 中垂直距离为 0, 主要变化的是水平距离。

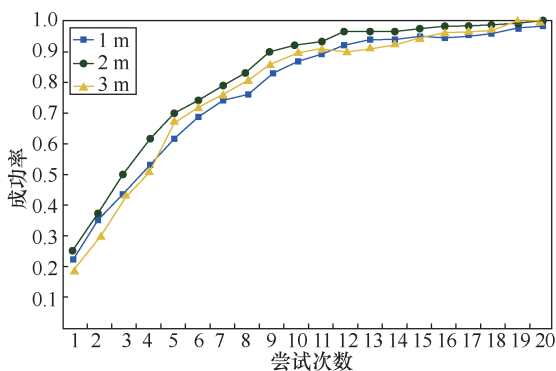


图 7 场景 1 水平距离对破解成功率的影响
Figure 7 Impact of filming distance on cracking in scenario 1

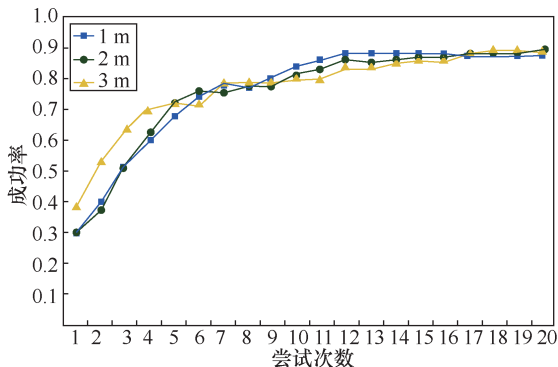


图 8 场景 2 水平距离对破解成功率的影响
Figure 8 Impact of filming distance on cracking in scenario 2

在场景 1 中, 破解成功率随距离增加降低。当水平距离为 1 m 时, 5 次尝试可以破解 70% 的手势图形密码, 并且在所有尝试次数中成功率始终高于 2 m 和 3 m。20 次尝试后, 3 个距离的成功率相对接近。

在场景 2 中, 3 m 的 5 次以内尝试成功率明显高于 1 m 和 2 m 两个距离, 在 5 次及以上尝试次数中, 3 m 的成功率不如 1 m 和 2 m。总体来说, 场景 2 在合适距离内, 成功率受距离变化的影响不明显。

3.4 密码强度的影响

3.1 节中讨论了密码强度公式, 本文按照得分将手势图形密码分为简单、中等和复杂 3 类。密码强度对破解成功率的影响如图 9 所示。

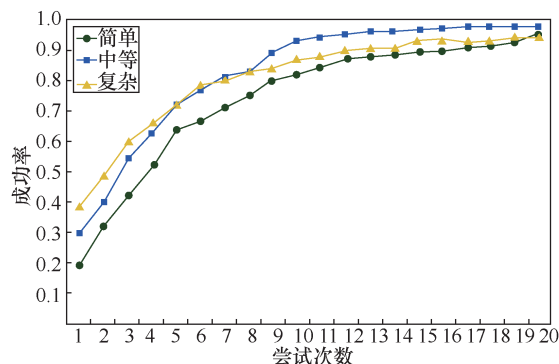


图 9 密码强度对破解成功率的影响
Figure 9 Impact of pattern complexity on cracking

一般来说, 密码越复杂, 其安全性越高, 攻击能力越强。但是实验结果证明, 密码强度对于本文的破解方法影响不大, 即复杂密码并不能有效抵抗本文提出的方法, 甚至在所有尝试中, 复杂密码的破解成功率一直高于简单密码。

分析其原因, 本文提出的方法进行轨迹到手势图形密码的映射时, 将每一个手势图形密码进行 3 个点为一组的拆分, 因此长度、连接点的个数对于本文的取证方法影响不大。除此之外, 绘制复杂手势图形密码时用户倾向于更加细致, 动作变形更少, 并且视频中泄露的手势图形密码信息会更多, 因此复杂密码破解成功率比简单密码有少量提升, 这与 Ye 等在文献[2]中的研究结果一致。

3.5 拍摄角度的影响

在场景 1 中, 选取了前方和左侧两个拍摄角度, 并且让志愿者坐在左、中、右 3 个不同的位置, 即共计 6 种拍摄角度。算法通过检测人脸方向来自动判断监控摄像和手机设备之间的方位关系, 并对轨迹进行对应方位的旋转处理。实验结果表明, 监控摄像在左侧的破解成功率更高, 可能是一般用户习惯用右手绘制手势图形密码, 左侧视角拍摄遮挡更少造成的。

在场景 2 中, 由于手机是被拍摄者手持的状态, 一般无法精确地以垂直于手机屏幕的视角拍摄。实验发现, 当拍摄路径与手机屏幕的垂面夹角度数在 5°以内时, 对成功率几乎没有影响。

4 结束语

本文提出了一种智能化的基于视频的多场景手势图形密码分析与还原技术方法,在特定场景下能够对手势图形密码的有效破解。虽然前人提出了手势图形密码可以被一些侧信道方法破解,但是本文的实验证明,在合适的威胁模型下,手势图形密码这种身份认证机制被破解的概率会大大增加。有经验的取证人员可以用本文方法,在较短时间内实现手势图形密码的破解。

本文提出的方法仍然存在一定的局限性。一方面,受拍摄条件的限制,监控摄像的清晰度并不总能为本文方法提供有效支持。另一方面,个人习惯会对破解成功率造成影响,如在输入手势图形密码时仅移动手指而不是整个手部,将会显著降低场景 2 中的破解成功率。

此外,本文的思想可以扩展到其他应用场景,如扩展到对 PIN 码、手写输入、键盘触碰等移动设备的其他输入内容的破解和猜测上,这对相关取证技术的研究提供了新的方向和思路。

参考文献:

- [1] WEISS R, DE LUCA A. PassShapes: utilizing stroke based authentication to increase password memorability[C]//Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges. 2008: 383-392.
- [2] YE G X, TANG Z Y, FANG D Y, et al. Cracking android pattern lock in five attempts[C]//Proceedings 2017 Network and Distributed System Security Symposium. 2017.
- [3] AVIV A J, GIBSON K L, MOSSOP E, et al. Smudge attacks on smartphone touch screens[J]. Woot, 2010, 10: 1-7.
- [4] ZHANG J, ZHENG X L, TANG Z Y, et al. Privacy leakage in mobile sensing: your unlock passwords can be leaked through wireless hotspot functionality[J]. Mobile Information Systems, 2016, (2016): 8793025.
- [5] ABDELRAHMAN Y, KHAMIS M, SCHNEEGASS S, et al. Stay cool! understanding thermal attacks on mobile-based user authentication[C]//Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. 2017: 3751-3763.
- [6] ZHOU M, WANG Q, YANG J X, et al. PatternListener: cracking android pattern lock using acoustic signals[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 1775-1787.
- [7] EIBAND M, KHAMIS M, VON ZEISCHWITZ E, et al. Understanding shoulder surfing in the wild: stories from users and observers[C]//Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. 2017: 4254-4265.
- [8] WIEDENBECK S, WATERS J, SOBRADO L, et al. Design and evaluation of a shoulder-surfing resistant graphical password scheme[C]//Proceedings of the Working Conference on Advanced Visual Interfaces. 2006: 177-184.
- [9] KUMAR M, GARFINKEL T, BONEH D, et al. Reducing shoulder-surfing by using gaze-based password entry[C]//Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07. 2007: 13-19.
- [10] ROTH V, RICHTER K, FREIDINGER R. A PIN-entry method resilient against shoulder surfing[C]//Proceedings of the 11th ACM Conference on Computer and Communications Security. 2004: 236-245.
- [11] WINKLER T, RINNER B. User-centric privacy awareness in video surveillance[J]. Multimedia Systems, 2012, 18(2): 99-121.
- [12] GELBORD B, ROELOFSEN G. New surveillance techniques raise privacy concerns[J]. Communications of the ACM, 2002, 45(11): 23-24.
- [13] WINKLER T, RINNER B. Security and privacy protection in visual sensor networks: a survey[J]. ACM Computing Surveys, 2014, 47(1): 2.
- [14] SCHIFF J, MEINGAST M, MULLIGAN D K, et al. Respectful cameras: detecting visual markers in real-time to address privacy concerns[M]//Protecting Privacy in Video Surveillance. 2009: 65-89.
- [15] KORSHUNOV P, EBRAHIMI T. Using warping for privacy protection in video surveillance[C]//Proceedings of 2013 18th International Conference on Digital Signal Processing (DSP). 2013: 1-6.
- [16] GUERAR M, MIGLIARDI M, PALMIERI F, et al. Securing PIN-based authentication in smartwatches with just two gestures[J]. Concurrency and Computation: Practice and Experience, 2020, 32(18): e5549.
- [17] LU C X, DU B W, WEN H K, et al. Snoopy[J]. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2018, 1(4): 1-29.
- [18] WANG C, GUO X N, CHEN Y Y, et al. Personal PIN leakage from wearable devices[J]. IEEE Transactions on Mobile Computing, 2018, 17(3): 646-660.
- [19] SHUKLA D, PHOHA V V. Stealing passwords by observing hands movement[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(12): 3086-3101.
- [20] SHUKLA D, KUMAR R, SERWADDA A, et al. Beware, your hands reveal your secrets![C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 904-917.
- [21] CHEN T, FARCASIN M, CHAN-TIN E. Smartphone passcode prediction[J]. IET Information Security, 2018, 12(5): 431-437.
- [22] BALAGANI K S, CONTI M, GASTI P, et al. SILK-TV: secret information leakage from keystroke timing videos[M]//Computer Security. Cham: Springer International Publishing, 2018: 263-280.
- [23] BALAGANI K, CARDAIOLI M, CONTI M, et al. PILOT: password and PIN information leakage from obfuscated typing vid-

- eos[J]. Journal of Computer Security, 2019, 27(4): 405-425.
- [24] XU Y, HEINLY J, WHITE A M, et al. Seeing double: reconstructing obscured typed input from repeated compromising reflections[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. 2013: 1063-1074.
- [25] YUE Q G, LING Z, FU X W, et al. Blind recognition of touched keys on mobile devices[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 1403-1414.
- [26] Barrett D. One surveillance camera for every 11 people in Britain, says CCTV survey[J]. The Telegraph, 2013, 10.
- [27] REDMON J, FARHADI A. YOLOv3: an incremental improvement[J]. arXiv preprint arXiv:1804.02767, 2018.
- [28] SIMON T, JOO H, MATTHEWS I, et al. Hand keypoint detection in single images using multiview bootstrapping[C]//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. 2017: 4645-4653.
- [29] LUKEŽIĆ A, VOJÍR T, ZAJC L C, et al. Discriminative correlation filter with channel and spatial reliability[C]//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. 2017: 4847-4856.
- [30] DOUGLAS D H, PEUCKER T K. Algorithms for the reduction of the number of points required to represent a digitized line or its caricature[J]. Cartographica: the International Journal for Geographic Information and Geovisualization, 1973, 10(2): 112-122.
- [31] KENDALL M G. Rank correlation methods[J]. Biometrika, 1957, 44(1/2): 298.
- [32] SPEARMAN C. General intelligence, objectively determined and measured[J]. The American Journal of Psychology, 1904, 15(2): 201-292.
- [33] SUN C, WANG Y, ZHENG J. Dissecting pattern unlock: the effect of pattern strength meter on pattern selection[J]. Journal of Information Security and Applications, 2014, 19(4/5): 308-320.

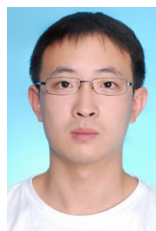
[作者简介]



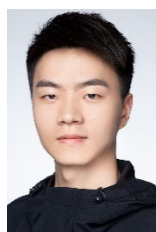
裘佳浩（1999-），男，浙江杭州人，上海交通大学硕士生，主要研究方向为计算机取证、密码安全。



邱卫东（1973-），男，江西修水人，上海交通大学教授、博士生导师，主要研究方向为计算机取证、密码分析、人工智能安全、大数据隐私保护。



王杨德（1987-），男，辽宁沈阳人，上海交通大学博士生，主要研究方向为计算机取证、密码分析。



查言（2000-），男，安徽安庆人，上海交通大学硕士生，主要研究方向为人工智能、密码安全。



谢宇明（1996-），男，湖北武汉人，上海交通大学硕士生，主要研究方向为人工智能、密码安全。



李岩（1985-），男，湖北老河口人，硕士，司法鉴定科学研究院高级工程师，主要研究方向为电子数据、声像资料鉴定技术及标准化。