视线交互的图像密码认证系统

淳新益[1] 栗战恒[1] 郑秀娟[1*] 刘华茜[1] 张 昀[2] 刘 凯[1]

[1](四川大学电气工程学院 四川 成都 610065)

[2](西安交通大学电子与信息工程学院 陕西 西安 710049)

摘 要 针对图像认证系统易受到窥探攻击的问题,提出一种基于视线交互的图像认证系统。系统中,眼动仪记录用户的眼球运动并将其作为输入控制信号,用以生成系统的用户名和密码,进而抵御窥探攻击。用户测试研究验证系统的可用性和有效性,实验的平均成功率为 85.71%;随着用户熟悉程度的提高,用户认证成功率逐渐升高。

关键词 视线跟踪 图像认证系统 视线交互

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.09.046

A GRAPHICAL PASSWORD AUTHENTICATION SYSTEM BASED ON GAZE INTERACTION

Chun Xinyi[1] Li Zhanheng[1] Zheng Xiujuan[1*] Liu Huaqian[1] Zhang Yun[2] Liu Kai[1]

[1](*College of Electrical Engineering*, *Sichuan University*, *Chengdu 610065*, *Sichuan*, *China*)

[2](*School of Electronic and Information Engineering*, *Xi'an Jiaotong University*, *Xi'an 710049*, *Shaanxi*, *China*)

Abstract Aiming at the problem that graphical authentication systems are vulnerable to shoulder-surfing, this paper proposes a graphical authentication system based on gaze interaction. In this authentication system, the eye-tracker recorded the eye movement of the user and used it as the input control signal to generate the user name and password of the system. The system can resist observation attack. The usability and effectiveness of the system are verified by user test research, and the average success rate of the experiment is 85.71%. With the improvement of user familiarity, the success rate of user authentication gradually increases.

Keywords Eye tracking Graphical authentication system Gaze interaction

0 引 言

用户是安全系统的薄弱环节,许多安全问题产生于人机交互环节。例如,基于生物特征识别的系统 BBID(Biometrics-based Identification)是基于用户自身属性,不会丢失和遗忘,但是易被记录或盗取,其存在的一个严重问题是克隆。为了应对人们对复杂文本密码的记忆难题,近几年有人开始探索图像密码的认证方案[1]。这种方案在解决密码的记忆问题方面表现良好,但是却无法有效地抵御窥探攻击。眼睛的运动直接体现了用户视线的改变,与人们的关注目标以及任务意图有着非常密切的联系,是一种高效、快捷的交互方式。眼动数据由眼动系统收集,眼睛特征难以被人类观察者直接提取。因此,眼动对窥探攻击有高抵抗性,完全适合在认证系统中使用。一些研究人员将图像系统和眼球运动的优势结合在一起,尝试开发基于眼动的图形认证系统[2]。配备视线跟踪技术的图形密码系统不仅可以解决安全问题,而且可以提升用户体验。Maeder 等[3]和 Hoanca 等[4]都提出了基于用户注视的图形认证系统。此外,Dunphy 等[5]在 Passfaces 上配备了视线跟踪设备并将其实施到 ATM 系统上。

收稿日期:2019-07-15。四川省科技计划项目(2019YFS0140)。**淳新益**,硕士生,主研领域:视线跟踪技术,数据分析。**栗战恒**,硕士生。**郑秀娟**,副教授。**刘华茜**,硕士生。**张昀**,副研究员。**刘凯**,教授。

本文提出一种基于视线交互的图像密码认证系统。利用眼动的优点并与基于识别的图像身份认证系统相结合,系统基于注视的交互进行设计,并通过用户测试对该系统的可用性和有效性进行验证。

1　系统设计

本文提出的图像密码认证系统中使用图像组合作为用户名和密码,并以眼动仪代替鼠标和键盘作为输入设备。本研究有如下假设:1) 用户在背景和尺寸不同的图像上有不同的浏览时间(数据密度、展示介质及压力在视觉搜索性能上有不同的贡献[6],这里只考虑背景和尺寸的影响);2) 用户在感兴趣区域 AOI (Area of Interest)花费的时间多于其他区域。

1.1　眼动输入方式

基于注视的交互和基于扫视的交互是使用视线跟踪技术进行人机交互的两种可用模式,最常用的是基于注视的人机交互[7]。在基于注视的交互中,一个很重要的问题是触发方式的选择,一般有基于眨眼和基于驻留两种方式。在过去的研究中,基于注视驻留的方法被认为是最佳的触发方式。Hansen 等[8]研究后发现:基于注视驻留的视线交互方法能够建立一个比鼠标点击速度更快的眼控接口。本文采用基于注视驻留的交互方式设计图像认证系统。

1.2　系统图像尺寸与背景

用实验测试不同背景、尺寸图像组合对用户视觉搜索性能的影响,图像背景分别被设置为 Round、Square、None 3 种,尺寸被设置为 tiny(95 ×95 pixels)、small(113 ×113 pixels)、medium(150 ×150 pixels)和 large(188 ×188 pixels)4 种,共组成 12 种组合。每种图像组合包含 9 个相同尺寸图像,图 1 是尺寸为 large 时的三种组合。

图 1　尺寸为 large 时的三种图像组合

实验共招募 16 名受试者用于验证假设 1,通过实验选择适合系统的最佳图像尺寸和图像背景。实验前,向受试者介绍整个实验,以确保他们熟悉实验流程。实验开始时首先进行 9 点视线标定,大约用时 1 min。之后,显示器呈现以上 12 种图像组合,每种组合随机出现 5 次,每次呈现图像位置随机分布。受试者浏览每个图像组合,并用鼠标单击他们最感兴趣的一幅,之后呈现下一图像组合,直至图像组合呈现完毕(12 ×5 共 60 次)。实验过程中使用眼动仪获取用户的视线位置,同时记录每个图像组合中用户所选中的图像,即用户最感兴趣的图像 IOI(Image of Interest)。

对所有眼动数据进行统计分析,排除一个采样率过低受试者的实验数据,表 1 为其他 15 个受试者的实验数据统计。其中:Style 是图像组合样式;SelectDur 是用户视线在 IOI 上的平均停留时间;BrowsDur 是用户视线在非 IOI 图像上的最大停留时间的平均值;Acc 是注视正确率,指视线估计点所在图像与鼠标点击图像一致的比例。

表 1　每种图像组合的统计结果

Style 背景_尺寸	SelectDur/s 均值(标准差)	BrowsDur/s 均值(标准差)	Acc/%
Square_tiny	0.867(0.529)	0.860(0.634)	77.33
Square_small	1.005(0.769)	0.967(0.837)	94.67
Square_medium	1.074(0.619)	0.813(0.829)	97.33
Square_large	0.911(0.631)	0.685(0.550)	97.33
Round_tiny	1.219(0.816)	1.694(1.016)	89.33
Round_small	1.479(1.328)	1.946(1.100)	97.33
Round_medium	1.271(0.761)	1.656(0.864)	100.00
Round_large	1.591(1.263)	2.136(1.165)	98.67
None_tiny	0.914(0.430)	0.709(0.563)	90.67
None_small	1.128(0.889)	1.137(0.980)	93.33
None_medium	1.302(0.906)	1.057(1.053)	96.00
None_large	1.106(0.793)	0.89(1.049)	98.67

使用双因素可重复方差分析(Two-wayANOVA)分析实验数据,如图 2(a)所示,图像尺寸相同时随着图像背景从 Round 到 None 再到 Square,受试者在 IOI 上的视线停留时间显著减少($p < 0.001$,p 为双因素可重复方差分析中的一个重要参数);同样尺寸下当图像背景为 Square 时,受试者搜索 IOI 所需的时间最短。如图 2(b)所示,当图像背景为 IOI 时,随图像尺寸增加受试者在 IOI 上的视线停留时间先增大后减小($p < 0.05$)。当图像尺寸为 tiny 与 large 时,受试者搜索 IOI 所需的时间较短。由表 1 结果可得,当图像尺寸很小时注视正确率一般低于 90%,这可以由用户的眼睛生理机制及眼动数据准确性来解释。

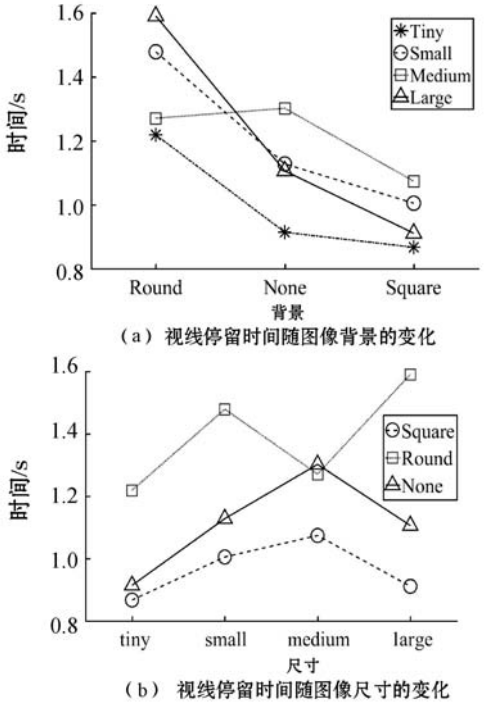


图 2 不同图像组合下 IOI 上注视时间的变化

实践中图像认证系统的用户界面大小一定,如果密码图像的尺寸无限大,系统将包含过少的图像从而容易受到密码猜测攻击。因此,综合以上因素我们选择 Square_large 作为最佳图像组合,并设置 0.911 s 作为用户选中目标图像的时间阈值(根据表 1),设置 0.676 s作为“清除”、“保存”等功能键的时间阈值(数据通过类似的实验获得)。

1.3 系统实施

图像认证系统示意图如图 3 所示,Tobii EyeX 固定在 23 英寸显示器(分辨率为 1 920 ×1 080 pixels)底部,受试者坐在离屏幕约 65 cm 的位置,保持坐姿舒适。系统中的图像作为生成用户名和密码的个人识别图像集 PIIs(Personal Identification Images),基于用户识别进行身份认证,系统包括注册和登录两个阶段。

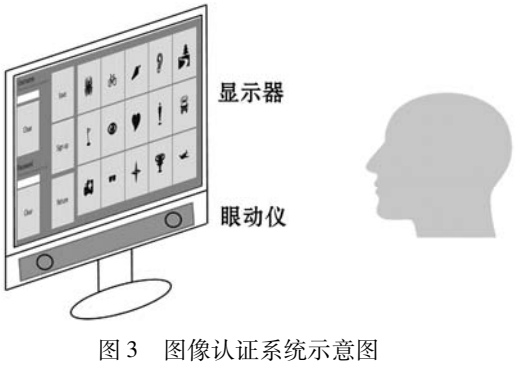


图 3 图像认证系统示意图

图 4 为系统注册界面示意图(登录界面与注册界面类似),用户界面左侧为功能按键,右侧以 3 ×5 的网格显示 15 幅图像作为 PIIs,以避免图像界面过大并降低窥探攻击的风险,系统中密码图像和功能键依据之前的实验结果进行设置。系统使用 Tobii EyeX 提取用户的视线位置,将其作为像鼠标一样的输入设备。通过注视目标图像 0.911 s,用户可以选中该图像;通过注视功能键 0.676 s,用户可以激活对应功能键,图像或功能键被激活后会发出蜂鸣声。在注册阶段,用户可以分别选取 2 ~6 幅图像作为用户名或密码,然后这些账户信息被加密并存储在数据库中。

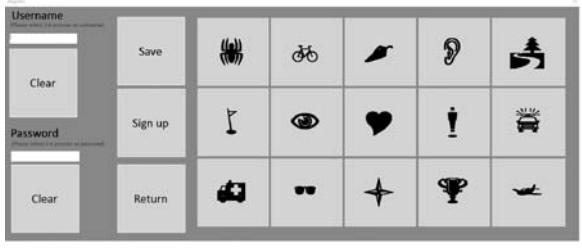


图 4 系统注册界面示意图

用户注册过程如图 5 所示(用户密码重置过程与注册时类似)。在注册阶段,同一图像可以被用户选取多次,用户只需要稍后选择并再次激活它。然后,用户在登录阶段识别并认证他们预先选择的 PIIs,以便进行身份验证。在每次登录过程中,系统以 3 ×5 个网格显示 15 幅图像,图像位置随机分布,每 5 s 刷新一次,时间间隔定义为刷新帧。

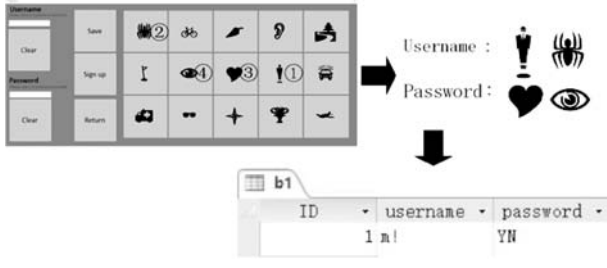


图 5 账户注册过程示意图

本系统中,将使用的注视定义为 AOI 中一系列注视总持续时间的叠加与平均位置的结合。在注册阶段,用户名图像被选中时对应图像变为红色,密码图像被选中时对应图像变为黄色;在登录阶段图像被选中时无任何视觉反馈,通过发出“嘀”的声音提醒用户图像被选中,以抵御用户登录时可能存在的窥探攻击。

2 用户测试及系统可用性评估

2.1 用户测试实验

招募 20 名受试者进行用户测试研究(14 名男性、6 名女性),受试者的年龄从 23 岁到 26 岁,平均为 24.25 岁。其中 7 名受试者视力正常,其余受试者通过戴眼镜矫正至视力正常。所有受试者均没有使用基于

视线交互的图像认证系统的经验。为了进行有效评估,账户中用户名和密码的长度都被设置为 2。在简要介绍图像认证系统的使用流程之后,受试者开始使用 Tobii EyeX 进行视线标定,然后依次完成注册和登录两项任务。出于评估的目的,将两个任务划分为若干子任务,每个子任务在不同的用户界面上进行。对于每次测试,受试者被指示依次进行如下任务:(1) 选取用户名图像;(2) 确认用户名;(3) 选取密码图像;(4) 确认密码并注册;(5) 使用账户信息登录;(6) 退出。

在实验期间,受试者可以重复尝试、跳过或重新启动任务(重新创建用户名或重新创建新密码)。受试者重复测试直到他们成功进行 3 次完整测试。每次测试间隔 10 分钟,每个受试者要在 2 小时内完成整个实验。记录所有受试者的实验数据,并要求每位受试者填写一份关于图像认证系统可用性的调查问卷。

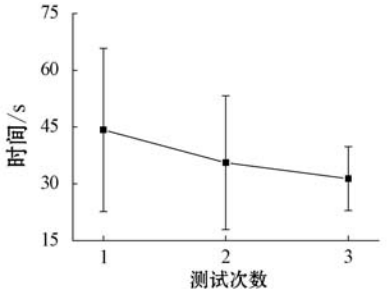
2.2　实验结果与分析

所有受试者的实验结果如表 2 所示。可以看出,只有 1 名受试者进行了 5 次测试(最大测试次数),比例为 5%;8 名受试者进行了 4 次,比例为 40%;11 名受试者进行了 3 次,比例为 55%。实验结果表明,受试者对任务几乎没有困难,他们可以成功完成测试,但是可能需要多次尝试。受试者完成一个完整测试的总时间从 40.35 s 到 152.66 s 不等,注册过程大约花费了 42.80% 的时间,登录过程与注册过程相比花费的时间更多,这是由于账户登录过程中密码图像输入时无视觉反馈,这增加了实验难度。

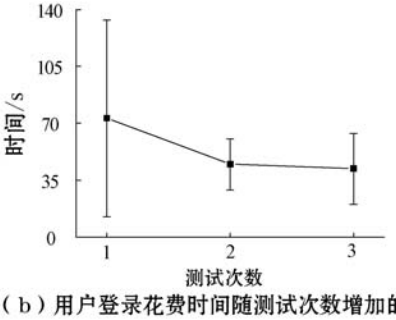
表 2　每个受试者进行的总测试次数

测试次数	人次	比例/%
3	11	55
4	8	40
5	1	5

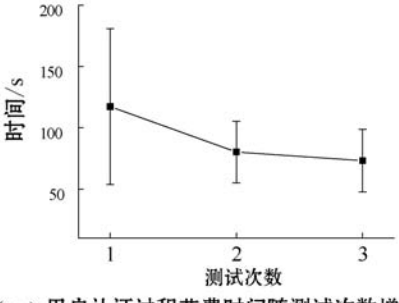
对所有受试者在各个阶段花费的时间进行比较,结果如图 6 所示。可以看出单次测试花费的时间随着实验测试次数的增加逐渐下降,无论在哪个阶段受试者第一次测试都花费更多时间。当受试者熟悉认证系统时,实验花费的时间会减少。这表明受试者在各阶段花费的时间与用户对图像认证系统的熟悉程度高度相关。当有错误 PII 输入时,用户通常需要额外的时间来移除和修复,所以用户在同一阶段花费的时间可能由于输入错误而具有大的标准偏差,这是图 6(b)中第三次登录时标准偏差较大的原因。



(a) 用户注册花费时间随测试次数增加的变化



(b) 用户登录花费时间随测试次数增加的变化



(c) 用户认证过程花费时间随测试次数增加的变化

图 6　受试者随测试数增加在各个阶段花费时间的变化

实验中忘记确认用户名的现像出现了 7 次,这是由用户习惯导致的(虽然在实验前已经介绍并特别提醒),这表明固有的生活习惯对人们的行为影响很大。实验失败的主要原因是受试者在登录时无法适应密码刷新频率,占所有错误的 79.49%,紧接的错误类型是忘记密码、记错密码、重新输入密码前未清零等。从调查问卷可以看出,所有受试者都指出基于视线交互的方法比基于点击的方法需要更多的操作时间。大部分的受试者表示愿意在将来使用基于视线交互的图像认证系统。

3　结　语

本文提出一种基于视线交互的图像密码认证系统,并通过用户测试研究验证了系统的可用性和有效性。视线跟踪技术的引入增加系统的可靠性、可用性以及对窥探攻击的抵抗能力。本文系统相比传统的鼠标或键盘输入的密码认证更加安全,但是基于注视驻留的视线交互过于缓慢且存在一定出错的概率,同时

(下转第 290 页)

向了源文件,得到 Java 代码,便可以分析秘密份额存储位置,从而获取密钥。本文方案则是在密钥保护阶段,通过与多云平台交互,将秘密份额存在不同的云服务端上,逆向不能得到密钥存储的相关信息,具有更高的安全性。

由于实验环境、设备参数、代码复杂度等因素存在差异,所以实验结果会有一定的误差,但是总体来看时间差稳定在 100 ~ 150 ms 内,不会影响用户体验。

4 结 语

本文提出了一种新的 Android 密钥管理技术,通过结合多云存储和秘密共享的思想,在密钥处理阶段,将秘密份额存放在 n 个云服务端上,与现有方案相比,减少了逆向得到密钥信息的可能性,能够避免云客户端和云服务端的合谋攻击,实现了 Android 客户端密钥的安全存放。在大文件加解密时,对加解密总时间的影响会显著减少,具有实用性。

参 考 文 献

[1] 张玉清,王凯,杨欢,等. Android 安全综述[J]. 计算机研究与发展,2014,51(7):1385 - 1396.

[2] 谢佳筠,伏晓,骆斌. Android 防护技术研究进展[J]. 计算机工程,2018,44(2):163 - 170,176.

[3] Sufatrio,Tan D J J,Chua T W,et al. Securing android:a survey,taxonomy,and challenges[J]. ACM Computing Surveys,2015,47(4):1 - 45.

[4] 李成吉,雷灵光,林璟锵,等. 安全的 Android 移动终端内容保护方案[J]. 计算机工程与设计,2016,37(3):591 - 596.

[5] 秦文仙,王琼霄,高能,等. 基于 RFID 智能卡的 Android 移动终端数据保护方案[J]. 计算机工程与应用,2016,52(2):112 - 116,126.

[6] 安迪,杨超,姜奇,等. 一种新的基于指纹与移动端协助的口令认证方法[J]. 计算机研究与发展,2016,53(10):2399 - 2410.

[7] Wang D,Cheng H B,He D B,et al. On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices[J]. IEEE Systems Journal,2018,12(1):916 - 925.

[8] He D B,Zeadally S,Wu L B,et al. Certificateless public auditing scheme for cloud-assisted wireless body area networks[J]. IEEE Systems Journal,2018,12(1):64 - 73.

[9] 孔琰,赵帅兵,刘若琳,等. 基于安卓平台的多云存储系统[J]. 计算机应用,2017,37(S1):39 - 44,48.

[10] You L,Chen Y L,Yan B,et al. A novel location-based encryption model using fuzzy vault scheme[J]. Soft Computing,2018,22:3383 - 3393.

[11] 刘培鹤,闫翔宇,何文才,等. 基于 Android 的密钥分存方案[J]. 计算机应用与软件,2018,35(2):320 - 324,333.

[12] 王志中,周城,牟宇飞. 基于分离密钥的云存储加密解决方案[J]. 电信科学,2013,29(1):51 - 56.

[13] 杨波. 密码学中的可证明安全性[M]. 清华大学出版社,2017.

[14] 张玉清,王晓菲,刘雪峰,等. 云计算环境安全综述[J]. 软件学报,2016,27(6):1328 - 1348.

[15] 傅颖勋,罗圣美,舒继武. 安全云存储系统与关键技术综述[J]. 计算机研究与发展,2013,50(1):136 - 145.

(上接第 285 页)

激活图像的时间阈值也需要进一步研究,以改善交互体验。并且用户测试也存在一定的局限性,无法对该认证系统进行全面评估。未来将进一步探索基于注视的 PII 输入策略,同时在系统设计时考虑用户本身的固有习惯,以提高认证系统的效率和可用性。

参 考 文 献

[1] Valles P A S, Villalobos-Serrano J G, Martinez-Pelaez R, et al. My personal images as my graphical password [J]. IEEE Latin America Transactions, 2018, 16(5): 1516 - 1523.

[2] Mihajlov M, Jerman-Blazic B. Eye tracking graphical passwords [C]//International Conference on Applied Human Factors and Ergonomics, 2017.

[3] Maeder A, Fookes C, Sridharan S. Gaze based user authentication for personal computer applications [C]//Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004.

[4] Hoanca B, Mock K. Secure graphical password system for high traffic public areas [C]//Proceedings of the Eye Tracking Research and Application Symposium, 2006.

[5] Dunphy P, Fitch A, Olivier P. Gaze-contingent passwords at the ATM [C]//4th Conference on Communication by Gaze Interaction (COGAIN), 2008.

[6] Dan W H, Ji Q. In the eye of the beholder: a survey of models for eyes and gaze [J]. IEEE Trans Pattern Anal Mach Intell, 2010, 32(3): 478 - 500.

[7] Zhang Y, Mou X. Survey on eye movement based authentication systems[C]//CCF Chinese Conference on Computer Vision, 2015.

[8] Hansen J P, Rajanna V, MacKenzie I S, et al. A fitts' law study of click and dwell interaction by gaze, head and mouse with a head-mounted display [C]//Workshop on Communication by Gaze Interaction, 2018: 1 - 5.