แฮปติกพอยท์ : การยืนยันตัวตนด้วยรหัสผ่านรูปภาพแบบคิวด์รีคอลล์

HAPTICPOINTS : A CUED RECALL BASED GRAPHICAL PASSWORD SYSTEM

ธรรศ รัชสัน

TRUST RATCHASAN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2562

KMITL-2019-SC-M-002-027

แฮปติกพอยท์ : การยืนยันตัวตนด้วยรหัสผ่านรูปภาพแบบคิวด์รีคอลล์

HAPTICPOINTS : A CUED RECALL BASED GRAPHICAL PASSWORD SYSTEM

ธรรศ รัชสัน

TRUST RATCHASAN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2562

KMITL-2019-SC-M-002-027

HAPTICPOINTS : A CUED RECALL BASED GRAPHICAL PASSWORD SYSTEM

TRUST RATCHASAN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE FACULTY OF SCIENCE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2019
KMITL-2019-SC-M-002-027

หัวข้อวิทยานิพนธ์ แฮปติกพอยท์ : การยืนยันตัวตนด้วยรหัสผ่านรูปภาพแบบคิวด์รีคอลล์

ชื่อนักศึกษา ธรรศ รัชสัน

รหัสประจำตัว 58605087

ปริญญา วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

ภาควิชา วิทยาการคอมพิวเตอร์

พ.ศ. 2562

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์

บทคัดย่อ

รหัสผ่านรูปภาพเป็นระบบยืนยันตัวตนที่มีเป้าหมายในการแก้ปัญหาความยากในการจำของรหัสผ่านตัวอักษร แต่ระบบรหัสผ่านรูปภาพที่มีความปลอดภัยสูงส่วนใหญ่มีความง่ายในการใช้งานต่ำจึงไม่เป็นที่นิยมในการนำมาประยุกต์ใช้ในการยืนยันตัวตนตนบนสมาร์ทโฟน งานวิจัยนี้มีวัตถุประสงค์ในการพัฒนารหัสผ่านรูปภาพใหม่ที่มีความปลอดภัยสูง มีความง่ายในการจำ และมีความง่ายในการใช้งาน โดยแบ่งการทำงานเป็น 2 ส่วน ส่วนที่หนึ่งคือการพิสูจน์ว่าความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพบนสมาร์ทโฟนจะเพิ่มมากขึ้นเมื่อทำการใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ โดยทดสอบกับรหัสผ่านรูปภาพ 3 ระบบ คือ พาสโก พาสเฟซ และ พาสพอยท์ กับผู้ใช้งานจำนวน 40 คน ผลการทดสอบพบว่าทุกรหัสผ่านรูปภาพมีความง่ายในการใช้งานเพิ่มขึ้นทั้งทางปริมาณและทางคุณภาพ และพาสพอยท์คือรหัสผ่านรูปภาพที่เหมาะสมที่สุดในการนำมาพัฒนาเพิ่มความปลอดภัย ในส่วนที่สองงานวิจัยนี้จึงทำการเพิ่มรหัสผ่านปลอมด้วยการสั่นแบบแฮปติกเพื่อป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิง และใช้หลักการของอิมเมจซาเลียนซี่ด้วยอัลกอริทึมดีพเกซในการเพิ่มความปลอดภัยจากการโจมตีแบบฮอทสปอต ผลการทดสอบสรุปได้ว่ารหัสผ่านรูปภาพแบบแฮปติกพอยท์มีความง่ายในการจำใกล้เคียงกับรหัสผ่านตัวเลขหกหลัก มีความง่ายในการใช้งานไม่แตกต่างจากรหัสผ่านรูปภาพพาสพอยท์หลังจากได้ใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์แบบไม่มีนัยสำคัญด้วยการทดสอบที และมีความปลอดภัยสูงกว่าพาสพอยท์

คำสำคัญ : ระบบการยืนยันตัวตน, รหัสผ่านรูปภาพ, ปฏิสัมพันธ์ระหว่างมนุษย์กับคอมพิวเตอร์, ความง่ายในการใช้งาน, ระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์, พาสพอยท์, แฮปติกพอยท์

Thesis Title	Hapticpoints : A cued recall based graphical password system
Student Name	Trust Ratchasan
Student ID	58605087
Degree	Master of Science (Computer Science)
Department	Computer Science
Year	2019
Thesis Advisor	Dr. Rungrat Wiangsripanawan

Abstract

Graphical password systems have been proposed to solve the memorability problem of text passwords. High security graphical password systems seem to provide low usability, There is a trade-of between usability and security. Hence, graphical password systems are not popular for smartphone authentication system. The objective of this thesis is to develop the new graphical password system which provides high security, memorability and usability. The thesis consists of two parts. The first part is to prove the hypothesis that the usability of graphical password system on smartphones will increase after using it consecutively for one week. The experiment has been done with 3 graphical password systems: Pass-Go, PassFace and PassPoints with 40 participants. Both quantitative and qualitative result suggests that PassPoints is the most suitable system to be extended. This thesis adds haptic feedback as additional decoy click points to prevent shoulder surfing attack and implements image saliency using DeepGaze to prevent dictionary attacks with hotspot. The consequence shows that Hapticpoints' memorability is closed to six-digit PINs, its usability is insignificantly different from PassPoints with T-Test. Besides, it provides higher security from PassPoints.

Keywords : Authentication System, Graphical Password System, Human and Computer Interaction , Usability, Cued-recall Graphical Password System, PassPoints, HapticPoints

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ จะไม่สามารถสำเร็จลงได้ด้วยดีหากขาดการช่วยเหลือ และสนับสนุนของบุคคลหลายท่าน ผู้จัดทำขอขอบพระคุ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ที่กรุณาให้คำปรึกษา คำแนะนำด้านการออกแบบ วิเคราะห์ ทดสอบขั้นตอนวิธีและแนวทางการแก้ปัญหารวมถึงการตรวจสอบ และแก้ไขการเขียนวิทยานิพนธ์ฉบับนี้อย่างละเอียด

ขอขอบพระคุณ ผศ.ดร.ชัยพร ใจแก้ว ผศ.ดร.วรางคณา กิ้มปาน ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ และ คณะกรรมการสอบหัวข้อวิทยานิพนธ์ ที่ให้คำแนะนำตลอดข้อชี้แนะจนทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้

ขอขอบคุณผู้ร่วมทดสอบกว่า 60 คนที่เข้าร่วมการทดสอบเก็บข้อมูลในวิทยานิพนธ์ฉบับนี้ที่ให้การสนับสนุนช่วยเหลือในการทดสอบขั้นตอนวิธีจนสำเร็จสมบูรณ์

สุดท้ายนี้ขอกราบขอบพระคุณคุณครอบครัวผู้เป็นแรงกายแรงใจสำคัญนั่นคือครอบครัวตั้งแต่ต้นจนจบ นอกจากนี้อาจมีบุคคลท่านอื่นที่ไม่ได้กล่าวไว้ ณ ที่นี้ จึงใคร่ขอขอบพระคุณทุกท่านที่ให้ความกรุณา มีส่วนร่วมในการให้ความช่วยเหลือ ให้คำปรึกษา ให้คำแนะนำ ตลอดจนให้กำลังใจในการทำวิทยานิพนธ์ฉบับนี้

ธรรศ รัชสัน

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันบนสมาร์ทโฟนมีการพัฒนาเป็นอย่างมาก เช่น กล้องถ่ายรูปคุณภาพสูง การเชื่อมต่ออินเทอร์เน็ตที่รวดเร็ว มีแอปพลิเคชันให้เลือกใช้งานเป็นจำนวนมาก รวมไปถึงการใช้เทคโนโลยีการยืนยันตัวตนด้วยรหัสผ่านชีวภาพ เช่น การยืนยันตัวตนด้วยลายนิ้วมือ หรือ การยืนยันตัวตนด้วยม่านตา แต่เมื่อใดก็ตามที่การยืนยันตัวตนเหล่านี้มีเหตุขัดข้อง สมาร์ทโฟนยังจำเป็นที่ต้องใช้การยืนยันตัวตนแบบเดิม คือ รหัสผ่านตัวอักษร รหัสผ่านตัวเลข และ วิธีการปลดล็อคของแอนดรอยด์

รหัสผ่านตัวอักษรที่แข็งแรงมักมีความยากในการจำ ทำให้ผู้ใช้ส่วนใหญ่สร้างตัวอักษรที่ไม่แข็งแรงพอ รหัสผ่านตัวเลขมีความง่ายในการจำมากกว่ารหัสผ่านตัวอักษรแต่รหัสผ่านตัวสี่ถึงหกหลักเลขมีเอนโทรปีหรือความแข็งแรงของรหัสผ่าน เพียง 16 ถึง 20 บิต วิธีการปลดล็อคของแอนดรอยด์มีความง่ายในการจำและความง่ายในการใช้งานแต่วิธีการปลดล็อคของแอนดรอยด์มีความปลอดภัยที่ต่ำที่สุดในระบบรหัสผ่านทั้งหมดที่กล่าวถึง ระบบรหัสผ่านรูปภาพเป็นหนึ่งในวิธีการยืนยันตัวตนที่มีศักยภาพสูงและมีความปลอดภัยที่สูงกว่าการใช้รหัสผ่านตัวเลขและวิธีการปลดล็อคของแอนดรอยด์ และยังสามารถจดจำได้ดีโดยเฉพาะระบบรหัสผ่านแบบคิวด์รีคอลล์ ซึ่งสามารถจดจำได้ง่ายที่สุดในบรรดาประเภทของรหัสผ่านรูปภาพเพราะมีรูปภาพในการช่วยจำ แต่ปัญหาโดยทั่วไปของรหัสผ่านรูปภาพที่มีความปลอดภัยสูงคือมีความง่ายในการใช้งานต่ำ จึงไม่เป็นที่นิยมในการนำมาประยุกต์ใช้ในการยืนยันตัวตนบนสมาร์ทโฟน อีกปัญหาหนึ่งของระบบรหัสผ่านรูปภาพที่พบส่วนใหญ่คือการโจมตีแบบโชลเดอร์เซิร์ฟฟิง คือการโจมตีด้วยการสังเกตุการป้อนข้อมูลรหัสผ่านระหว่างที่ผู้ใช้กำลังยืนยันตัวตนจากด้านหลังหรือด้านข้าง

งานวิจัยนี้จึงถูกแบ่งเป็นสองส่วน ส่วนแรกคือการทดสอบสมมติฐานเรื่องความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพบนสมาร์ทโฟนจะเพิ่มมากขึ้นเมื่อทำการอบรมและใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ และส่วนที่สองคือการพัฒนารหัสผ่านรูปภาพใหม่บนสมาร์ทโฟนที่มีความปลอดภัยและความง่ายในการจำสูงกว่ารหัสผ่านตัวอักษรและรหัสผ่านตัวเลขโดยไม่ลดความง่ายในการใช้งาน ในส่วนแรกนั้นผู้วิจัยทำการอบรมการใช้งานของระบบรหัสผ่านรูปภาพแบบรีคอลล์ ระบบรหัสผ่านรูปภาพแบบรีคอกนิชัน และ ระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ โดยเลือกวิธีที่มีศักยภาพสูงสุดในแต่ละประเภท และทดลองให้ผู้ใช้ใช้งานระบบรหัสผ่านรูปภาพอย่างต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ โดยผู้วิจัยได้ทำการวัดผลการทดสอบความง่ายในการใช้งานเป็นสองหมวดหมู่ คือ การทดสอบเชิงปริมาณ และ การทดสอบเชิงคุณภาพ พารามิเตอร์ในการทดสอบเชิงปริมาณประกอบด้วย อัตราความผิดพลาดซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด จำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ ระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จ ส่วนการทดสอบเชิงคุณภาพใช้แบบทดสอบความง่ายใน

การใช้งานหลังการใช้งานระบบ โดยมีพารามิเตอร์ในการทดสอบคือ ประโยชน์ในการใช้งานของระบบ (SysUse) คุณภาพในการแสดงผลข้อมูลของระบบ (InfoQual) ส่วนติดต่อระหว่างผู้ใช้และระบบ (InterQual) และ ความพึงพอใจโดยรวมต่อระบบ (Overall) โดยผู้วิจัยได้นำผลการทดสอบมาค้นหาความแตกต่างในเชิงสถิติโดยใช้การทดสอบทีเพื่อวัดนัยสำคัญของความเปลี่ยนแปลงในวันแรกและวันสุดท้ายของการทดสอบ จากนั้นนำระบบรหัสผ่านรูปภาพที่มีศักยภาพที่สุดมาวิเคราะห์ความปลอดภัยและภัยคุกคาม แล้วทำการปรับปรุงพัฒนาเป็นระบบใหม่นั่นคือระบบรหัสผ่านรูปภาพแฮปติกพอยท์โดยมีเป้าหมายสูงสุดคือ มีความปลอดภัยมากกว่าระบบรหัสผ่านตัวเลข มีความง่ายในการจำ และมีความง่ายในการใช้งานใกล้เคียงกับระบบรหัสผ่านตัวเลขหกหลัก

1.2 วัตถุประสงค์ของการวิจัย

1) เพื่อค้นหาระบบรหัสผ่านรูปภาพที่มีอยู่ที่มีอยู่แล้วที่มีความปลอดภัยและความง่ายในการจำสูงกว่ารหัสผ่านตัวอักษรและรหัสผ่านตัวเลข
2) ทดสอบสมมติฐานเรื่องความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพบนสมาร์ทโฟนจะเพิ่มมากขึ้นเมื่อทำการอบรมและใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์
3) พัฒนาระบบรหัสผ่านรูปภาพใหม่บนสมาร์ทโฟนที่มีความปลอดภัยและความง่ายในการจำสูงกว่ารหัสผ่านตัวอักษรและรหัสผ่านตัวเลขโดยไม่ลดความง่ายในการใช้งาน

1.3 สมมติฐานของการวิจัย

1) หลังจากทำการอบรมเป็นเวลาหนึ่งสัปดาห์แล้วผู้ใช้มีความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพที่ดีขึ้น
2) ระบบรหัสผ่านรูปภาพระบบใหม่ที่สร้างขึ้นต้องมีความแข็งแรกของรหัสผ่านมากกว่ารหัสผ่านตัวเลขหกหลัก (20 บิต)
3) ระบบรหัสผ่านรูปภาพระบบใหม่ที่สร้างขึ้นต้องมีความง่ายในการใช้งานไม่ต่างจากระบบปัจจุบันมากเกินไป
4) ระบบรหัสผ่านรูปภาพระบบใหม่ที่สร้างขึ้นต้องมีความสามารถในการป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิง

1.4 ขอบเขตของการวิจัย

1) กลุ่มตัวอย่างในการทดสอบความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพ คือ บุคคลทั่วไปที่ทำงานบริษัทไอทีที่ใช้สมาร์ทโฟนในชีวิตประจำวัน มีอายุ 23 - 35 ปี จำนวน 40 คน
2) กลุ่มตัวอย่างในการทดสอบความง่ายในการใช้และการทดสอบความปลอดภัยของระบบรหัสผ่านรูปภาพแฮปติกพอยท์ คือ บุคคลทั่วไปที่ทำงานบริษัทไอทีที่ใช้สมาร์ทโฟนในชีวิตประจำวันมีอายุ 24 - 33 ปี จำนวน 35 คน

3) ทำการทดลองและพัฒนาระบบรหัสผ่านรูปภาพบนสมาร์ทโฟนแอนดรอยด์ซึ่งมีขนาดหน้าจอ 4.5 - 5.5 นิ้ว

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) เพิ่มทางเลือกให้ผู้ใช้สมาร์ทโฟนในการยืนยันตัวด้วยรหัสผ่านรูปภาพ
2) ระบบรหัสผ่านรูปภาพระบบใหม่มีความปลอดภัยที่สูงกว่าระบบยืนยันตัวตนที่เป็นที่นิยมในปัจจุบันและมีความง่ายในการใช้งานสูง
3) นักพัฒนาสามารถนำระบบรหัสผ่านรูปภาพระบบใหม่ไปประยุกต์ใช้กับการยืนยันตัวตนของแอปพลิชันต่างๆบนสมาร์ทโฟนได้

1.6 ขั้นตอนของการวิจัย

1) ศึกษาและวิจัยรหัสผ่านรูปภาพที่มีในปัจจุบันพร้อมทั้งข้อดีและข้อเสีย
2) เลือกรหัสผ่านรูปภาพที่มีความปลอดภัยสูงและมีความง่ายในการใช้งานมาพัฒนาเป็นต้นแบบ
3) นำต้นแบบมาทดสอบและสำรวจความคิดเห็นของผู้ใช้จำนวน 40 คน
4) ศึกษาผลการทดลองและเปรียบเทียบกับรหัสผ่านตัวเลขบนสมาร์ทโฟนแบบปัจจุบัน
5) วิเคราะห์ผลการทดลองและเลือกรหัสผ่านรูปภาพที่มีประสิทธิภาพดีที่สุดการสร้างรหัสผ่านรูปภาพแบบใหม่
6) วิเคราะห์ความปลอดภัยของรหัสผ่านรูปภาพที่เลือก
7) พัฒนาต้นแบบของแฮปติกพอยท์โดยมีวัตถุประสงค์ในการป้องกันการโจมตีของรหัสผ่านรูปภาพแบบบรูทฟอร์ซ ดิกชันนารี และโดยเฉพาะอย่างยิ่งการโจมตีแบบโชลเดอร์เซิร์ฟฟิง
8) ทำการทดสอบความง่ายในการใช้งานกับผู้ใช้และวิเคราะห์ความปลอดภัยเพื่อเปรียบเทียบกับรหัสผ่านรูปภาพแบบเดิม
9) สรุปและวิเคราะห์ผลการทดลอง
10) จัดทำเอกสารและเสนอรายงานวิทยานิพนธ์ฉบับสมบูรณ์

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 รหัสผ่านรูปภาพ (Graphical Password)

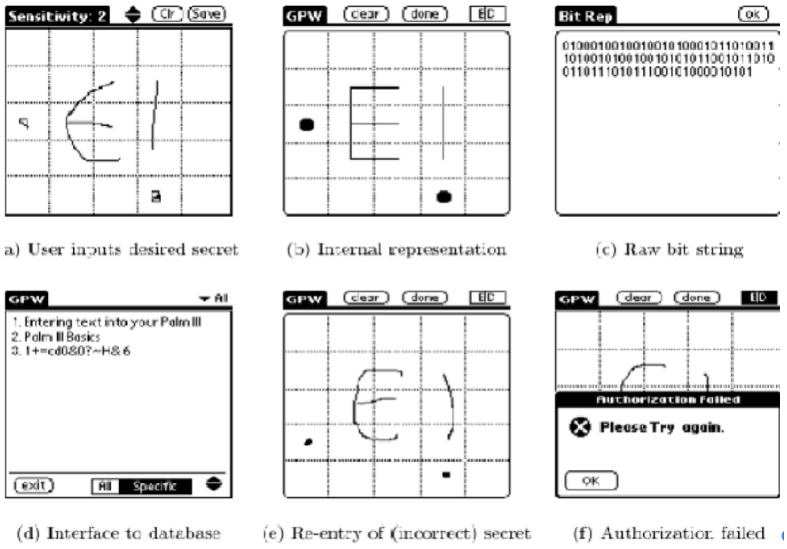
รหัสผ่านรูปภาพคือระบบยืนยันตัวผ่านรูปภาพโดยให้ผู้ใช้เลือกรูปภาพหรือจุดในรูปภาพเป็นรหัสผ่าน รหัสผ่านรูปภาพเป็นหนึ่งในระบบยืนยันตัวตนทางเลือกที่มีเป้าหมายในการแก้ไขปัญหาความยากในการจำของรหัสผ่านตัวอักษร [1, 2] จากการศึกษาด้านจิตวิทยาพบว่าการจดจำรูปภาพนั้นทำได้ง่ายตัวอักษรหรือตัวเลข [3, 4] แต่การใช้รหัสรูปภาพยังมีข้อเสียบางอย่างอยู่คือความง่ายในการใช้ เช่น ใช้เวลาเพื่อการเข้าสู่ระบบที่นานเกินไป หรือ อัตราความผิดพลาดในการเข้าสู่ระบบที่สูง [5] บิดเดิลและคณะ ได้จำแนกและเปรียบเทียบรหัสผ่านรูปภาพไว้ 3 ประเภท คือ ระบบรหัสผ่านรูปภาพแบบรีคอลล์ (recall-based system) ระบบรหัสผ่านรูปภาพแบบรีคอกนิชัน (recognition-based system) และ ระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ (cued-recall system)

2.1.1 ระบบรหัสผ่านรูปภาพแบบรีคอลล์ (Recall-based graphical password system)

รหัสผ่านรูปภาพระบบนี้เป็นระบบที่ให้ผู้ใช้เรียกคืนความจำผ่านการวาดเส้นลงบนพื้นที่ว่างเปล่าหรือตาราง รหัสผ่านรูปภาพระบบนี้จึงมักถูกเรียกว่าระบบดรอว์เมตริค [6] (drawmetric system) การเรียกคืนความจำในระบบรหัสผ่านรูปภาพระบบนี้เป็นสิ่งที่ยากสำหรับสมองเนื่องจากการเรียกคืนนั้นถูกกระทำโดยไม่มีตัวช่วยใดๆปรากฏอยู่บนรูปภาพ เป็นการจำแบบเดียวกันกับรหัสผ่านตัวอักษร

1.) รหัสผ่านรูปภาพดีเอเอส (Draw-A-Secret DAS) [7] : ระบบรหัสผ่านรูปภาพระบบนี้เป็นรหัสผ่านรูปภาพแรกที่ถูกสร้างขึ้นของระบบรหัสผ่านรูปภาพแบบรีคอลล์ โดยให้ผู้ใช้วาดเส้นลงบนตารางสองมิติด้วยเมาส์หรือปากกาสไตลัส (รูปที่ 2.1) ในหนึ่งเส้นของการวาดนับจากการวาดเส้นต่อเนื่อง จนกว่าจะยกปากกาขึ้นซึ่งในหนึ่งรหัสผ่านสามารถมีได้หลายเส้น สำหรับการยืนยันตัวตนผู้ใช้จะต้องวาดเส้นรหัสผ่านด้วยเส้นเหล่านั้นให้เหมือนเส้นที่สร้างขึ้นลงบนตาราง

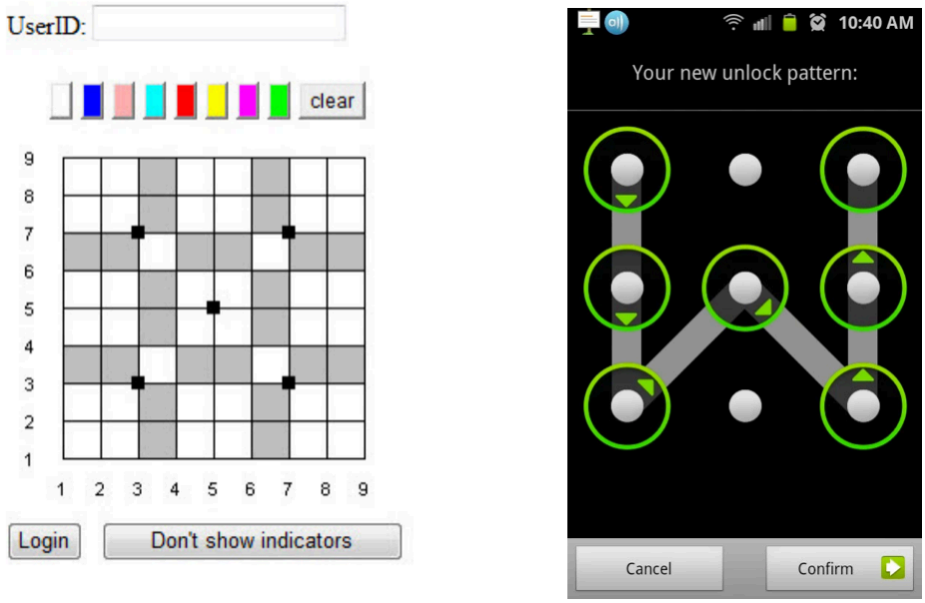
2.) รหัสผ่านรูปภาพบีดีเอเอส (BDAS) [8] : เป็นรหัสผ่านรูปภาพที่นำรหัสผ่านรูปภาพดีเอเอสมาปรับปรุงโดยนำภาพพื้นหลังใส่ลงไปบนตารางสองมิติเพื่อกระตุ้นให้ผู้ใช้สร้างรหัสผ่านที่ยากขึ้น จากผลการทดลองแสดงให้เห็นว่ารหัสผ่านรูปภาพระบบนี้สามารถทำให้ผู้ใช้สร้างรหัสผ่านที่แข็งแรงขึ้นได้โดยที่ใช้ความจำเท่าเดิมเมื่อเปรียบเทียบกับรหัสผ่านรูปภาพดีเอเอสแต่การนำพื้นหลังมาใส่ก็อาจตกเป็นเป้าหมายสำหรับการคาดเดารหัสผ่านโดยผู้โจมตีได้ง่ายขึ้นเช่นกัน



รูปที่ 2.1 รหัสผ่านรูปภาพดีเอเอส

3.) รหัสผ่านรูปภาพพาสโก (Pass-Go) [9] : รหัสผ่านรูปภาพระบบนี้ได้รับแรงบันดาลใจมาจากข้อผิดพลาดในการใช้งานของรหัสผ่านรูปภาพดีเอเอสนั่นคือความยากในการวาดเส้นที่แม่นยำและเหมือนกันทุกครั้ง รหัสผ่านรูปภาพพาสโกจึงบังคับให้ผู้ใช้วาดเส้นหรือจุดผ่านจุดตัดของตารางสองมิติเท่านั้น (เหมือนกับการวางหมากบนตารางหมากรุกโกะนั่นเอง) ซึ่งวิธีนี้สามารถลดความยุ่งยากในการใส่รหัสผ่านของรหัสผ่านรูปภาพดีเอเอสได้เป็นอย่างดี นอกจากนั้นรหัสผ่านรูปภาพพาสโกยังมีจำนวนรหัสผ่านที่มากกว่ารหัสผ่านรูปภาพดีเอเอสอีกด้วย (เนื่องจากตารางสองมิติที่มีความละเอียดกว่า และมีตัวเลือกในการเลือกสีของเส้นรหัสผ่าน) รหัสผ่านรูปภาพพาสโกยังถูกนำไปพัฒนาต่อในภายหลังเป็น การปลดล็อคของแอนดรอยด์ (รูปที่ 2.2) ที่ใช้กันอยู่ในปัจจุบันอีกด้วยเพียงแต่มีการปรับขนาดของตารางสองมิติให้น้อยลง เหลือเพียง 3x3 เท่านั้น

การโจมตีระบบรหัสผ่านรูปภาพแบบรีคอลล์ที่สำคัญได้แก่ การโจมตีแบบโชลเดอร์เซิฟฟิง (shoulder surfing attack) ผู้โจมตีจะสามารถสังเกตหรือบันทึกวีดีโอได้โดยง่ายจากรูปภาพทั้งหมดจะปรากฏบนหน้าจอขณะที่กำลังยืนยันตัวตน ซึ่งการโจมตีแบบโชลเดอร์เซิร์ฟฟิงเพียงครั้งเดียวก็มีรหัสผ่านอาจถูกเปิดเผยได้ การโจมตีแบบฟิชชิง (phishing) ผู้โจมตีเพียงสร้างหน้าเว็บไซต์ปลอมด้วยที่เหมือนเว็บไซต์จริงทุกประการที่ผู้ใช้จะทำการยืนยันตัวตนรวมไปถึงส่วนที่ผู้ใช้ใส่รหัสผ่านรูปภาพเมื่อผู้ใช้ใส่รหัสผ่านรูปภาพลงในเว็บไซต์ปลอม ผู้บุกรุกจะสามารถนำข้อมูลรหัสผ่านไปใช้ในเว็บไซต์จริงได้ทันที รหัสผ่านรูปภาพระบบนี้ไม่สามารถป้องกันการโจมตีแบบมัลแวร์ (malware attacks) ด้วยการใช้การบันทึกหน้าจอ (screen scrapers) หรือ การบันทึกรูปแบบการใช้เมาส์ (mouse loggers) ผู้โจมตีก็จะสามารถรู้ถึงตำแหน่งในการป้อนข้อมูลของรหัสผ่านรูปภาพระบบนี้ได้ ในส่วนถัดไปจะเป็นการยกตัวอย่างของรหัสผ่านรูปภาพที่ประยุกต์ใช้ของระบบรหัสผ่านรูปภาพระบบนี้



รูปที่ 2.2 รหัสผ่านรูปภาพพาสโก

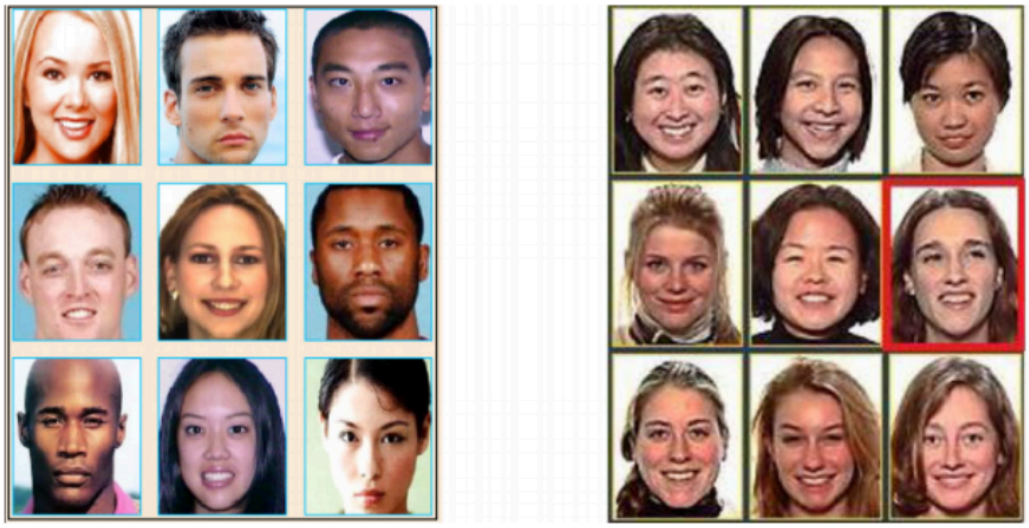
2.1.2 ระบบรหัสผ่านรูปภาพแบบรีคอกนิชัน (Recognition-based graphical password systems)

มนุษย์มีความสามารถในการจดจำรูปภาพเป็นอย่างดี แม้จะพึ่งเคยเห็นไม่นานก็ตาม [10, 11] รหัสผ่านรูปภาพระบบนี้นำความสามารถในการจำของมนุษย์มาประยุกต์ใช้โดยจะให้ผู้ใช้จดจำชุดของรูปภาพจำนวนหนึ่งในระหว่างการสร้างรหัสผ่านและเลือกจำแนกรูปภาพเหล่านี้ออกจากชุดของรูปภาพทั้งหมดในการยืนยันตัวตน แต่ในทางความปลอดภัยรหัสผ่านรูปภาพระบบนี้ไม่สามารถนำมาใช้แทนรหัสผ่านตัวอักษรได้เลย จำนวนรหัสผ่านของระบบนี้มีจำนวนเทียบเท่าเพียงรหัสผ่านตัวเลข 4 ถึง 5 หลักเท่านั้น รูปภาพที่ถูกนำมาใช้กับระบบนี้คือ รูปภาพหน้าคน รูปภาพศิลปะ วัตถุสิ่งของ และ ไอคอนในส่วนถัดไปจะเป็นการยกตัวอย่างของรหัสผ่านรูปภาพที่ประยุกต์ใช้ของระบบรหัสผ่านรูปภาพระบบนี้

1.) รหัสผ่านรูปภาพพาสเฟซ (Passfaces) [12] : เป็นรหัสผ่านรูปภาพที่ได้รับความนิยมที่สุดของรหัสผ่านรูปภาพระบบรีคอกนิชัน รหัสรูปภาพระบบนี้จะให้ผู้เลือกรูปภาพใบหน้ามนุษย์เป็นรหัสผ่าน โดยมีรูปภาพหลอกผสมอยู่ในชุดของรูปภาพทั้งหมด (รูปที่ 2.3) ในหนึ่งรอบผู้ใช้จะต้องเลือกรูปภาพรหัสผ่าน 1 รูปจากทั้งหมด 9 รูป โดยจะทำซ้ำทั้งหมดอย่างน้อย 4 รอบ และในแต่ระรอบหากผู้ใช้เลือกผิดจะต้องเลือกใหม่ตั้งแต่ต้น จำนวนรหัสผ่านของระบบนี้สามารถคำนวณได้จาก M = 9 (รูปทั้งหมด) และ n = 4 (จำนวนรอบ) เพราะฉนั้นจะมีขนาดของ จำนวนรหัสผ่านประมาณ 6561 หรือ 13 บิต จากการทดลองของผู้ใช้จำนวน 77 คน โดย วาเลนไทน์และคณะ [13] พบว่ารหัสผ่านระบบนี้มีอัตราความสำเร็จในการเข้าสู่ระบบถึงร้อยละ 72 ถึง 100 และผลการทดลองจาก บรอสตอฟและคณะ [12] พบว่าผู้ใช้มักจะกลับไปใช้รหัสผ่านตัวอักษรแทนรหัสผ่านรูปภาพระบบนี้ เนื่องจากใช้เวลา

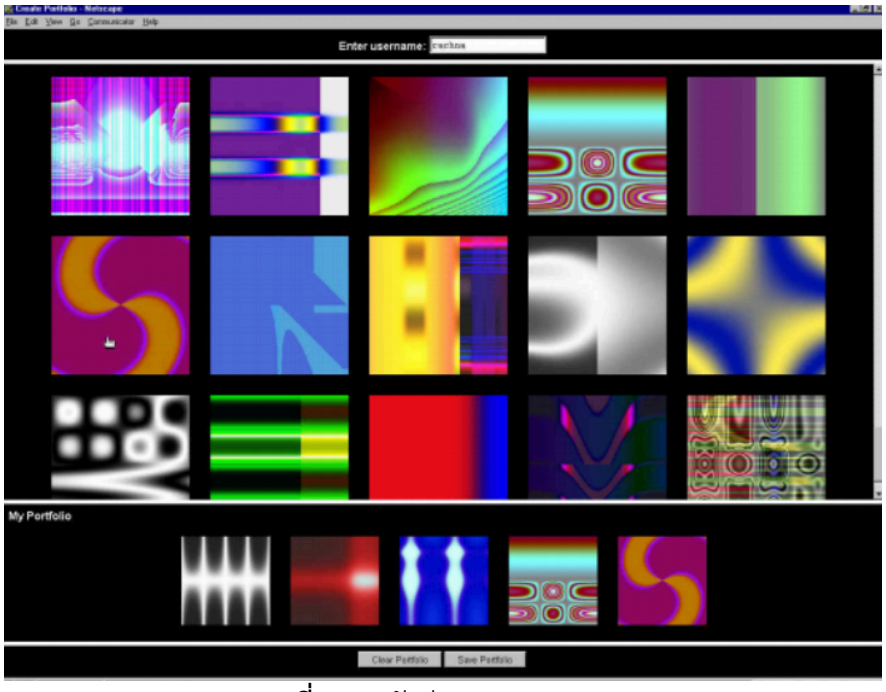
ในการเข้าสู่ระบบนานเกินไป ซึ่งสอดคล้องกับข้อมูลบนเว็บไซต์ของ รหัสผ่านรูปภาพพาสเฟซที่กล่าวว่าการเข้าสู่ระบบหนึ่งครั้งใช้เวลา 3 ถึง 5 นาที

2.) รหัสผ่านรูปภาพสตอรี่ซิสเต็ม (Story system) [14] : รหัสผ่านรูปภาพระบบนี้มีการทำงานคล้ายกับรหัสผ่านรูปภาพพาสเฟซแต่เปลี่ยนจากการใช้รูปใบหน้ามนุษย์ เป็นรูปภาพใดๆก็ได้ และให้ผู้ใช้เลือกรูปเป็นลำดับในขณะเข้าสู่ระบบ เพื่อที่จะให้ผู้ใช้เชื่อมรูปรหัสผ่านตามลำดับเป็นเรื่องราวซึ่งจะทำให้ผู้ใช้สามารถจดจำรหัสผ่านได้ง่ายขึ้น การเลือกรหัสผ่านรูปภาพในระหว่างเข้าสู่ระบบของผู้ใช้นั้นจะเลือกรหัสผ่าน 4 รูป จากรูปทั้งหมด 9 รูป จำนวนรหัสผ่านของระบบนี้สามารถคำนวณได้จาก 9 x 8 x 7 x 6 = 3024 หรือ 12 บิต เท่านั้น แต่จากการทดลองนั้นผลลัพธ์ออกมาตรงกันข้าม ผู้ใช้มีความยากในการจดจำมากขึ้น (อัตราความสำเร็จในการเข้าสู่ระบบประมาณร้อยละ 85) และผู้ใช้ส่วนใหญ่มักผิดพลาดในการเลือกลำดับของรหัสผ่าน



รูปที่ 2.3 รหัสผ่านรูปภาพพาสเฟซ

3.) รหัสผ่านรูปภาพเดจาวู (D´ej`a Vu) [15] : มีวิธีการใช้เหมือนกับรหัสผ่านรูปภาพพาสเฟซแต่ใช้รูปภาพศิลปะ (รูปที่ 2.4) แทนรูปภาพใบหน้ามนุษย์ ผู้ใช้จะต้องจดจำชุดของรหัสผ่านรูปภาพจำนวน 5 รูป จากชุดรูปภาพศิลปะจำนวน 25 รูป (ใหญ่กว่ารหัสผ่านรูปภาพพาสเฟซ และรหัสผ่านรูปภาพสตอรี่ซิสเต็ม) สำหรับการเข้าสู่ระบบนั้นรูปภาพศิลปะจะถูกแสดงทั้งหมด และเลือก 5 รูปภาพรหัสผ่านในครั้งเดียวโดยไม่ต้องมีลำดับในการเลือก ภาพศิลปะที่ถูกนำมาใช้นั้นเกิดจากการสร้างรูปภาพโดยสุ่ม จำนวนรหัสผ่านของรหัสผ่านรูปภาพระบบนี้คำนวณได้จากความน่าจะเป็นจากรูปภาพทั้งหมด 25 รูป เลือกเพียง 5 รูปจะได้ทั้งหมด 53130 หรือประมาณ 16 บิต รหัสผ่านรูปภาพระบบนี้ถูกออกแบบมาเพื่อป้องกันการโจมตีแบบดิกชันนารี (dictionary attack) เนื่องจากการทดลองพบว่าผู้ใช้มักเลือกรูปที่ไม่ซ้ำกัน นอกจากนั้นยังพบว่ารูปภาพศิลปะที่ผู้ใช้เลือกนั้นยากที่จะอธิบายให้คนอื่นเข้าใจได้กล่าวคือโอกาสที่รหัสผ่านจะถูกเปิดเผยด้วยผู้ใช้เองนั้นยากมาก อย่างไรก็ตามรหัสผ่านระบบนี้ผู้ใช้ต้องใช้เวลานานต่อการเข้าสู่ระบบหนึ่งครั้ง



รูปที่ 2.4 รหัสผ่านรูปภาพเดจาวู

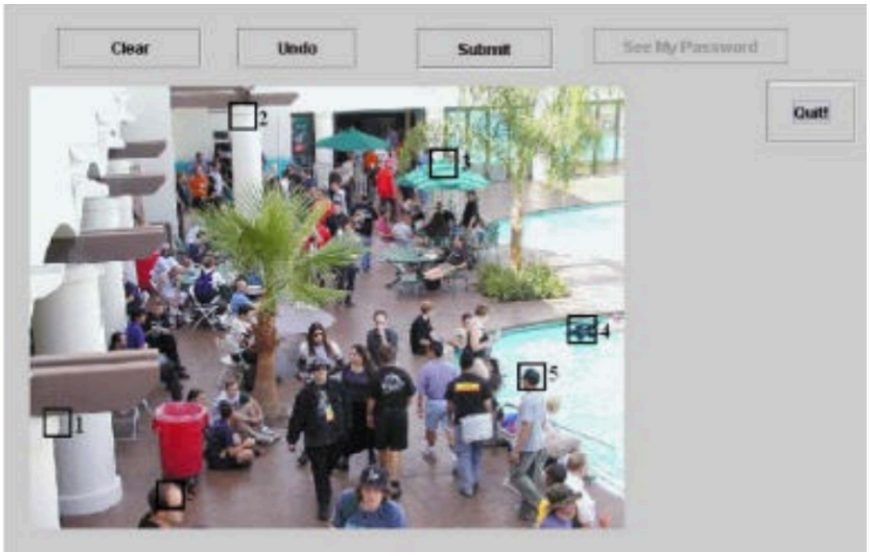
การโจมตีแบบฟิชชิงกับรหัสผ่านรูปภาพแบบนี้ทำได้ยากเนื่องจากรหัสผ่านรูปภาพทั้งหมดจะต้องถูกแสดงก่อนที่ผู้ใช้จะเริ่มทำการยืนยันตัวตน นั่นหมายความว่าการสร้างเว็บไซต์ปลอมของผู้โจมตีนั้นจะต้องมีการดึงข้อมูลจากเว็บไซต์จริงแบบเรียลไทม์แล้วนำข้อมูลชุดของรูปภาพไปแสดงบนเว็บไซต์ปลอม การโจมตีแบบนี้ต้องอาศัยการโจมตีแบบแมนอินเดอะมิดเดิล (man-in-the-middle) ด้วย ส่วนการโจมตีแบบโซลเดอร์เซิร์ฟฟิงก็สามารถทำได้เช่นเดียวกับรหัสผ่านรูปภาพระบบรีคอลล์เบสท์ แต่มีหลายรหัสผ่านรูปภาพหลายแบบในระบบนี้พยายามป้องกันการโจมตีแบบโซลเดอร์เซิร์ฟฟิงโดยการกระทำเพิ่มเติมลงไปในการเลือกรูปภาพรหัสผ่านแทนการเลือกรูปภาพด้วยเมาส์โดยตรง เช่นการพิมพ์ระบุตำแหน่งของรูปภาพแทน ในกรณีนี้ผู้โจมตีจำเป็นจะต้องใช้เวลาในการสังเกตุในการยืนยันตัวตนของผู้ใช้เป็นเวลานาน อย่างไรก็ตามการป้องกันการโจมตีแบบโซลเดอร์เซิร์ฟฟิงผู้ใช้จะใช้เวลาในการยืนยันตัวตนมากขึ้นและมีผลเสียกับการใช้งานของผู้ใช้

2.1.3 ระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ (Cued-recall graphical password systems)

รหัสผ่านรูปภาพระบบนี้ปกติแล้วจะให้ผู้ใช้จดจำตำแหน่งหรือจุดบนรูปภาพโดยใช้รูปภาพเป็นตัวช่วยในการจดจำรหัสผ่านซึ่งง่ายกว่าการจดจำของระบบรหัสผ่านรูปภาแบบรีคอลล์ ระบบนี้มักถูกเรียกว่าระบบโลซิเมตริค [6] (locimetric) เนื่องจากรหัสผ่านนั้นอ้างอิงจากตำแหน่งของรูปภาพโดยตรง จากงานวิจัยของฮอลลิงเวิร์ทและคณะ[16] พบว่าการจดจำเพียงจุดหรือตำแหน่งของรูปภาพ

นั้นง่ายและแม่นยำสำหรับผู้ใช้กว่าการจำทั้งรูปภาพอีกด้วย การจดจำแบบนี้เป็นผลดีกับเพียงผู้ใช้เท่านั้น ไม่มีผลต่อการคาดเดาของผู้โจมตี

1.) รหัสผ่านรูปภาพพาสพอยท์ (PassPoints) [17] : ระบบรหัสผ่านรูปภาพที่ถูกนำไปพัฒนาและศึกษาต่อมากที่สุดของระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ (รูปที่ 2.5) ก็คือรหัสผ่านรูปภาพระบบนี้ โดยมีวิธีการใช้คือการเลือกลำดับของจุดหรือตำแหน่งใดๆของรูปภาพจำนวน 5 จุดบนรูปภาพที่กำหนด สำหรับการเข้าสู่ระบบผู้ใช้จะต้องเลือกจุดดังกล่าวและเลือกตามลำดับอย่างถูกต้อง จำนวนรหัสผ่านของรหัสผ่านรูปภาพระบบนี้ขึ้นอยู่กับจำนวนจุดของรหัสผ่านและขนาดพื้นที่ของการกำหนดจุดยิ่งจุดเล็กยิ่งทำให้ผู้ใช้นั้นใช้งานยากขึ้นเช่นกัน โดยเฉลี่ยแล้ว จำนวนรหัสผ่านของระบบนี้อยู่ที่ประมาณ 43 บิต



รูปที่ 2.5 รหัสผ่านรูปภาพพาสพอยท์

วิเด็นเบ็คและคณะ [18] ทำการทดลองทดสอบความง่ายในการใช้ของระบบรหัสผ่านรูปภาพนี้พบว่าผู้ใช้ใช้เวลาในการสร้างรหัสผ่าน 64 วินาที และใช้เวลาในการเรียนรู้และจดจำรหัสผ่าน 171 วินาทีโดยเฉลี่ย ระยะเวลาในการเข้าสู่ระบบประมาณ 9 ถึง 19 วินาที อัตราความสำเร็จในการเข้าสู่ระบบนั้นมีกว้างถึงร้อยละ 55 ถึง 90 ขึ้นอยู่กับขนาดพื้นที่ของการกำหนดจุดรหัสผ่านซึ่งเป็นสาเหตุหลักที่ทำให้ผู้ใช้ล้มเหลวในการเข้าสู่ระบบ วิเด็นเบ็คจึงได้แนะนำขนาดพื้นที่ของการกำหนดจุดรหัสผ่านควรจะมีขนาดขั้นต่ำ 14 x 14 พิกเซล

เชียส์สันและคณะ [19] ได้ทำการวิจัยรหัสผ่านรูปภาพระบบนี้และพบว่าการเลือกรูปภาพนั้นมีผลต่อความง่ายในการใช้งาน และการจำรหัสผ่านรูปภาพของรหัสผ่านรูปภาพรหัสผ่านระบบนี้มากกว่าหนึ่งรหัสผ่านนั้นมีผลทำให้การจดจำรหัสผ่านนั้นแย่ลง บางงานวิจัยนั้นได้ระบุอีกด้วยว่าการจดจำรหัสผ่านมากกว่าหนึ่งรหัสผ่านของรหัสผ่านรูปภาพพาสพอยท์นั้นมีผลกระทบในการจดจำน้อยกว่าการจดจำรหัสผ่านตัวอักษรมากกว่าหนึ่งรหัสผ่านอีกด้วย [20] บีชัคคีและคณะ [21] นำรหัสผ่าน

รูปภาพระบบนี้ไปพัฒนาและประยุกต์ใช้เป็นมาสเตอร์พาสเวิร์ด (master password) บนเว็บเบราว์เซอร์และได้สรุปว่าการใช้รหัสผ่านรูปภาพระบบนี้มีการใช้งานที่ง่ายกว่าการใช้รหัสผ่านรูปภาพตัวอักษร

การโจมตีที่พบในรหัสผ่านรูปภาพระบบนี้ที่พบนอกเหนือจากระบบอื่นคือ การโจมตีด้วยฮอตสปอต [24, 32] ซึ่งเป็นการคาดเดารหัสผ่านจากจุดที่เด่นบนรูปภาพซึ่งสามารถนำข้อมูลจากการโจมตีประเภทนี้ไปทำการโจมตีแบบดิกชันนารีได้อีกด้วย นักวิจัยหลายคนพยายามป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิง เช่นรหัสผ่านรูปภาพของซูโอะ (Suo) [22] โดยนำการเลือกจุดโดยตรงจากภาพออกและใช้การโฟกัสที่บริเวณหนึ่งของรูปภาพและทำการเบลอส่วนที่เหลือออก หากส่วนที่ถูกโฟกัสนั้นคือรหัสผ่านของผู้ใช้ ผู้ใช้จะต้องพิมพ์ “Y” หากไม่ใช้ผู้ใช้จะต้องพิมพ์ “N” โดยจะทำอย่างต่อเนื่อง 10 รอบ การป้องกันป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิงประเภทนี้จะทำให้ผู้ใช้จะใช้เวลาในการเข้าสู่ระบบมากกว่าเดิม

2.) รหัสผ่านรูปภาพคิวด์คลิกพอยท์ [23] (Cued Click-Points) : รหัสผ่านรูปภาพระบบนี้ทำงานโดยให้ผู้ใช้เลือกหนึ่งจุดบนรูปภาพจากรูปภาพทั้งหมด 5 รูป และรูปภาพทั้งหมดนั้นจะถูดแสดงตามลำดับทุกครั้ง หากผู้ใช้เลือกรหัสผ่านที่ผิดระบบจะตอบสนองทันทีว่าผิดและบังคับให้เริ่มใหม่ตั้งแต่ภาพแรก จากการทดลองพบว่าผู้ใช้มีอัตราความสำเร็จในการเข้าสู่ระบบสูงถึงร้อยละ 96 โดยเฉลี่ยแล้วผู้ใช้ใช้เวลา 25 วินาทีในการสร้างรหัสผ่าน และใช้เวลา 7 วินาทีในการเข้าสู่ระบบ แต่การจำรหัสผ่านรูปภาพเป็นจำนวนหลายรูปนั้นมีผลกับความทรงจำระยะยาวของผู้ใช้เช่นกัน รหัสผ่านรูปภาพระบบนี้เป็นการจดจำจุดหรือพื้นที่บนรหัสผ่านหนึ่งจุดต่อหนึ่งรูปโดยต้องจำทั้งหมด

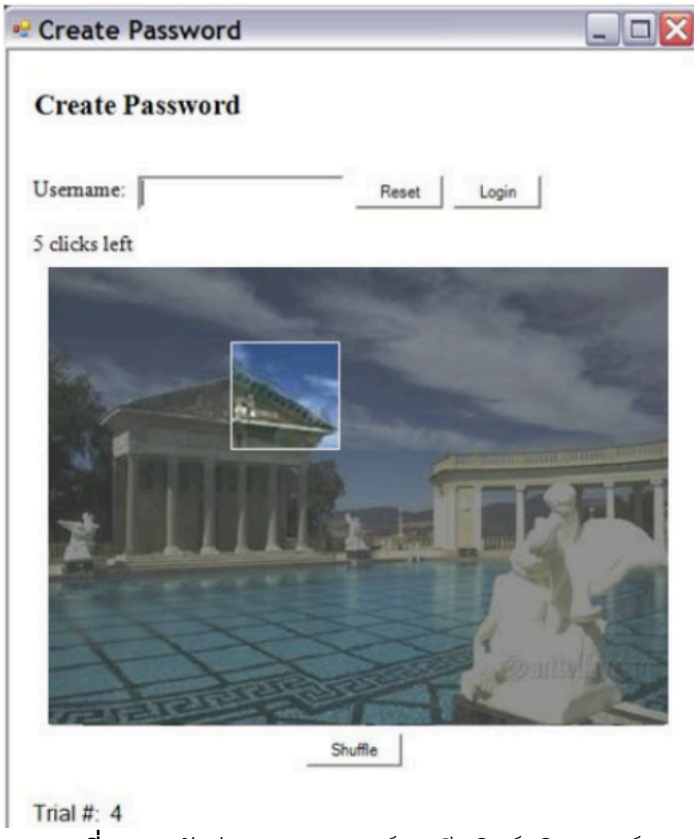
3.) รหัสผ่านรูปภาพเพอร์ซูเอซีฟคิวด์คลิกพอยท์ (Persuasive Cued Click-Points) [24] : เป็นระบบรหัสผ่านรูปภาพที่ถูกพัฒนาต่อมาจากระบบ cued click-points แต่มีการปรับปรุงความหลากหลายในการสร้างรหัสผ่านของผู้ใช้โดยระบบจะเลือกพื้นที่หนึ่งให้ผู้ใช้เลือกใช้เป็นรหัสผ่าน แต่ถ้าผู้ใช้ไม่พอใจกับพื้นที่ที่ระบบแนะนำนั้นผู้ใช้สามารถกดปุ่มเพื่อเปลี่ยนพื้นที่ได้ (รูปที่ 2.6) จากการทดลองอัตราความสำเร็จในการเข้าสู่ระบบนั้นมีเท่ากันกับระบบ cued click-points แต่ระยะเวลาในการสร้างรหัสผ่านนั้นเพิ่มขึ้นเป็น 50 วินาที โดยเฉลี่ย

การป้องกันต่อการโจมตีต่างๆของรหัสผ่านรูปภาพระบบนี้มีจุดที่สามารถโจมตีได้แบบเดียวกับ recognition-based คือ การโจมตีแบบโชลเดอร์เซิร์ฟฟิง มัลแวร์ และ ฟิชชิง การโจมตีแบบ โชลเดอร์เซิร์ฟฟิงนั้นผู้โจมตีหากทำการการสังเกตุเพียงครั้งเดียวก็อาจจะสามารถทำให้รหัสผ่านถูกเปิดเผยได้ทันที

2.2 การโจมตีบนระบบรหัสผ่านรูปภาพ

ในส่วนนี้จะกล่าวถึงการโจมตีต่างๆสำหรับรหัสผ่านรูปภาพโดยนำการโจมตีโดยทั่วไปของรหัสผ่านและเชื่อมโยงว่ามีความเกี่ยวข้องอย่างไรกับรหัสผ่านรูปภาพ การโจมตีจะถูกแบ่งเป็น การ

โจมตีแบบ บรูทฟอร์ซ (brute-force attacks) ดิกชันนารี (dictionary attacks) โชลเดอร์เซิร์ฟฟิง (shoulder-surfing attacks) มัลแวร์ (malware attacks) และ ฟิชชิง (phishing attacks)



รูปที่ 2.6 รหัสผ่านรูปภาพเพอร์ซูเอซีฟคิวด์คลิกพอยท์

2.2.1 การโจมตีแบบบรูทฟอร์ซ (Brute-force attacks หรือ Exhaustive-search attacks)

การโจมตีชนิดนี้เกิดจากการลองผิดลองถูกจากความเป็นไปได้ทั้งหมดของรหัสผ่านการโจมตีชนิดนี้รหัสผ่านตัวอักษรและรหัสผ่านรูปภาพมีวิธีการโจมตีที่เหมือนกัน การโจมตีชนิดนี้มีความเป็นไปได้น้อยที่จะสามารถแกะรหัสผ่านได้สำเร็จหากรหัสผ่านนั้นๆมีขนาดที่ใหญ่พอ การโจมตีแบบดิกชันนารีจึงเป็นที่นิยมมากกว่าสำหรับผู้โจมตี อย่างไรก็ตามการโจมตีชนิดนี้ในรหัสผ่านตัวอักษรถูกนำไปปรับปรุงเพื่อให้ทำงานได้รวดเร็วยิ่งขึ้น เช่น การเริ่มหารหัสผ่านที่มีความยาวน้อยก่อนและเพิ่มความยาวไปเรื่อยๆ [25] ตัวอย่างคือ การโจมตีจากรหัสผ่านความยาว 4 ตัวหากไม่เจอจึงเพิ่มเป็น 5, 6, 7 และเพิ่มไปเรื่อยๆจนกว่าจะเจอรรหัสผ่าน สำหรับการโจมตีแบบนี้สามารถทำการโจมตีบนระบบรหัสผ่านรูปภาพได้เช่นเดียวกัน เช่นการโจมตีบนรหัสผ่านรูปภาพดีเอเอส เริ่มจากการวาดรหัสผ่านด้วยเส้นที่สั้น แล้วทำการเพิ่มความยาวของเส้นไปเรื่อยๆแทน

ข้อดีของการโจมตีชนิดนี้แบบออฟไลน์ (exhaustive offline attacks) คือ หากมีเวลาในการโจมตีและเครื่องมือที่มีกำลังคำนวณที่มากพอจะทำให้รหัสผ่านถูกค้นพบได้อย่างแน่นอน แต่ในความ

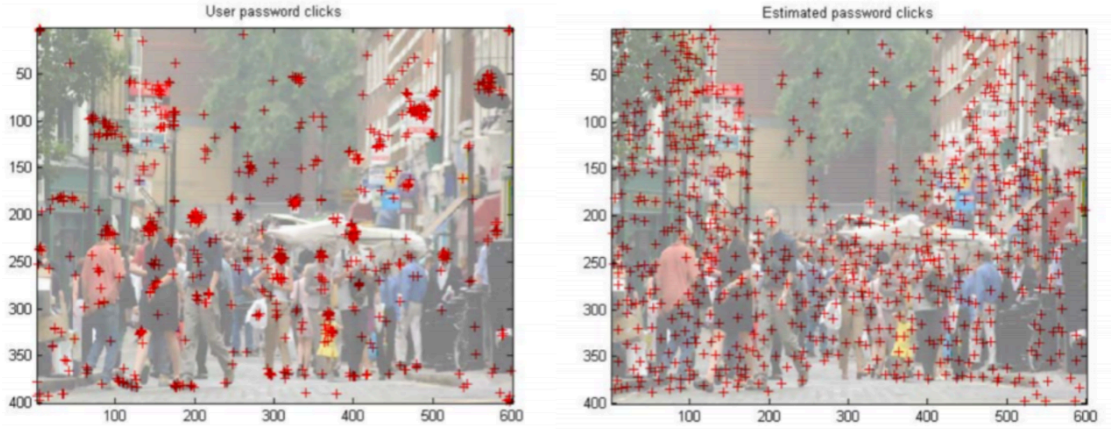
เป็นจริงแล้วถ้าจำนวนรหัสผ่านมีจำนวนที่เยอะมาก ผู้บุกรุกมักเลือกที่จะค้นหารหัสผ่านเพียงส่วนหนึ่งเท่านั้นเนื่องจากข้อจำกัดทางเวลาและกำลังในการคำนวณซึ่งไปการันตีว่าจะสามารถค้นหารหัสผ่านได้ เพราะฉนั้นหากต้องการหลีกเลี่ยงจากการโจมตีชนิดนี้ จำนวนรหัสผ่านควรจะมีจำนวนที่มากพอที่จะทำให้ผู้บุกรุกไม่สามารถทำการค้นหาทั้งหมดได้ (full-search) แต่ในระบบรหัสผ่านรูปภาพหลายระบบมี จำนวนรหัสผ่านที่น้อยมากโดยเฉพาะรหัสผ่านระบบรูปภาพแบบรีคอกนิชัน เช่น รหัสผ่านรูปภาพพาสเฟซที่มีขนาดเพียง 12 บิต หนึ่งในวิธีป้องกันการโจมตีชนิดนี้คือการจำกัดจำนวนครั้งในการป้อนรหัสผ่าน หรือ สามารถนำไปรวมกับการยืนยันตัวตนชนิดอื่น เช่น การยืนยันตัวตนสองขั้นตอน (two factor authentication) [26] ก็สามารถลดความเสี่ยงจากการโจมตีชนิดนี้ได้

2.2.2 การโจมตีแบบดิกชันนารี (Dictionary attacks)

การโจมตีแบบดิกชันนารีของรหัสผ่านรูปภาพนั้นสามารถทำได้แบบเดียวกับที่ทำบนรหัสผ่านตัวอักษร [28,29] การโจมตีชนิดนี้อาศัยความสามารถของโครงสร้างข้อมูล (data structure) ในการค้นหารหัสผ่านที่ทั้งหมดเป็นไปได้ (ซึ่งมีขนาดของการค้นหาเล็กมากเมื่อเทียบกับ การโจมตีแบบบรูทฟอร์ซ) จากนั้นจึงทำการป้อนรหัสผ่านที่ได้จากการค้นหาทั้งหมด โดยการโจมตีชนิดนี้มีความน่าจะเป็นและความเร็วในการค้นหารหัสผ่านสูงกว่าการโจมตีแบบบรูทฟอร์ซ

การที่มีจำนวนรหัสผ่าน (password space) ที่ใหญ่มากอาจจะสามารถป้องกันการโจมตีแบบ brute-force attacks ได้ แต่ไม่สามารถการันตีความปลอดภัยของรหัสผ่านในการโจมตีชนิดนี้ได้เลย จึงเป็นคำถามให้กับรหัสผ่านรูปภาพว่า การที่มีจำนวนรหัสผ่าน ที่ใหญ่มากนั้นไม่ได้แปลว่าปลอดภัย หากรหัสผ่านที่ผู้ใช้สร้างขึ้นนั้นถูกคาดเดาได้ง่าย (ซึ่งในส่วนของรหัสผ่านที่สามารถคาดเดาได้ถูกเรียกว่า “สับสเปซ (subspaces)” [29]) ในส่วนถัดไปจึงจะเป็นการวิเคราะห์การโจมตีชนิดนี้ของทุกระบบรหัสผ่านรูปภาพ

1.) การโจมตีแบบดิกชันนารีบนระบบรหัสผ่านรูปภาพแบบรีคอลล์ : จากการวิจัยความปลอดภัยของรหัสผ่านรูปภาพดีเอเอส และ รหัสผ่านรูปภาพพาสโก [29,30] ทำการค้นหาจำนวนรหัสผ่านที่แท้จริง (subspaces) ของระบบเหล่านี้จากการวาดเส้นรหัสผ่านของผู้ใช้พบว่าผู้ใช้ส่วนใหญ่จะวาดรหัสผ่านเป็นตัวอักษรขึ้นต้นของชื่อผู้ใช้ หรือ สัญลักษณ์ต่างๆที่ผู้ใช้ชื่นชอบ (ซึ่งไม่เป็นข้อมูลที่เป็นความลับ) ทำให้การโจมตีแบบดิกชันนารีของรหัสผ่านระบบนี้สามารถทำได้ง่ายและมีความเป็นไปได้ที่รหัสผ่านจะถูกเปิดเผยสูงกว่าการค้นหาทั้งหมด (full-search)



รูปที่ 2.7 เครื่องมือวิเคราะห์รูปภาพอัตโนมัติเพื่อค้นหาฮอตสปอตบนรูปภาพโดย ดีริคและคณะ

2.) การโจมตีแบบดิกชันนารีบนระบบรหัสผ่านรูปภาพแบบรีคอกนิชัน : การวิเคราะห์ความปลอดภัยของการโจมตีแบบดิกชันนารีของรหัสผ่านรูปภาพระบบนี้ถูกทำบนรหัสผ่านรูปภาพพาสเฟซ และ รหัสผ่านรูปภาพสตอรี่ซิสเต็ม [14] โดยทำการจัดเตรียมชุดข้อมูล (data set) ของรหัสผ่านโดย 80% เป็นรูปภาพจริงที่ผู้ใช้เลือกเป็นรหัสผ่านและ 20% เป็นรหัสผ่านที่ระบบจัดเตรียมไว้ให้ สำหรับรูปภาพใบหน้าพบว่าผู้ใช้มักเลือกรูปภาพที่ตรงกันกับเชื้อชาติของตนเอง (เช่น คนเอเชีย, คนตะวันตก, คนผิวสี) หากผู้โจมตีรู้ลักษณะเชื้อชาติของผู้ใช้นั้นก็อาจจะมีความเสี่ยงในการเปิดเผยรหัสผ่านได้ เพศของผู้ใช้ก็เป็นปัจจัยในการเลือกรหัสผ่านใบหน้าเพศเดียวกันเช่นกัน

3.) การโจมตีแบบดิกชันนารีบนระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ : รหัสผ่านรูปภาพพาสพอยท์ถูกจับตามองมากที่สุดสำหรับการโจมตีชนิดนี้โดยมีปัจจัยสำคัญคือ ฮอตสปอต (hotspots) [24,32] คือจุดหรือพื้นที่ของรูปภาพที่โดดเด่นและผู้ใช้มักเลือกเป็นรหัสผ่านรูปภาพ ตัวช่วยเครื่องมือวิเคราะห์รูปภาพอัตโนมัติ (automated image processing tools) ถูกสร้างมาเพื่อช่วยค้นหาฮอตสปอต บนรูปภาพโดยเฉพาะโดยดีริคและคณะ [31] (รูปที่ 2.7) จากการสังเคราะห์ข้อมูลของรูปภาพเพื่อค้นหาฮอตสปอตมาประกอบทำการโจมตีแบบดิกชันนารี ทำให้โอกาสที่รหัสผ่านจะถูกเปิดเผยนั้นมีมาก จากข้อมูลข้างต้นของการโจมตีแบบดิกชันนารี ของรหัสผ่านรูปภาพนั้นผู้โจมตีจะต้องใช้ความพยายามมากว่าการโจมตีแบบดิกชันนบนรหัสผ่านตัวอักษรเนื่องจากแต่ละระบบรหัสผ่านรูปภาพนั้นต้องการอัลกอริทึมและชุดข้อมูลที่แตกต่างกันออกไปจากรหัสผ่านตัวอักษร

2.2.3 การโจมตีแบบโชลเดอร์เซิร์ฟฟิง (Shoulder-surfing attacks)

การโจมตีแบบโชลเดอร์เซิร์ฟฟิง [32-34] คือการโจมตีด้วยการสังเกตุการป้อนข้อมูลรหัสผ่านระหว่างที่ผู้ใช้กำลังยืนยันตัวตนจากด้านหลังหรือด้านข้าง การสังเกตุนั้นสามารถทำได้โดยการเพ่งมองโดยตรงหรือการบันทึกวีดีโอ กล้องวีดีโอความละเอียดสูงเป็นอันตรายอย่างมากหากวีดีโอสามารถแสดงให้เห็นถึงจุดหรือเส้นที่ผู้ใช้ใช้เป็นรหัสผ่าน รหัสผ่านรูปภาพหลายระบบพยายามจะป้องกันการ

จมตีชนิดนี้แต่ต้องแลกมากับความยุ่งยากในการใช้ของระบบนั้นๆ [35] ผลลัพธุ์คือผู้ใช้ไม่สามารถใช้ระบบนั้นเป็นการยืนยันตัวตนในชีวิตประจำวันได้

รูปที่ 2.8 ตัวอย่างการโจมตีแบบโซลเดอร์เซิร์ฟฟิง

2.2.4 การโจมตีแบบมัลแวร์ (Malware attacks)

การติดตั้งซอฟต์แวร์ที่ไม่ได้รับการอนุญาตให้ใช้งาน (unauthorized) นั้นมักจะมีโอกาสในการโดนฝัง มัลแวร์ (malware) โทรจัน (trojans) ไวรัส (viruses) และ เวิร์ม (worms) หรือบางครั้งอาจฝังไว้กับหน้าเว็บไซต์ (บนจาวาสคริป์ หรือ แฟลชคอมโพเนนท์) [36] โดยจะมีการแอบบันทึกกิจกรรมต่างๆของผู้ใช้ได้ เช่น การบันทึกรูปแบบการพิมพ์ (Keystroke-loggers) เป็นการแอบบันทึกการใช้งานคีย์บอร์ดของผู้ใช้ การบันทึกรูปแบบการใช้เมาส์ (mouse-loggers) และ การบันทึกหน้าจอ (screen scrappers) แอบบันทึกความเคลื่อนไหวของหน้าจอผู้ใช้ สำหรับรหัสผ่านตัวอักษรนั้นการใช้คีย์สโตรคลอกเกอร์ก็เพียงพอต่อการเปิดเผยรหัสผ่านของผู้ใช้แต่รหัสผ่านรูปภาพนั้นผู้โจมตีต้องอาศัยการรวมกันของการบันทึกหน้าจอ กับการบันทึกรูปแบบการใช้เมาส์ หรือ การบันทึกหน้าจอ กับ การบันทึกรูปแบบการพิมพ์ เพราะผู้โจมตีจำเป็นต้องเห็นหน้าจอของผู้ใช้ว่ากำลังป้อนข้อมูลรหัสผ่านบนจุดใดของหน้าจอ

2.2.5 การโจมตีแบบฟิชชิง (Phishing attacks)

การโจมตีชนิดนี้ [37] ผู้โจมตีจะสร้างหน้าเว็บไซต์ปลอมโดยการคัดลอกจากเว็บไซต์เพื่อหลอกให้ผู้ใช้กรอกข้อมูลรหัสผ่าน ตัวอย่างเช่นแนบที่อยู่ของเว็บไซต์ปลอมไปกับอีเมลล์ แต่สำหรับการสร้างเว็บไซต์ปลอมสำหรับกรอกข้อมูล ระบบรหัสผ่านรูปภาพแบบรีคอกนิชันและรีคอลล์นั้นผู้โจมตีจำเป็นต้องรู้ชุดรูปภาพของรหัสผ่านบนเว็บไซต์จริงก่อน ผู้โจมตีจึงต้องทำการโจมตีแบบแมนอินเดอะมิดเดิลระหว่างเว็บไซต์จริงและผู้ใช้ และนำข้อมูลรูปภาพรหัสผ่านบนเว็บไซต์จริงมาแสดงผลบน

เว็บไซต์ปลอมแบบเรียลไทม์แล้วจึงนำข้อมูลรหัสผ่านที่ผู้ใช้กรอกลงบนเว็บไซต์ปลอมไปกรอกบนเว็บไซต์จริง ซึ่งถือเป็นการโจมตีที่ต้องอาศัยความพยายามมากสำหรับผู้โจมตี

2.3 แบบสอบถามความง่ายในการใช้งานพีเอสเอสยูคิว (PSSUQ)

พีเอสเอสยูคิว [38] คือแบบสอบถามเพื่อใช้ในการประเมินความง่ายในการใช้งานและความพึงพอใจที่มีต่อระบบซึ่งถูกพัฒนาโดยบริษัทไอบีเอ็ม แบบสอบถามความง่ายในการใช้งานนี้ประกอบไปด้วยคำถามสำหรับการใช้งาน 19 ข้อ โดยมี 5 วัตถุประสงค์ในการชี้วัดคือ ความรวดเร็วในการใช้งาน ความง่ายในการเรียนรู้ คุณภาพของข้อมูล ความครบถ้วนของคุณสมบัติในการใช้งาน และ ความรวดเร็วในการทำความคุ้นเคยของการใช้งาน คำถามเหล่านี้ถูกแบ่งเป็น 4 หมวดหมู่ย่อยคือ ประโยชน์ในการใช้งานของระบบ (SysUse) คุณภาพในการแสดงผลข้อมูลของระบบ (InfoQual) ส่วนติดต่อระหว่างผู้ใช้และระบบ (InterQual) และ ความพึงพอใจโดยรวมต่อระบบ (Overall) ซึ่งมีเกณฑ์การให้คะแนนจากหนึ่งถึงเจ็ด โดยหนึ่งคือไม่เห็นด้วยที่สุดและเจ็ดคือ เห็นด้วยที่สุด คำถามทั้ง 19 มีดังนี้

1.) โดยภาพรวมฉันพึงพอใจต่อความง่ายในการใช้งานของระบบนี้ (Overall, I am satisfied with how easy to use this system)
2.) ฉันสามารถใช้งานได้อย่างง่ายดาย (It was simple to use this system)
3.) ฉันสามารถใช้งานระบบนี้ได้ทุกคุณสมบัติอย่างมีประสิทธิผล (I could effectively complete the tasks and scenarios using this system)
4.) ฉันสามารถใช้งานระบบนี้ได้ทุกคุณสมบัติอย่างรวดเร็ว (I was able to complete tasks and scenarios quickly using this system)
5.) ฉันสามารถใช้งานระบบนี้ได้ทุกคุณสมบัติอย่างมีประสิทธิภาพ (I was able to efficiently complete the tasks and scenarios using this system)
6.) ฉันรู้สึกสะดวกสบายในการใช้งานระบบนี้ (I felt comfortable using this system)
7.) ฉันสามารถเรียนรู้ระบบนี้ได้อย่างง่ายดาย (It was easy to learn to use this system)
8.) ฉันเชื่อว่าฉันสามารถใช้งานระบบนี้ได้เต็มประสิทธิภาพโดยเร็ว (I believe I could become productive quickly using this system)
9.) เมื่อระบบเกิดข้อผิดพลาดระบบสามารถให้ข้อมูลในการแก้ปัญหาอย่างชัดเจน (The system gave error messages that clearly told me how to fix problems)
10.) เมื่อฉันทำผิดพลาดต่อระบบ ฉันสามารถกู้คืนความผิดพลาดได้อย่างรวดเร็ว (Whenever I made mistake using this system, I could recover easily and quickly)
11.) ข้อมูลของระบบมีการแสดงผลที่ชัดเจน (The information provided with this system was clear)
12.) ฉันสามารถหาข้อมูลที่ต้องการได้อย่างง่ายดาย (It was easy to find information I needed)

13.) ข้อมูลของระบบสามารถเข้าใจได้อย่างง่ายดาย (The information provided for the system was easy to understand)

14.) ข้อมูลของระบบทำให้ให้ฉันสามารถใช้ระบบได้ครบถ้วนทุกคุณสมบัติ (The information was effective in helping me complete the tasks and scenarios)

15.) การจัดการข้อมูลในการแสดงผลมีความชัดเจน (The organization of information on the system screens was clear)

16.) อินเตอร์เฟซของระบบมีความสวยงาม (The interface of this systems was pleasant)

17.) ฉันชอบใช้อินเตอร์เฟซของระบบ (I liked using the interface of this system)

18.) ระบบมีคุณสมบัติครบถ้วนตามที่คาดหวังไว้ (The system has all the functions and capabilities I expect it to have)

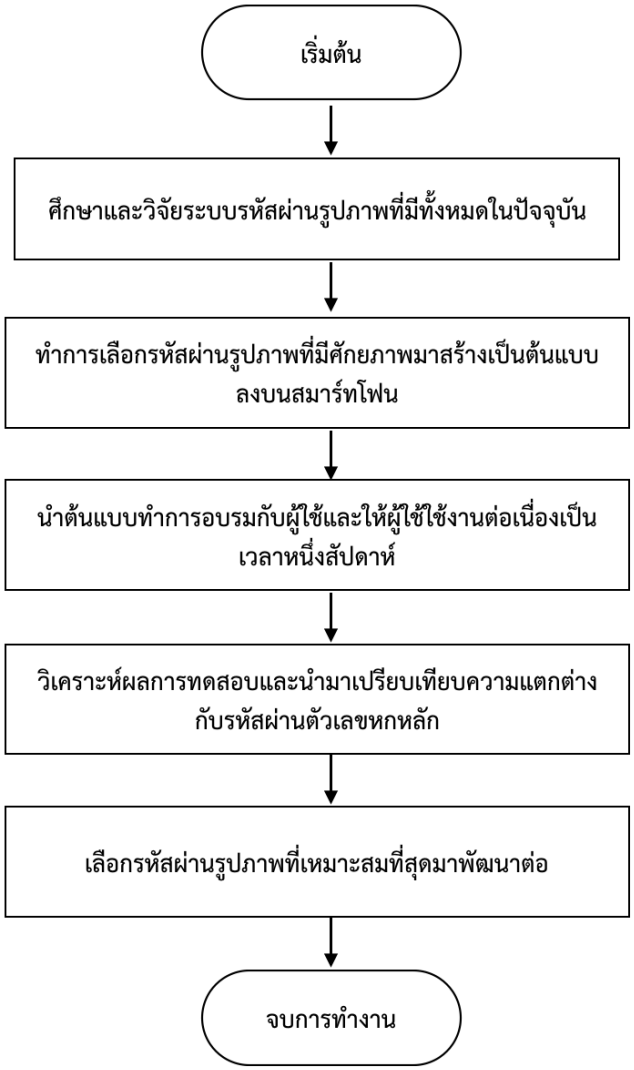
19.) โดยรวมฉันพึงพอใจต่อระบบ (Overall, I am satisfied with this system)

บทที่ 3
วิธีการดำเนินงานวิจัย

งานวิจัยนี้มีวัตถุประสงค์ในการพัฒนารหัสผ่านรูปภาพบนสมาร์ทโฟนที่ใช้งานได้ง่าย และมีความปลอดภัย โดยแบ่งวิธีดำเนินงานวิจัยเป็นสองส่วน คือ ส่วนที่หนึ่งคือการทดสอบสมมติฐานเรื่องความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพจะเพิ่มมากขึ้นเมื่อทำการอบรมและใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ โดยทำการทดสอบกับรหัสผ่านรูปภาพพาสเฟซ พาสโก และ พาสพอยท์ หลังจากนั้นนำผลการทดสอบมาทำการวิเคราะห์เพื่อหารหัสผ่านรูปภาพที่มีความเหมาะสมเพื่อนำไปพัฒนารหัสผ่านรูปภาพใหม่ที่มีความปลอดภัยสูง มีความง่ายในการจำ และมีความง่ายในการใช้งานในส่วนที่สอง

3.1 การทดสอบสมมติฐานเรื่องความง่ายในการใช้งาน

การทดสอบสมมติฐานเรื่องความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพบนสมาร์ทโฟนจะเพิ่มมากขึ้นเมื่อทำการอบรมและใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ มีขั้นตอนดังรูปที่ 3.1 โดยผู้วิจัยได้ทำการศึกษาระบบรหัสผ่านรูปภาพทั้ง 3 ระบบคือ ระบบรหัสผ่านรูปภาพแบบรีคอลล์ ระบบรหัสผ่านรูปภาพแบบรีคอกนิชัน และ ระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ จากนั้นผู้วิจัยเลือกระบบรหัสผ่านรูปภาพมาอย่างละ 1 ระบบ รหัสผ่านรูปภาพแบบรีคอลล์ ผู้วิจัยเลือกรหัสผ่านรูปภาพพาสโกเนื่องจากมีจำนวนรหัสผ่านที่สูงกว่า รหัสผ่านรูปภาพดีเอเอส และรหัสผ่านรูปภาพบีดีเอเอส นอกจากนั้นรหัสผ่านรูปภาพดีเอเอส และบีดีเอเอสนั้นมีปัญหาในการใช้งานที่ต้องวาดเส้นรหัสผ่านให้เหมือนกับรหัสผ่านที่สร้าง ทำให้อัตราความสำเร็จในการเข้าสู่ระบบนั้นมีต่ำมาก สำหรับระบบรหัสผ่านรูปภาพรีคอกนิชัน ผู้วิจัยเลือกรหัสผ่านรูปภาพพาสเฟซเนื่องจากรหัสผ่านรูปภาพสตอรีซิสเต็ม ผู้ใช้มักผิดพลาดในการเรียงลำดับของภาพทำให้อัตราความสำเร็จในการเข้าสู่ระบบและระยะเวลาในการเข้าสู่ระบบแย่กว่ารหัสผ่านรูปภาพพาสเฟซ ส่วนรหัสผ่านรูปภาพเดจาวูเนื่องจากเป็นภาพศิลปะซึ่งระบุเอกลักษณ์ของรูปภาพได้ยากผู้ใช้จึงต้องใช้ระยะเวลาในการค้นหารูปภาพเป็นเวลานาน ทำให้ระยะเวลาในการเข้าสู่ระบบใช้เวลานานมาก และสุดท้ายระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ ผู้วิจัยเลือกรหัสผ่านรูปภาพพาสพอยท์ เพราะการจดจำจุดหรือพื้นที่บนรหัสผ่านของรหัสผ่านรูปภาพซีซีพี และ รหัสผ่านรูปภาพพีซีซีพี หนึ่งจุดต่อหนึ่งรูปโดยต้องจำทั้งหมดห้ารูปมีความยากในการจดจำมากกว่าการจดจำหลายจุดหรือพื้นที่ในหนึ่งรูปของพาสพอยท์ จากนั้นผู้วิจัยจะทำการทดสอบความง่ายในการใช้งานเป็นเวลาหนึ่งสัปดาห์แล้วเปรียบเทียบผลการทดสอบระหว่างก่อนทำการทดสอบและหลังทำการทดสอบ และหลังจากการทดสอบนี้ผู้ใช้จะทำการวิเคราะห์เพื่อทำการเลือกระบบรหัสผ่านที่เหมาะสมที่สุดมาพัฒนาเป็นระบบรหัสผ่านรูปภาพใหม่



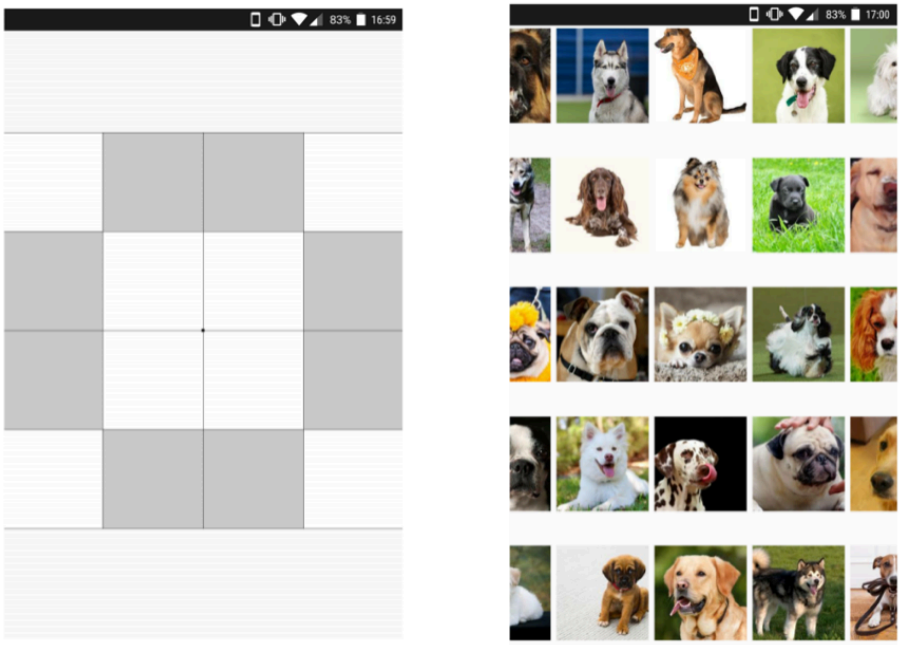
รูปที่ 3.1 ขั้นตอนการทดสอบสมมติฐานเรื่องความง่ายในการใช้งาน

3.1.1 การพัฒนาต้นแบบของรหัสผ่านรูปภาพเพื่อทำการทดสอบ

ผู้วิจัยได้พัฒนาต้นแบบเป็นแอปพลิเคชันบนระบบปฏิบัติการแอนดรอยด์โดยทำการปรับปรุงระบบรหัสผ่านรูปภาพพาสโก พาสเฟซและพาสพอยท์ให้เหมาะสมกับการใช้งานบนสมาร์ทโฟนขนาดหน้าจอ 4.5 ถึง 5.5 นิ้ว และสามารถเปรียบเทียบได้ง่าย โดยมีเงื่อนไขคือต้องมีความแข็งแรงของรหัสผ่านมากกว่ารหัสผ่านแบบตัวเลขหกหลักซึ่งมีขนาด 20 บิต และรหัสผ่านรูปภาพที่ถูกเลือกมาจะต้องปรับปรุงให้มีขนาดที่ไม่ต่างกันเกินไป

1.) การตั้งค่าและปรับปรุงรหัสผ่านรูปภาพพาสโก : เนื่องจากหน้าจอของสมาร์ทโฟนมีจอขนาดเล็กกว่าหน้าจอของคอมพิวเตอร์ผู้วิจัยจึงปรับขนาดของขนาดตารางสองมิติจาก 9 x 9 เหลือ 5 x 5 จำนวนรหัสผ่านหลังจากปรับขนาดของตารางสองมิติแล้วเท่ากับ 28 บิต ซึ่งมีขนาดเทียบเท่ากับรหัสผ่านตัวอักษร 6 ตัวที่มีตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ และ ตัวเลข

2.) การตั้งค่าและปรับปรุงรหัสผ่านรูปภาพพาสเฟซ : โดยปกติแล้วรหัสผ่านระบบนี้ใช้การเลือกรหัสผ่าน 1 รูป จากรูปภาพทั้งหมด 9 รูป จำนวน 4 รอบต่อการเข้าสู่ระบบหนึ่งครั้งซึ่งมีขนาดของ จำนวนรหัสผ่านคือ 6561 หรือ 13 บิต ผู้วิจัยจึงทำการตั้งค่าโดยให้เลือก 1 รูป จากทั้งหมด 50 รูป จำนวน 5 รอบต่อการเข้าสู่ระบบหนึ่งครั้งทำให้ จำนวนรหัสผ่านมีขนาดเป็น 28 บิต (50^5) นอกจากนี้ผู้วิจัยได้ทำการใช้ใบหน้าของสุนัขแทนใบหน้าของใบหน้าของมนุษย์เพื่อเพิ่มความหลากหลายในการเลือกรูปภาพ



รูปที่ 3.2 รหัสผ่านรูปภาที่ถูกปรับปรุงบนสมาร์ทโฟน
ด้านซ้าย แสดง รหัสผ่านรูปภาพพาสโก
ด้านขวา แสดง รหัสผ่านรูปภาพพาสเฟซ

3.) การตั้งค่าและปรับปรุงของผ่านรูปภาพพาสพอยท์ : สำหรับรหัสผ่านรูปภาพนี้เดิมทีมีขนาดของจำนวนรหัสผ่านประมาณ 43 บิต แต่การใช้งานของรหัสผ่านรูปภาพนี้ปกติแล้วจะทำการเลือกรหัสผ่านโดยใช้เมาส์ซึ่งทำให้พื้นที่ของการเลือกจุดหรือพื้นที่นั้นเล็กมาก เนื่องจากการใช้งานบนสมาร์ทโฟนนั้นใช้นิ้วมือในการเลือกรหัสผ่านทางผู้วิจัยจึงได้ขยายขนาดของพื้นที่ในการเลือกรหัสผ่านให้เหมาะสมกับนิ้วมือมนุษย์ แต่ทำให้ขนาดของจำนวนรหัสผ่านลดลงเหลือ 29 บิต (60^5)

3.1.2 การดำเนินการทดสอบ

ผู้วิจัยได้ทำการทดสอบกับกลุ่มตัวอย่าง 40 คน โดยเป็นกลุ่มคนที่ใช้สมาร์ทโฟนในชีวิตประจำวัน มีช่วงอายุอยู่ที่ 23 ถึง 35 ปี แบ่งเป็นเพศหญิง 16 คน และ เพศชาย 24 คน ในการทดสอบครั้งแรกผู้ทดสอบทุกคนจะได้รับคำอธิบายขั้นตอนการใช้งานรหัสเกี่ยวกับระบบรหัสผ่านรูปภาพที่ผู้วิจัยได้

เตรียมไว้ให้เข้าใจ หลังจากนั้นผู้ทดสอบจะทำการสร้างรหัสผ่านในแต่ระบบและทำการทดลองการเข้าสู่ระบบโดยผู้วิจัยจะเฝ้าสังเกตุและให้คำแนะนำทันทีหากผู้ทดสอบเกิดข้อสงสัยหรือข้อผิดพลาด เมื่อผู้ทดสอบทุกคนมีความเข้าใจในการใช้งานเป็นอย่างดีแล้ว ในทุกวันหลังเลิกงานผู้ทดสอบจะต้องเข้าสู่ระบบด้วยรหัสผ่านรูปภาพทั้งสามระบบเป็นเวลาติดต่อกันหนึ่งสัปดาห์ สำหรับการทดสอบรหัสผ่านตัวเลขหกหลักทำการทดสอบเฉพาะในวันแรกและวันสุดท้ายเท่านั้นเนื่องจากผู้ทดสอบคุ้นเคยกับการใช้รหัสผ่านตัวเลขอยู่แล้ว

ผู้วิจัยได้ทำการเก็บข้อมูลของผู้ทดสอบเพื่อเปรียบเทียบและศึกษาความง่ายในการใช้งานของทั้งสามระบบรหัสผ่านรูปภาพ และระบบรหัสผ่านตัวเลขในวันแรกและวันสุดท้ายของการทดสอบโดยใช้เกณฑ์ในการวัดคือ อัตราความล้มเหลวซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด (error rate of clicking incorrect points) จำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ (number of attempts required for successful authentication) ระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จ (login time required in a successful authentication) และ แบบสำรวจความยากในการใช้งานของระบบโดยใช้แบบสอบถามความง่ายในการใช้งานพีเอสเอสยูคิว โดยผู้วิจัยได้นำการผลการทดสอบมาค้นหาค่าความแตกต่างโดยใช้การทดสอบที (t-test) เพื่อวัดนัยสำคัญของความเปลี่ยนแปลงจากวันแรกถึงวันสุดท้ายของการทดสอบ

3.1.3 ผลการทดสอบอัตราความผิดพลาดซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด

อัตราความล้มเหลวซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด (ตารางที่ 3.1) คำนวณจากจำนวนครั้งที่ผู้ใช้เลือกรหัสผ่านผิดกับจำนวนครั้งที่ผู้ทดสอบทำการเลือกรหัสผ่านทั้งหมด โดยคิดเป็นอัตราเฉลี่ยร้อยละของผู้ทดสอบทั้งหมด ผลการทดสอบจากค่าเฉลี่ยของวันสุดท้ายพบว่ารหัสผ่านรูปภาพที่มีอัตราความผิดพลาดน้อยที่สุดคือรหัสผ่านรูปภาพพาสเฟซคือ ร้อยละ 3.686 ซึ่งมีผลลัพธ์ใกล้เคียงกับรหัสผ่านตัวเลขคือ ร้อยละ 0 ตามมาด้วยรหัสผ่านรูปภาพพาสโกคือ ร้อยละ 6.105 และรหัสผ่านรูปภาพพาสพอยท์คือ 13.855 จากการทดสอบทีพบว่าอัตราความผิดพลาดของรหัสผ่านรูปภาพทั้ง 3 ระบบ และรหัสผ่านตัวเลขหกหลักนั้นมีผลลัพธ์ไปในทางที่ดีขึ้นระหว่างวันแรกและวันสุดท้ายโดยมีความแตกต่างอย่างมีนัยสำคัญทั้งหมดโดยรหัสผ่านรูปภาพพาสเฟซ P น้อยกว่า 0.0001 รหัสผ่านรูปภาพพาสโก P เท่ากับ 0.002 รหัสผ่านรูปภาพพาสพอยท์ P เท่ากับ 0.006 และรหัสผ่านตัวเลขหกหลัก P เท่ากับ 0.0051

3.1.4 ผลการทดสอบจำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ

ตารางที่ 3.2 แสดงผลการทดสอบจำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จจากผู้ทดสอบทั้งหมด ผลการทดสอบจากค่าเฉลี่ยของวันสุดท้ายพบว่ารหัสผ่านตัวเลขหกหลังมีผลลัพธ์ที่ดีที่สุดคือ 1 ครั้ง ตามมาด้วยรหัสผ่านรูปภาพพาสเฟสคือ 1.194 ครั้ง ตามมาด้วยรหัสผ่านรูปภาพพาสโก 1.355 ครั้ง และ รหัสผ่านรูปภาพพาสเฟซ 1.387 ครั้ง จากการทดสอบทีพบว่าจำนวนครั้งของการ

พยายามล็อกอินจนเข้าสู่ระบบสำเร็จรูปภาพทั้ง 3 ระบบ ผลลัพธ์ไปในทางที่ดีขึ้นระหว่างวันแรกและวันสุดท้ายโดยมีความแตกต่างอย่างมีนัยสำคัญ โดยรหัสผ่านรูปภาพพาสโก P เท่ากับ 0.0013 รหัสผ่านรูปภาพพาสเฟซ P เท่ากับ 0.0014 รหัสผ่านรูปภาพพาสพอยท์ P เท่ากับ 0.0075 แต่รหัสผ่านตัวเลขหกหลักนั้นมีทั้งหมดมีการเปลี่ยนแปลงอย่างไม่มีนัยสำคัญโดยมีค่า P เท่ากับ 0.0425

ตารางที่ 3.1 ตารางผลการทดสอบอัตราความล้มเหลวซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด (ร้อยละ)

	วันที่ทดสอบ	ค่าเฉลี่ย (Mean)	ผลการทดสอบที (t-test)	ส่วนเบี่ยงเบนมาตรฐาน (SD)	ค่าต่ำสุด (Min)	ค่าสูงสุด (Max)
รหัสผ่านตัวเลขหกหลัก	วันแรก	3.224	t = 2.9010 P = 0.0051	6.069	0.00	14.28
	วันสุดท้าย	0.000		0.000	0.00	0.00
รหัสผ่านรูปภาพพาสโก	วันแรก	24.444	t = 4.0100 P = 0.0020	23.428	0.00	70.00
	วันสุดท้าย	6.105		8.852	0.00	25.00
รหัสผ่านรูปภาพพาสพอยท์	วันแรก	28.280	t = 2.8520 P = 0.0060	23.930	0.00	73.33
	วันสุดท้าย	13.855		13.952	0.00	42.85
รหัสผ่านรูปภาพพาสเฟซ	วันแรก	18.980	t = 4.3870 P < 0.0001	17.741	0.00	55.26
	วันสุดท้าย	3.686		7.708	0.00	20.00

ตารางที่ 3.2 ตารางผลการทดสอบจำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ (ครั้ง)

	วันที่ทดสอบ	ค่าเฉลี่ย (Mean)	ผลการทดสอบที (t-test)	ส่วนเบี่ยงเบนมาตรฐาน (SD)	ค่าต่ำสุด (Min)	ค่าสูงสุด (Max)
รหัสผ่านตัวเลขหกหลัก	วันแรก	1.611	t = 2.0730 P = 0.0425	0.374	1	2
	วันสุดท้าย	1.000		0.000	1	1
รหัสผ่านรูปภาพพาสโก	วันแรก	2.355	t = 3.392 P = 0.0013	1.539	1	6
	วันสุดท้าย	1.355		0.486	1	2
รหัสผ่านรูปภาพพาสพอยท์	วันแรก	1.935	t = 2.772 P = 0.075	0.964	1	5
	วันสุดท้าย	1.387		0.495	1	3
รหัสผ่านรูปภาพพาสเฟซ	วันแรก	1.709	t = 3.361 P = 0.0014	0.740	1	4
	วันสุดท้าย	1.194		0.401	1	2

3.1.5 ผลการทดสอบระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จ

ตารางที่ 3.3 แสดงผลทดสอบระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จของระบบรหัสผ่านรูปภาพจากผู้ทดสอบทั้งหมด จากค่าเฉลี่ยของวันสุดท้ายพบว่ารหัสผ่านรูปภาพพาสโกใช้ระยะเวลาในการเข้าสู่ระบบที่เร็วที่สุดคือ 4.344 วินาที ตามาด้วยรหัสผ่านตัวเลขหกหลักคือ 4.296 วินาที ตามมาด้วยรหัสผ่านรูปภาพพาสพอยท์คือ 4.389 วินาที และ รหัสผ่านรูปภาพพาสเฟซคือ 15.088 วินาที จากการทดสอบทีพบว่าระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จของรหัสผ่านรูปภาพทั้ง 3 ระบบ

ผลลัพธ์ไปในทางที่ดีขึ้นระหว่างวันแรกและวันสุดท้ายโดยมีความแตกต่างอย่างมีนัยสำคัญ โดยรหัสผ่านรูปภาพพาสเฟซ พาสโก และพาสพอยท์ มีค่า P น้อยกว่า 0.0001 แต่รหัสผ่านตัวเลขหกหลักนั้นมีทั้งหมดมีการเปลี่ยนแปลงอย่างไม่มีนัยสำคัญโดยมีค่า P เท่ากับ 0.5

ตารางที่ 3.3 ตารางผลการทดสอบระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จ (วินาที)

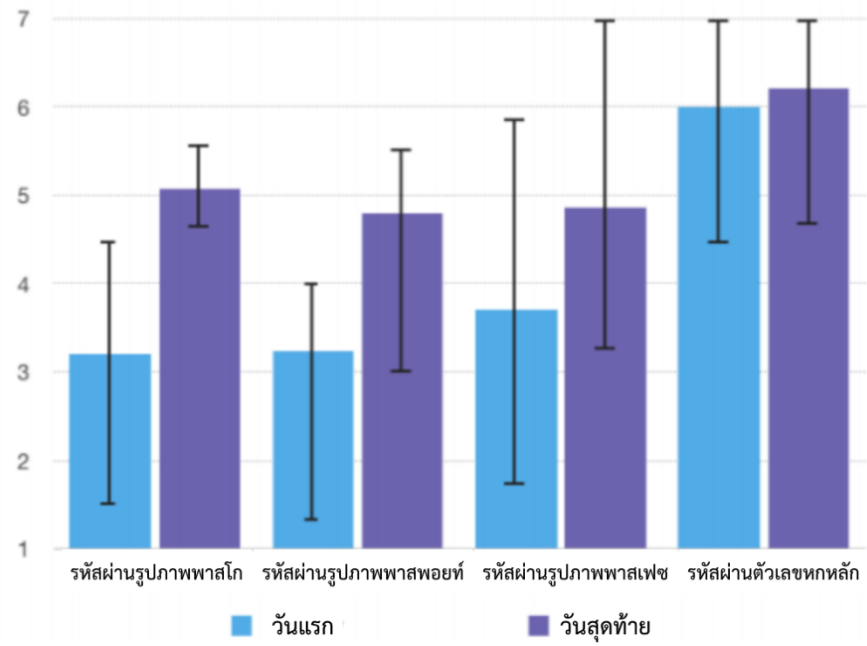
	วันที่ทดสอบ	ค่าเฉลี่ย (Mean)	ผลการทดสอบที (t-test)	ส่วนเบี่ยงเบนมาตรฐาน (SD)	ค่าต่ำสุด (Min)	ค่าสูงสุด (Max)
รหัสผ่านตัวเลขหกหลัก	วันแรก	4.677	t = 0.6590 P = 0.5000	1.911	1.78	9.93
	วันสุดท้าย	4.344		1.923	1.37	8.39
รหัสผ่านรูปภาพพาสโก	วันแรก	19.305	t = 6.6120 P < 0.0001	12.258	5.14	48.51
	วันสุดท้าย	4.296		2.076	1.80	10.21
รหัสผ่านรูปภาพพาสพอยท์	วันแรก	10.916	t = 6.2560 P < 0.0001	5.261	2.28	20.39
	วันสุดท้าย	4.389		2.0165	1.30	8.71
รหัสผ่านรูปภาพพาสเฟซ	วันแรก	28.755	t = 4.5470 P < 0.0001	15.611	12.07	71.37
	วันสุดท้าย	15.088		5.074	7.51	25.74

3.1.6 ผลการทดสอบความง่ายในการใช้งานด้วยแบบทดสอบพีเอสเอสยูคิว

ทางผู้วิจัยได้ทำการทดสอบความง่ายในการใช้งานด้วยแบบสำรวจพีเอสเอสยูคิว ซึ่งมีคำถามทั้งหมด 19 ข้อ มีเกณฑ์การให้คะแนนโดย 1 คือ ไม่เห็นด้วยที่สุดและ 7 คือ เห็นด้วยที่สุด รูปที่ 3.3 แสดงผลการทดสอบโดยเฉลี่ยของระบบรหัสผ่านรูปภาพทั้งหมดรวมถึงรหัสผ่านตัวเลขหกหลัก พบว่าระบบรหัสผ่านรูปภาพทุกระบบเมื่อเปรียบเทียบจากวันแรกและวันสุดท้ายมีผลลัพธ์ที่ดีขึ้นอย่างเห็นได้ชัด ในวันแรกที่ผู้วิจัยทำได้ทำการทดสอบนั้น ผู้ใช้ส่วนใหญ่มีความเห็นในเชิงลบกับระบบรหัสผ่านรูปภาพ เช่น “ทำไมต้องเปลี่ยนมาใช้ระบบรหัสผ่านที่ยากขึ้นแบบเดิมก็ใช้ได้ดีอยู่แล้ว” หรือ “ระบบรหัสผ่านรูปภาพนั้นใช้งานยากเกินไป” แต่ในวันสุดท้ายผู้วิจัยทำได้ทำการสอบถามความพึงพอใจต่อระบบรหัสผ่านรูปภาพอีกครั้งพบว่า ร้อยละ 66.67 เต็มใจที่จะเปลี่ยนมาใช้ระบบรหัสผ่านรูปภาพในชีวิตประจำวัน ร้อยละ 20 อาจจะเปลี่ยนมาใช้รหัสผ่านรูปภาพในชีวิตประจำวัน และอีกร้อยละ 13.33 เลือกที่จะใช้ระบบรหัสผ่านที่ตนเองใช้อยู่ในปัจจุบัน

3.2 วิเคราะห์ผลการทดสอบความง่ายในการใช้งาน

ผลการทดสอบความง่ายในการใช้งานพบว่าหลังจากให้ผู้ทดสอบใช้งานระบบรหัสผ่านรูปภาพเป็นเวลาหนึ่งสัปดาห์ผู้ทดสอบมีประสบการณ์การใช้งานที่ดีขึ้นอย่างมีนัยสำคัญ ทั้งอัตราความล้มเหลวซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด จำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ และระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จ มีค่าเกือบเทียบเท่าระบบรหัสผ่านตัวเลขหกหลัก และมีความสามารถในการจดจำที่ดีกว่าสำหรับผู้ใช้อีกด้วย



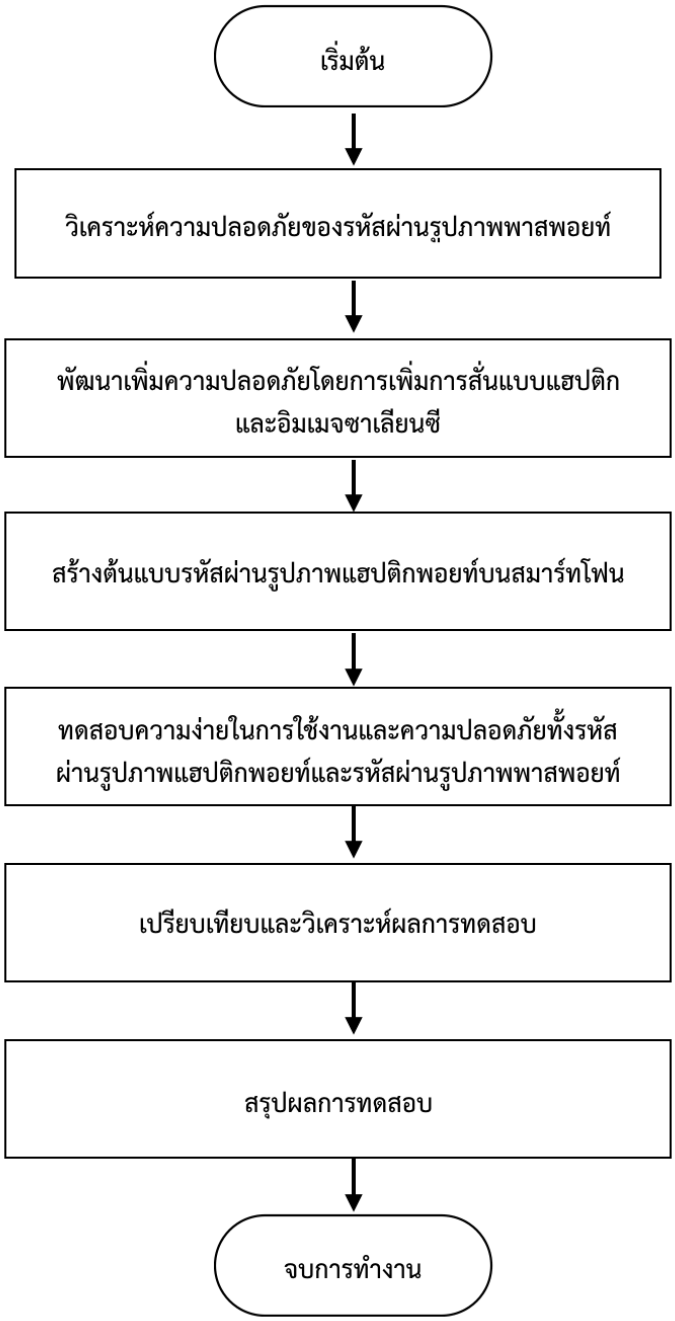
รูปที่ 3.3 ผลการทดสอบความง่ายในการใช้งานด้วยแบบทดสอบพีเอสเอสยูคิว

จากผลการทดสอบจะเห็นได้ว่าผลการทดสอบในด้านอัตราความล้มเหลวซึ่งเกิดจากการเลือกรหัสผ่านผิดจุดและจำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จรหัสผ่านรูปภาพพาสเฟซมีผลทดสอบหลังจากการอบรมและใช้งานต่อเนื่องที่ดีที่สุดตามมาด้วยรหัสผ่านรูปภาพพาสโก และรหัสผ่านรูปภาพพาสพอยท์ แต่อย่างไรก็ตามรหัสผ่านรูปภาพพาสเฟซนั้นแม้ทำการอบรมกับผู้ใช้แล้วระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จใช้เวลาสูงกว่าระบบอื่นมาก (รหัสผ่านตัวเลขหกหลัก 4.344 วินาที รหัสผ่านรูปภาพพาสโก 4.296 วินาที รหัสผ่านรูปภาพพาสพอยท์ 4.389 วินาที และรหัสผ่านรูปภาพพาสเฟซ 15.088 วินาที) และจากการวิเคราะห์ของบิดเดิลและคณะ [5] ที่ว่าปัจจัยที่สำคัญที่สุดของความง่ายในการใช้งานคือระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จจึงทำให้รหัสผ่านรูปภาพพาสเฟซไม่เหมาะสมในการนำมาพัฒนาและใช้งานจริง

ถึงแม้ว่ารหัสผ่านรูปภาพพาสโกมีผลการทดสอบโดยรวมที่ดีกว่ารหัสผ่านรูปภาพพาสพอยท์เล็กน้อย แต่ปัญหาหลักของรหัสผ่านรูปภาพพาสโกคือปัญหาในการจดจำระยะยาว [5] เนื่องจากรหัสผ่านรูปภาพพาสโกจัดอยู่ในระบบรหัสผ่านรูปภาพแบบรีคอลล์ กล่าวคือการเรียกคืนความจำของผู้ใช้นั้นถูกกระทำโดยไม่มีตัวช่วย ตรงกันข้ามกับรหัสผ่านรูปภาพพาสพอยท์ซึ่งเป็นระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ ซึ่งจะใช้องค์ประกอบในรูปภาพของรหัสผ่านเป็นตัวช่วยในการเรียกคืนความจำของผู้ใช้

การวิเคราะห์ในส่วนนี้ผู้วิจัยมีจุดประสงค์เพื่อหาระบบรหัสผ่านที่มีความง่ายในการใช้งานใกล้เคียงกับระบบรหัสผ่านที่เป็นที่นิยมที่สุดบนสมาร์ทโฟน (รหัสผ่านตัวเลขหกหลัก) และมีความสามารถใน

การจดจำที่ดีกว่า ผู้วิจัยจึงเลือกรหัสผ่านรูปภาพพาสพอยท์มาพัฒนาต่อ โดยจะมีการวิเคราะห์ความปลอดภัยของระบบในลำดับถัดไป



รูปที่ 3.4 ขั้นตอนการพัฒนารหัสผ่านรูปภาพแฮปติกพอยท์

3.3 การพัฒนาระบบรหัสผ่านรูปภาพระบบใหม่

ขั้นตอนการพัฒนาระบบรหัสรูปภาพใหม่จากระบบรหัสรูปภาพพาสพอยท์เป็นดังรูปที่ 3.4 ผู้วิจัยจะเริ่มจากการวิเคราะห์หาช่องโหว่และการโจมตีเรื่องความปลอดภัยของรหัสผ่านรูปภาพพาส

พอยท์ แล้วเสนอวิธีการใหม่นั่นคือการสั่นแบบแฮปติกและอิมเมจซาเลียนซีเพื่อป้องกันการโจมตี หลังจากนั้นจึงนำวิธีการใหม่ไปสร้างต้นแบบบนสมาร์ทโฟน และนำไปให้ผู้ใช้ทดลองใช้ร่วมกับรหัสผ่านรูปแบบพาสพอยท์อย่างต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ โดยจะมีการให้ผู้ทดสอบตอบแบบสอบถามเรื่องความง่ายในการใช้งานในวันแรกและวันสุดท้ายของการใช้งาน หลังจากนั้นจะนำผลการทดสอบของทั้งสองระบบรหัสผ่านมาเปรียบเทียบโดยใช้การทดสอบที เพื่อยืนยันว่าระบบรหัสผ่านแบบแฮปติกแม้ว่าจะมีขั้นตอนการทำงานเพิ่มจากระบบรหัสผ่านแบบพาสพอยท์เพื่อความปลอดภัยที่สูงกว่าแต่ไม่ได้ลดความง่ายในการใช้งาน

3.3.1 การวิเคราะห์ความปลอดภัยของรหัสผ่านรูปภาพพาสพอยท์

จากงานวิจัยของ บิดเดิลและคณะ [5] ได้ทำการศึกษาช่องโหว่และการโจมตีที่เป็นไปได้ของระบบรหัสผ่านรูปภาพ รวมไปถึงรหัสผ่านรูปภาพพาสพอยท์โดยการโจมตีเหล่านั้นคือ โชลเดอร์เซิร์ฟฟิง บรูทฟอร์ซ ดิกชันนารี และ ฮอตสปอต ซึ่งผู้วิจัยได้กล่าวถึงภาพรวมของการโจมตีเหล่านี้กับระบบรหัสผ่านรูปภาพในเบื้องต้นในบทที่ 2 บางส่วนแล้ว

1.) การโจมตีแบบโชล์เดอร์เซิร์ฟฟิง (Shoulder surfing attacks) : หรือการโจมตีโดยการสังเกตุการรหัสผ่านของผู้ใช้ระหว่างทำการยืนยันตัวตน ถือเป็นช่องโหว่ที่สำคัญของระบบรหัสผ่านรูปภาพ แม้ว่ารหัสผ่านรูปภาพนั้นยากที่จะคาดเดารหัสผ่าน แต่ถ้าเมื่อใดก็ตามผู้โจมตีด้วยวิธีนี้ รหัสผ่านอาจจะถูกเปิดเผยได้อย่างง่ายดาย มีระบบรหัสผ่านรูปภาพหลายระบบพยายามจะป้องกันการโจมตีชนิดนี้แต่ก็ต้องแลกมาด้วยความยุ่งยากมากขึ้นในการใช้งานของระบบ เช่น ระบบรหัสผ่านของ โซบราโดและคณะ [39] โดยมีการแสดงตัวเลขใต้รูปภาพให้ผู้ใช้ และ ให้ผู้ใช้จำตัวเลขเหล่านั้นเพื่อใช้ในการยืนยันตัวตน สำหรับรหัสผ่านรูปภาพพาสพอยท์นั้นผู้วิจัยได้ทำการทดสอบเบื้องต้นของความสามารถในการป้องกันการโจมตีชนิดนี้โดยมีผู้ร่วมทดสอบทั้งหมด 20 คน โดยมีการจำกัดจำนวนครั้งในการเข้าสู่ระบบสำหรับผู้โจมตีเพียง 4 ครั้ง ผลการทำทดสอบการโจมตีแบบโชลเดอร์เซิร์ฟฟิงของรหัสผ่านรูปภาพพาสพอยท์ คือผู้โจมตี 12 จาก 20 คน (60%) ซึ่งถือเป็นอัตราที่สูงมากสำหรับผู้ใช้ ผู้วิจัยจึงต้องการจะพัฒนาระบบที่สามารถป้องกันการโจมตีชนิดนี้ได้โดยที่มีผลกระทบกับผู้ใช้งานน้อยที่สุด

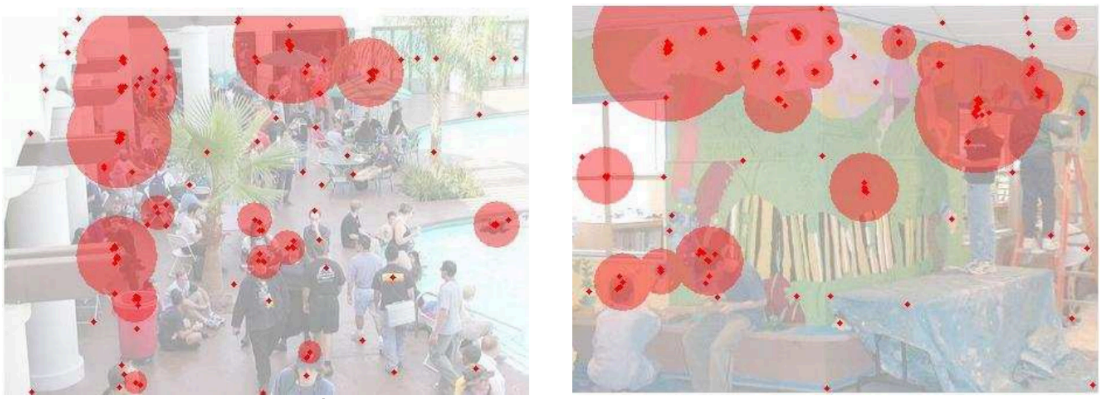
2.) การโจมตีแบบบรูทฟอร์ซ (Brute forced attacks) : การโจมตีชนิดนี้เกิดจากการทดลองรหัสผ่านความเป็นไปได้ทั้งหมดของรหัสผ่านการโจมตีชนิดนี้รหัสผ่านตัวอักษรและรหัสผ่านรูปภาพมีวิธีการโจมตีที่เหมือนกัน การโจมตีชนิดนี้มีความเป็นไปได้น้อยที่จะสามารถแกะรหัสผ่านได้สำเร็จหากรหัสผ่านนั้นมีขนาดที่ใหญ่พอ เพราะฉนั้นหากต้องการหลีกเลี่ยงจากการโจมตีชแบบบรูทฟอร์ซจำนวนรหัสผ่านที่เป็นไปได้ทั้งหมดควรจะมีจำนวนที่มากพอที่จะทำให้ผู้บุกรุกไม่สามารถทำการค้นหาทั้งหมดได้ (full-search) ในรหัสผ่านรูปภาพพาสพอยท์บนสมาร์ทโฟนที่มีหน้าจอขนาด 5 นิ้วและจำนวนของจุดทั้งหมดเท่ากับ 60 (6 ในแนวนอนและ 10 ในแนวตั้ง) มีจำนวนรหัสผ่านสำหรับรหัสผ่าน 4 จุด คือ 60^4 (23 บิต) 5 จุดคือ 60^5 (29 บิต) และ 6 จุดคือ 60^6 (35 บิต) ซึ่งหมายถึง

รหัสผ่านที่แข็งแรงของรหัสผ่านรูปภาพพาสพอยท์นั้นต้องแลกมากับการจำจำนวนจุดของรหัสผ่านที่มากขึ้น ผู้วิจัยจึงมีเป้าหมายที่จะเพิ่มจำนวนรหัสผ่านของรหัสผ่านรูปภาพพาสพอยท์โดยที่ผู้ใช้ไม่ต้องทำการจำจำนวนจุดที่มากขึ้น

3.) การโจมตีแบบดิกชันนารี (Dictionary attacks) : การโจมตีแบบดิกชันนารีของรหัสผ่านรูปภาพนั้นสามารถทำได้โดยใช้อัลกอริทึมในการวิเคราะห์พฤติกรรมการใช้รหัสผ่านของผู้ใช้ และโครงสร้างข้อมูลของรหัสผ่าน เพื่อค้นหาชุดของรหัสผ่านที่มีโอกาสสูง เพื่อที่จะนำรหัสผ่านเหล่านั้นไปทำการค้นหาและลองป้อนรหัสผ่านทั้งหมด

สำหรับรหัสผ่านรูปภาพพาสพอยท์การโจมตีแบบดิกชันนารีสามารถทำได้โดยการวิเคราะห์จุดบนภาพที่ผู้ใช้มักเลือกเป็นรหัสผ่าน (ฮอตสปอต) โดยใช้เครื่องมือช่วยวิเคราะห์รูปภาพอัตโนมัติ (automated image processing tools) ซึ่งรายละเอียดของการโจมตีแบบฮอตสปอตของพาสพอยท์จะกล่าวถึงในข้อถัดไป

4.) การโจมตีด้วยฮอตสปอต (Hotspots) : เนื่องจากการใช้งานรหัสรูปภาพแบบพาสพอยท์ผู้ใช้ทำการเลือกจุดที่สามารถจำได้บนรูปภาพมาประกอบกัน จึงเป็นเป้าหมายในการโจมตีแบบดิกชันนารีด้วยการใช้ฮอตสปอต ฮอตสปอตคือจุดหรือพื้นที่ของรูปภาพที่โดดเด่นและผู้ใช้มักเลือกเป็นรหัสผ่านรูปภาพ การค้นหาชุดของฮอตสปอตทำได้โดยการใช้อัลกอริทึมหรือเครื่องมือในการประมวลรูปภาพช่วยวิเคราะห์ ตัวอย่างการโจมตีแบบฮอตสปอตบนรหัสผ่านแบบพาสพอยท์ เช่น งานวิจัยของดีริคและคณะ [32] และ งานวิจัยของโทรปและคณะ [40] รูปที่ 3.5 แสดงตัวอย่างการวิเคราะห์ฮอตสปอตในงานวิจัยของโทรปและคณะ



รูปที่ 3.5 การโจมตีด้วยฮอตสปอตของโทรปและคณะ [40]

3.3.2 การพัฒนาระบบรหัสผ่านรูปภาพแฮปติกพอยท์

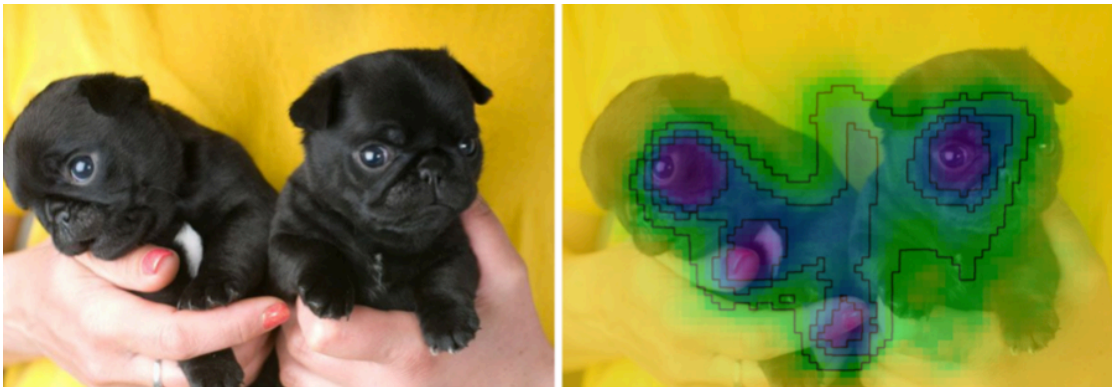
จากการวิเคราะห์รหัสผ่านรูปภาพแบบพาสพอยท์พบว่ามีช่องโหว่จากสองการโจมตีหลักคือ การโจมตีแบบโชลเดอร์เซิร์ฟฟิงและการโจมตีแบบฮอตสปอต ในการแก้ปัญหาการโจมตีแบบโชลเดอร์เซิร์ฟฟิงรหัสผ่านรูปภาพแฮปติกพอยท์ (HapticPoints) นำการสั่นแบบแฮปติก (การสั่นระยะสั้น) บน

สมาร์ทโฟนมาใช้เพื่อเป็นสัญญาณในการแจ้งผู้ใช้ว่าในรหัสผ่านรูปภาพตำแหน่งหลังจากที่เกิดการสั่นนั้น ผู้ใช้จะต้องป้อนรหัสผ่านหลอกหนึ่งครั้ง ระบบจะใช้การสุ่มสำหรับแต่ละตำแหน่งว่าจะมีการสั่นแบบแฮปติกหรือไม่ การสุ่มเพิ่มการสั่นแบบแฮปติกระหว่างการป้อนข้อมูลรหัสผ่านนั้นไม่สามารถสังเกตุด้วยตาเปล่าได้ ทำให้ผู้โจมตีแบบโชลเดอร์เซิร์ฟฟิงทราบได้ยากว่าจุดใดคือรหัสผ่านจริงและจุดใดที่ผู้ใช้ป้อนคือรหัสผ่านหลอก จำนวนของการเกิดการสั่นแบบแฮปติกนั้นสามารถคำนวณได้โดย

$$decoyPoints = ciel(actualPoints/2)$$

ขั้นตอนการสร้างรหัสผ่าน

จากงานวิจัยของ อัลเชชรี (Alshehri) [42] นั้นพบว่าการใส่อิมเมจซาเลียนซี (image saliency) ลงไปบนรูปภาพระหว่างการสร้างรหัสผ่านของรหัสผ่านรูปภาพพาสพอยท์เพื่อแสดงผลให้ผู้ใช้เห็นว่าจุดไหนของภาพเป็นจุดที่เด่นและมีโอกาสถูกโจมตี ทำให้ลดโอกาสของการโดนโจมตีด้วยเครื่องมือวิเคราะห์รูปภาพอัตโนมัติเพื่อหาฮอตสปอตของภาพไปทำการโจมตีแบบดิกชันนารีได้โดยที่มีผลกับการใช้งานผู้ใช้ในระหว่างการสร้างรหัสผ่านน้อยมาก ในระหว่างการสร้างรหัสผ่านนั้นผู้วิจัยจึงเลือกทำอิมเมจซาเลียนซี(รูปที่ 3.4) เช่นกัน โดยใช้อัลกอริทึมวิเคราะห์ภาพของดีพเกซ (DeepGaze) โดยผลลัพธ์ของรูปภาพที่ถูกประมวลผลแล้วมีดังนี้ สีเหลืองหมายถึงมีความเสี่ยงต่อการโจมตีด้วยฮอตสปอตต่ำ สีเขียวหมายถึงมีความเสี่ยงต่อการโจมตีด้วย ฮอตสปอตปานกลาง สีน้ำเงินหมายถึงมีความเสี่ยงต่อการโจมตีด้วยฮอตสปอตสูง และ สีม่วงหมายถึงมีความเสี่ยงต่อการโจมตีด้วยฮอตสปอตสูงมาก



รูปที่ 3.6 ตัวอย่างของการวิเคราะห์อิมเมจซาเลียนซี

ขั้นตอนในการสร้างรหัสผ่านของระบบรหัสผ่านรูปภาพแฮปติกพอยท์มีดังนี้

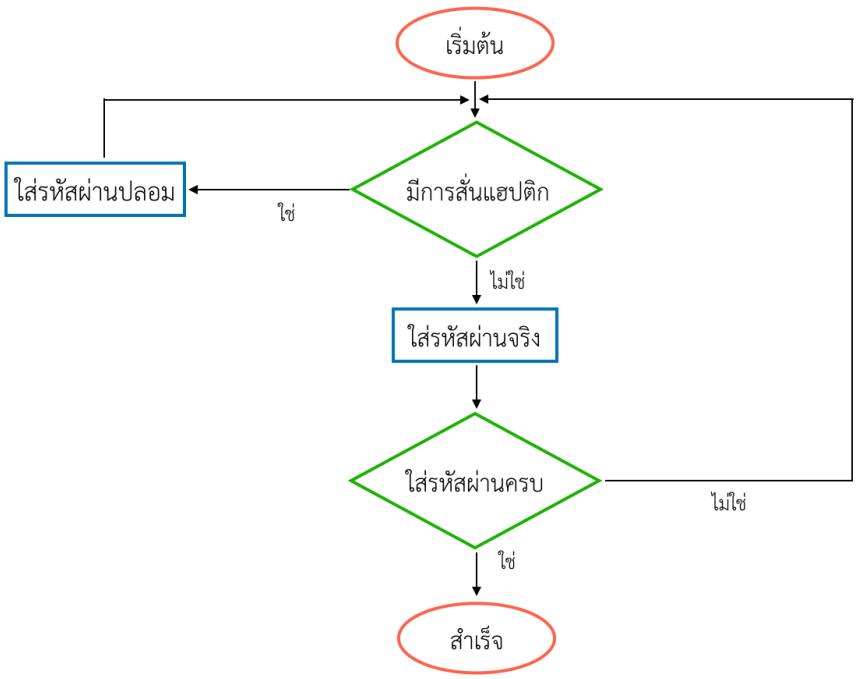
1) ผู้ใช้ทำการเลือกรูปภาพรหัสผ่านจากสมาร์ทโฟน โดยรูปภาพที่เลือกนั้นเป็นรูปภาพใดๆ ก็ได้
2) รูปภาพที่ผู้ใช้เลือกนั้นจะถูกนำมาวิเคราะห์อิมเมจซาเลียนซี โดยระบบจะทำการแจ้งผู้ใช้ว่าถ้าพื้นที่ของอิมเมจซาเลียนซีมีมากจะมีโอกาสน้อยที่จะถูกโจมตีจากผู้โจมตี

3) ถ้าผู้ใช้ยืนยันการใช้รูปภาพนั้นจะเริ่มให้ผู้ใช้เลือกจุดรหัสผ่านบนรูปภาพโดยมีความยาว 4 ถึง 6 จุด และต้องเรียงเป็นลำดับ ถ้าผู้ใช้ไม่ยืนยันผู้ใช้สามารถกลับไปเลือกรูปภาพใหม่ได้ในขั้นตอนที่ 1
4) ให้ผู้ใช้ทำการยืนยันจุดรหัสผ่านอีกครั้งหากการยืนรหัสผ่านผิดต้องกลับไปเริ่มที่ขั้นตอนที่ 3 ใหม่

ขั้นตอนการเข้าสู่ระบบ

หลังจากผู้ใช้ทำการสร้างรหัสผ่านสำเร็จแล้วผู้ใช้จะต้องนำรหัสผ่านที่สร้างขึ้นในขั้นตอนการสร้างรหัสผ่านมาใช้โดยมีขั้นตอนดังนี้

1) ผู้ใช้เริ่มทำการป้อนข้อมูลรหัสผ่านจุดแรกบนรูปภาพ
2) ถ้าผู้ใช้ได้รับสัญญาณการสั่นแฮปติกจากระบบ ผู้ใช้จะต้องสร้างรหัสผ่านปลอมโดยเลือกจุดใดๆบนรูปภาพหนึ่งครั้ง แต่ถ้าไม่มีสัญญาณการสั่นแฮปติกจากระบบผู้ใช้เริ่มการใส่รหัสผ่านจริงของจุดในลำดับถัดไป
3) ทำขั้นตอนที่ 1 และ 2 ต่อไปเรื่อยๆจนกว่าจะป้อนข้อมูลรหัสผ่านสำเร็จจนถึงจุดสุดท้าย
4) ถ้าผู้ใช้ตระหนักได้ว่าเกิดความผิดพลาดระหว่างป้อนข้อมูลรหัสผ่านนั้นผู้ใช้สามารถยกเลิกและกลับไปที่ขั้นตอนที่ 1 ได้ทันที



รูปที่ 3.7 แผนผังการเข้าสู่ระบบของแฮปติกพอยท์

3.4 การทดสอบความง่ายในการใช้ของรหัสผ่านรูปภาพแฮปติกพอยท์

ผู้วิจัยได้พัฒนาต้นแบบเป็นแอปพลิเคชันบนระบบปฏิบัติการแอนดรอยด์ และ ทำการรับสมัครผู้ทดสอบจำนวน 35 คน เป็นกลุ่มคนที่ใช้สมาร์ทโฟนในชีวิตประจำวัน โดยมีช่วงอายุอยู่ที่ 24 ถึง 33 ปี แบ่งเป็นเพศหญิง 14 คน และ เพศชาย 21 คน

การทดสอบความง่ายในการใช้งานผู้ทำการทดสอบทุกคนได้รับการอธิบายวิธีการใช้งานของทั้งสองระบบเป็นอย่างดีในทางทฤษฎี จากนั้นผู้ทดสอบทุกคนจะทำการทดลองสร้างและใช้งานรหัสผ่านของทั้งสองระบบ หลังจากมั่นใจแล้วว่าผู้ทดสอบทุกคนมีความเข้าใจในการใช้งานแล้วผู้ทดสอบจะต้องสร้างรหัสผ่านเพื่อใช้งานจริงของทั้งสองระบบ

การวัดผลการทดสอบความง่ายในการใช้งานแบ่งเป็นสองหมวดหมู่ คือ การวัดผลการทดสอบเชิงปริมาณ และ การวัดผลการทดสอบเชิงคุณภาพ การทดสอบเชิงปริมาณประกอบด้วย จำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ (number of attempts required for successful authentication) ระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จ (login time required in a successful authentication) และ อัตราความสามารถในการกู้คืนความจำ (recall success rate) การทดสอบเชิงคุณภาพประกอบด้วย แบบสำรวจความยากในการใช้งานของระบบโดยใช้แบบสอบถามความง่ายในการใช้งานพีเอสเอสยูคิว โดยผู้วิจัยได้นำการผลการทดสอบมาค้นหาค่าความแตกต่างโดยใช้การทดสอบที เพื่อวัดนัยสำคัญของความแตกต่างของรหัสผ่านรูปภาพพาสพอยท์และแฮปติกพอยท์

บทที่ 4
ผลการวิจัยและการอภิปรายผล

ในบทนี้เป็นการอธิบายผลการจัดเก็บข้อมูลการปรียบเทียบของรหัสผ่านรูปภาพแฮปติกพอยท์และรหัสผ่านรูปภาพพาสพอยท์ โดยมีสองส่วนคือการทดสอบความง่ายในการใช้งานของรหัสผ่านรูปภาพแฮปติกพอยท์ และความสามารถในการป้องกันการโจมตีของรหัสผ่านรูปภาพแฮปติกพอยท์

4.1 ผลการทดสอบความง่ายในการใช้ของรหัสผ่านรูปภาพแฮปติกพอยท์

4.1.1 ผลการทดสอบจำนวนครั้งเพื่อการเข้าสู่ระบบที่สำเร็จ

จำนวนครั้งเพื่อการเข้าสู่ระบบที่สำเร็จคือจำนวนครั้งต่อผู้ทดสอบหนึ่งคนในการป้อนรหัสผ่านข้อมูลหากผู้ทดสอบป้อนข้อมูลรหัสผ่านผิดระหว่างการเข้าสู่ระบบผู้ทดสอบจะต้องเริ่มทำการป้อนรหัสผ่านใหม่ตั้งแต่ต้นและจำนวนครั้งจะถูกเพิ่มทีละหนึ่งครั้งจนกว่าผู้ทดสอบจะเข้าสู่ระบบสำเร็จ ตารางที่ 4.1 แสดงผลการทดสอบจำนวนครั้งเพื่อการเข้าสู่ระบบที่สำเร็จเฉลี่ยจากผู้ทดสอบทั้งหมด รหัสผ่านรูปภาพพาสพอยท์มีผลลัพธ์คือ 1.645 ครั้ง โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 0.797 มีจำนวนครั้งต่ำที่สุดคือ 1 และจำนวนครั้งมากที่สุดคือ 4 ส่วนรหัสผ่านรูปภาพแฮปติกพอยท์มีผลลัพธ์คือ 1.709 ครั้ง โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 0.824 มีจำนวนครั้งต่ำที่สุดคือ 1 และจำนวนครั้งมากที่สุดคือ 4 และผลการทดสอบเพื่อวัดนัยสำคัญของความแตกต่างโดยการทดสอบที มีค่า t เท่ากับ 0.308 และ P เท่ากับ 0.759 กล่าวคือผลลัพธ์ของการทดสอบทั้งสองระบบนั้นไม่มีความแตกต่างอย่างมีนัยสำคัญ แต่จากผลทดสอบมีค่าเฉลี่ยของจำนวนครั้งมากขึ้นเล็กน้อยเนื่องจากระบบเพิ่มความซับซ้อนในการป้อนรหัสผ่านของระบบทำให้ผู้ทดสอบบางคนสับสนเล็กน้อย

ตารางที่ 4.1 ตารางผลการทดสอบจำนวนครั้งเพื่อการเข้าสู่ระบบที่สำเร็จ (ครั้ง)

	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบนมาตรฐาน (SD)	ค่าต่ำสุด (Min)	ค่าสูงสุด (Max)	ผลการทดสอบที (t-test)
รหัสผ่านรูปภาพพาสพอยท์	1.622	0.853	1	4	t = 0.5530 P = 0.7230
รหัสผ่านรูปภาพแฮปติกพอยท์	1.712	0.889	1	4	

4.1.2 ผลการทดสอบระยะเวลาเพื่อการเข้าสู่ระบบที่สำเร็จ

ตารางที่ 4.2 ตารางผลการทดสอบระยะเวลาเพื่อการเข้าสู่ระบบที่สำเร็จ (วินาที)

	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบนมาตรฐาน (SD)	ค่าต่ำสุด (Min)	ค่าสูงสุด (Max)	ผลการทดสอบที (t-test)
รหัสผ่านรูปภาพพาสพอยท์	8.319	3.655	3.32	15.52	t = 2.2030 P = 0.0470
รหัสผ่านรูปภาพแฮปติกพอยท์	10.432	4.981	4.01	17.37	

ระยะเวลาเพื่อการเข้าสู่ระบบที่สำเร็จคือระยะเวลาทั้งหมดที่ผู้ทดสอบใช้ในการเข้าสู่ระบบ โดยเริ่มจับเวลาตั้งแต่การป้อนข้อมูลรหัสผ่านจุดแรก และหยุดจับเวลาเมื่อผู้ใช้ป้อนข้อมูลรหัสผ่านตัวสุดท้ายโดยที่การป้อนข้อมูลรหัสผ่านนั้นจะต้องถูกต้องทุกจุดตรงกับรหัสผ่านที่ผู้ทดสอบสร้าง หากผู้ใช้ป้อนข้อมูลรหัสผ่านผิดจะต้องป้อนใหม่จนกว่าจะสำเร็จ ตารางที่ 4.2 แสดงผลการทดสอบระยะเวลาเพื่อการเข้าสู่ระบบที่สำเร็จเฉลี่ยจากผู้ทดสอบทั้งหมด รหัสผ่านรูปภาพพาสพอยท์มีผลลัพธ์คือ 8.421 วินาที โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 3.838 มีระยะเวลาที่ต่ำที่สุดคือ 3.35 วินาที และระยะเวลาที่มากที่สุดคือ 15.52 วินาที ส่วนรหัสผ่านแฮปติกพอยท์มีผลลัพธ์คือ 10.278 วินาที โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 4.178 ระยะเวลาที่ต่ำที่สุดคือ 4.01 วินาที และระยะเวลาที่มากที่สุดคือ 17.37 วินาที และผลการทดสอบเพื่อวัดนัยสำคัญของความแตกต่างโดยการทดสอบที มีค่า t เท่ากับ 1.793 และ P เท่ากับ 0.0782 กล่าวคือผลลัพธ์ของการทดสอบทั้งสองระบบนั้นไม่มีความแตกต่างอย่างมีนัยสำคัญ แต่จากผลทดสอบมีค่าเฉลี่ยของระยะเวลามากขึ้นเนื่องจากผู้ทดสอบต้องใช้เวลาในการป้อนรหัสผ่านเพิ่มสองจุด

4.1.3 ผลการทดสอบอัตราความสามารถในการกู้คืนความจำ

โดยปกติแล้วรหัสผ่านรูปภาพพาสพอยท์ จะมีอัตราความสามารถในการกู้คืนความจำที่ต่ำลงเมื่อไม่ได้ใช้รหัสผ่านเป็นระยะเวลาหนึ่ง ผู้วิจัยจึงทำการทดสอบเปรียบเทียบอัตราความสามารถในการกู้คืนความจำโดยแบ่งเป็นสองช่วงเวลาคือ หนึ่งชั่วโมง และ หนึ่งสัปดาห์ โดยในระยะเวลาดังกล่าวผู้ใช้จะถูกห้ามให้ป้อนรหัสผ่านรูปภาพจนกว่าจะถึงเวลาที่กำหนด ตารางที่ 4.3 แสดงผลการทดสอบอัตราความสามารถในการกู้คืนความจำเฉลี่ยจากผู้ทดสอบทั้งหมด การทดสอบความสามารถในการกู้คืนความจำหนึ่งชั่วโมงของรหัสผ่านระบบเดิมมีผลลัพธ์คือ ร้อยละ 95.97 โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 9.347 มีอัตราความสามารถในการกู้คืนความจำที่ต่ำที่สุดคือ ร้อยละ 75 และอัตราความสามารถในการกู้คืนความจำที่มากที่สุดคือ ร้อยละ 100 ส่วนรหัสผ่านแฮปติกพอยท์มีผลลัพธ์คือ

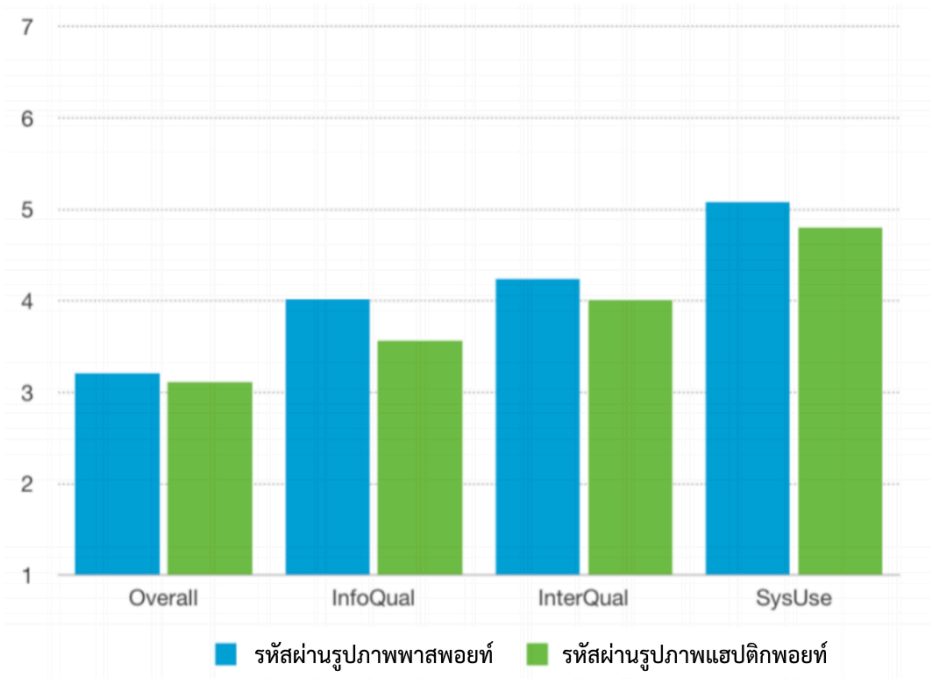
ร้อยละ 95.97 โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 9.347 มีอัตราความสามารถในการกู้คืนความจำที่ต่ำที่สุดคือ ร้อยละ 75 และอัตราความสามารถในการกู้คืนความจำที่มากที่สุดคือ ร้อยละ 100 และผลการทดสอบพื่อวัดนัยสำคัญของความแตกต่างโดยการทดสอบที มีค่า t เท่ากับ 0.912 และ P เท่ากับ 0.365 กล่าวคือผลลัพธ์ของการทดสอบทั้งสองระบบนั้นไม่มีความแตกต่างอย่างมีนัยสำคัญ และ การทดสอบความสามารถในการกู้คืนความจำหนึ่งสัปดาห์ของรหัสผ่านระบบเดิมมีผลลัพธ์คือ ร้อยละ 67.741 โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 29.006 มีอัตราความสามารถในการกู้คืนความจำที่ต่ำที่สุดคือ ร้อยละ 0 และอัตราความสามารถในการกู้คืนความจำที่มากที่สุดคือ ร้อยละ 100 ส่วนรหัสผ่านแฮปติกพอยท์มีผลลัพธ์คือ ร้อยละ 66.129 โดยมีค่าส่วนเบี่ยงเบนมาตรฐานคือ 33.259 มีอัตราความสามารถในการกู้คืนความจำที่ต่ำที่สุดคือ ร้อยละ 0 และอัตราความสามารถในการกู้คืนความจำที่มากที่สุดคือ ร้อยละ 100 และผลการทดสอบเพื่อวัดนัยสำคัญของความแตกต่างโดย t-test มีค่า t เท่ากับ 0.2002 และ P เท่ากับ 0.842 กล่าวคือผลลัพธ์ของการทดสอบทั้งสองระบบนั้นไม่มีความแตกต่างอย่างมีนัยสำคัญ จากผลทดสอบข้างต้นแสดงให้เห็นว่าอัตราความสามารถในการกู้คืนความจำของผู้ใช้ในระบบเดิมและระบบแฮปติกพอยท์นั้นมีความแตกต่างเพียงเล็กน้อยหรือไม่มีเลย เพราะฉนั้นการเพิ่มความซับซ้อนของการใช้งานด้วยวิธีของแฮปติดพอยท์ให้กับระบบรหัสผ่านเดิมนี้ไม่มีผลกับอัตราความสามารถในการกู้คืนความจำของผู้ทดสอบ

ตารางที่ 4.3 ตารางผลการทดสอบอัตราความสามารถในการกู้คืนความจำ (ร้อยละ)

ระยะเวลา	ประเภทรหัสผ่านรูปภาพ	ค่าเฉลี่ย (Mean)	ส่วนเบี่ยงเบนมาตรฐาน (SD)	ค่าต่ำสุด (Min)	ค่าสูงสุด (Max)	ผลการทดสอบที (t-test)
หนึ่งชั่วโมง	รหัสผ่านรูปภาพพาสพอยท์	96.010	9.512	75	100	t = 0.6510 P = 0.5170
	รหัสผ่านรูปภาพพาสพอยท์	94.420	10.598	75	100	
หนึ่งสัปดาห์	รหัสผ่านรูปภาพพาสพอยท์	67.722	30.012	0	100	t = 0.0280 P = 0.9780
	รหัสผ่านรูปภาพพาสพอยท์	67.521	31.112	0	100	

4.1.4 ผลการทดสอบความง่ายในการใช้งานด้วยแบบทดสอบพีเอสเอสยูคิว

ผู้วิจัยได้ทำการทดสอบความง่ายในการใช้งานด้วยแบบสำรวจมาตรฐานพีเอสเอสยูคิว ซึ่งมีคำถามทั้งหมด 19 ข้อ โดยมี 4 หมวดหมู่ย่อยคือ ประโยชน์ในการใช้งานของระบบ (SysUse) คุณภาพในการแสดงผลข้อมูลของระบบ (InfoQual) ส่วนติดต่อระหว่างผู้ใช้และระบบ (InterQual) และ ความพึงพอใจโดยรวมต่อระบบ (Overall)



รูปที่ 4.1 ผลการทดสอบความง่ายในการใช้งานด้วยแบบทดสอบพีเอสเอสยูคิว

มีเกณฑ์การให้คะแนนโดย 1 คือ ไม่เห็นด้วยที่สุดและ 7 คือ เห็นด้วยที่สุด รูปที่ 13 แสดงผลการทดสอบความง่ายในการใช้งานเปรียบเทียบระหว่างรหัสผ่านรูปภาพระบบเดิมและรหัสผ่านรูปภาพระบบแฮปติกพอยท์ ผลการทดสอบเพื่อวัดนัยสำคัญของความแตกต่างโดย t-test มีค่า t เท่ากับ 0.4412 และ P เท่ากับ 0.634 กล่าวคือผลลัพธ์ของการทดสอบทั้งสองระบบนั้นไม่มีความแตกต่างอย่างมีนัยสำคัญ

4.2 ความสามารถในการป้องกันการโจมตีของรหัสผ่านรูปภาพแฮปติกพอยท์

4.2.1 ความสามารถในการป้องกันการโจมตีแบบบรูทฟอร์ซ

ผู้วิจัยได้คำนวณขนาดของรหัสผ่านรูปภาพเพื่อวัดผลความปลอดภัยของแฮปติกพอยท์จากการโจมตีแบบบรูทฟอร์ซผู้วิจัยทำการพัฒนาบนระบบบนสมาร์ทโฟนที่มีการแสดงขนาด 5 นิ้วและจำนวนของจุดทั้งหมดเท่ากับ 60 (6 ในแนวนอนและ 10 ในแนวตั้ง) จากตารางที่ 4.4 เราจะพบว่าความแรงของรหัสผ่านของแฮปติกพอยท์จำนวน 4 จุดขนาดของรหัสผ่านจะเท่ากับรหัสผ่านรูปภาพพาสพอยท์จำนวน 6 จุด และเท่ากับรหัสผ่านตัวอักษรหกตัวประกอบด้วยตัวเลขตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ สอดคล้องกับเป้าหมายที่ผู้วิจัยต้องการให้ผู้ใช้ทำการจำรหัสผ่านเท่าระบบเดิม แต่มีจำนวนรหัสผ่านที่มากขึ้นโดยลดความง่ายในการใช้งานเล็กน้อย

ตารางที่ 4.4 ตารางผลการเปรียบเทียบเอนโทรปีของรหัสผ่านรูปภาพพาสพอยท์และรหัสผ่านรูปภาพแฮปติกพอยท์

	จำนวนจุดของรหัสผ่าน		
	4	5	6
เอนโทรปีของรหัสผ่านรูปภาพพาสพอยท์	23 บิต	29 บิต	35 บิต
เอนโทรปีของรหัสผ่านรูปภาพแฮปติกพอยท์	35 บิต	47 บิต	53 บิต

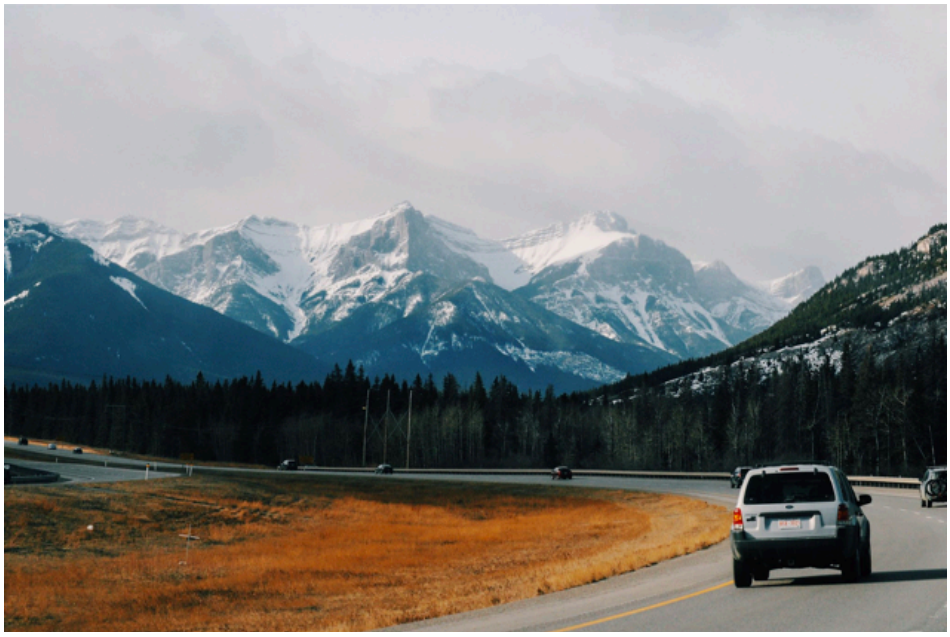
4.2.2 ความสามารถในการป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิง

ผู้วิจัยทำการทดสอบความสามารถในการป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิงตามวิธีการทดสอบทั่วไป ผู้ทดสอบจะได้เป็นทั้งผู้โจมตีและผู้ถูกโจมตี การทดสอบนี้นี้มีข้อได้เปรียบที่ผู้ทดลองสามารถฝึกการป้อนรหัสผ่านได้ ล่วงหน้าเพื่อให้แน่ใจว่าความเร็วในการเข้าร่วมและท่าทางร่างกายสำหรับผู้เข้าร่วมทั้งหมด ดังนั้น เราได้ประเมินความสามารถในการจดจำรหัสผ่านที่ผู้เข้าร่วมสังเกตการณ์ได้รับผ่านการฝึกอบรมแล้ว เมื่อเทียบกับการประเมินผู้โจมตีกับผู้ใช้เริ่มต้นในการทดสอบเป็นผู้โจมตีด้วย อายุเฉลี่ยอยู่ที่ 29 ปี ที่อายุน้อยที่สุด ผู้เข้าร่วมการทดสอบมีอายุ 23 ปีและอายุที่เก่าที่สุดคือ 44 ปี ผู้โจมจีจะอยู่ทางขวามือของผู้ถูกโจมตีและสามาถเปลี่ยนตำแหน่งไปทางซ้ายหรือหลังได้อย่างอิสระ นอกจากนี้เรายัง จำกัด จำนวนครั้งในการเข้าสู่ระบบสำหรับผู้โจมตีเพียง 4 ครั้ง ผลการทดสอบของรหัสผ่านรูปภาพพาสพอยท์คือผู้โจมตี 12 จาก 20 คน (60%) สามารถแกะรหัสผ่านได้ แต่ผลจาก แฮปติกพอยท์ คือ 1 ใน 20 (5%) เท่านั้น การที่ผู้โจมตีหนึ่งคนสามารถทำการโจมตีสำเร็จนั้นเนื่องมาจาก ผู้ใช้บางคนสร้างรหัสผ่านปลอมที่ทำให้ผู้โจมตีสามารถคาดเดาได้ว่ารหัสผ่านนั้นเป็นรหัสผ่านปลอมกล่าวคือผู้ใช้นั้นสร้างรหัสผ่านปลอมในบริเวณที่คาดเดาได้ง่ายเช่น ริมขอบของรูปภาพรวมไปถึงความเร็วในการใส่รหัสผ่าน ในการใส่รหัสผ่านจริงผู้ใช้นั้นจำเป็นจะต้องป้อนรหัสผ่านให้ตรงจุดจึงใช้เวลามาก แต่การใส่รหัสผ่านปลอมผู้ใช้ส่วนใหญ่ใช้เวลาในการป้อนรหัสปลอมเร็วกว่าการป้อนรหัสจริง อย่างไรก็ตามอัตราความสำเร็จในการทำโจมตีชนิดนี้ลดลงอย่างมีนัยสำคัญ

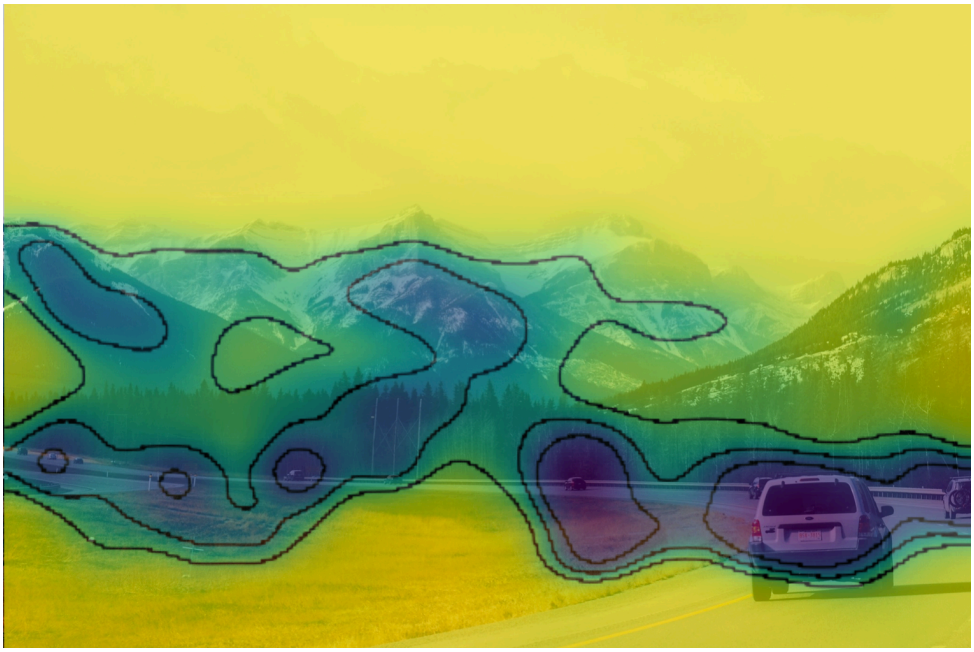
4.2.3 ความสามารถในการป้องกันการโจมตีแบบดิกชันนารีด้วยฮอตสปอต

โดยทั่วไปนั้นระบบรหัสผ่านรูปภาพมีความเสี่ยงสูงจากการโจมตีแบบดิกชันนารีดังที่กล่าวไว้ในการวิเคราะห์ความปลอดภัยของรหัสผ่านรูปภาพโดยการสืบค้นฮอตสปอต ด้วยระบบวิเคราะห์รูปภาพ (automated image processing) อย่างไรก็ตามจากงานวิจัยของ วิเด็นเบคและคณะ [35] และ นารยานันและคณะ[41] พบว่าการใช้อิมเมจซาเลียนซีสามารถช่วยจำลองฮอตสปอตที่จะเกิดขึ้นบนรหัสผ่านรูปภาพ ทำให้ผู้ใช้สามารถเลือกภาพที่มีความแข็งแรงและเหมาะสม ทำให้ผู้โจมทำการ

โจมตีรหัสผ่านรูปภาพแบบดิกชันนารีด้วยฮอตสปอตยากขึ้นและมีความเป็นไปได้ที่จะหารหัสผ่านน้อยลง สำหรับแฮปติกพอยท์นั้นได้ทำการเพิ่มคุณสมบัติการวิเคราะห์ ฮอตสปอตด้วยอิมเมจซาเลียนซีเช่นกัน ในขั้นตอนการสร้างรหัสผ่าน แต่จากการทดสอบความสามารถในการป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิงพบว่าการป้อนรหัสผ่านปลอมของผู้ใช้มีพฤติกรรมที่ต่างจากการป้อนรหัสผ่านจริง ผู้ใช้ส่วนใหญ่จะเลือกจุดนอกบริเวณฮอตสปอตทำให้เกิดความเสี่ยงในการถูกโจมตี ผู้โจมตีอาจสังเกตเห็นว่าจุดใดอาจจะเป็นรหัสผ่านปลอมและจุดใดอาจจะเป็นรหัสผ่านจริง

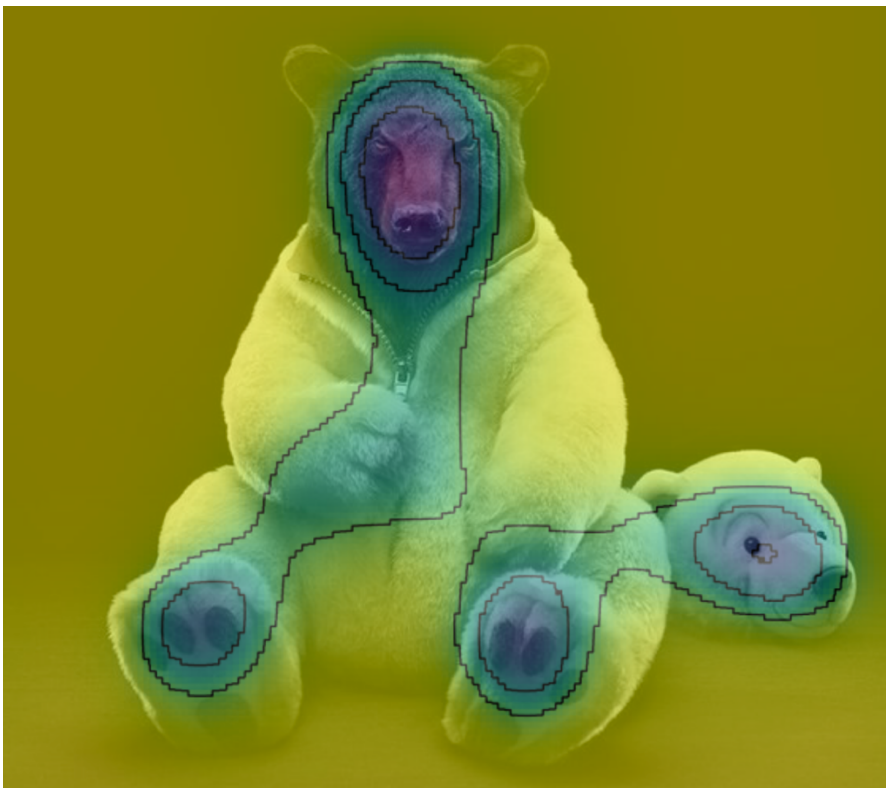


รูปที่ 4.2 ตัวอย่างรูปภาพ ก. ก่อนทำการประมวลผลรูปภาพอิมเมจซาเลียนซีด้วยดีพเกซ



รูปที่ 4.3 ตัวอย่างรูปภาพ ก. หลังทำการประมวผลรูปภาพอิมเมจซาเลียนซีด้วยดีพเกซ

รูปที่ 4.4 ตัวอย่างรูปภาพ ข. ก่อนทำการประมวผลรูปภาพอิมเมจซาเลียนซีด้วยดีพเกซ



รูปที่ 4.5 ตัวอย่างรูปภาพ ข. หลังทำการประมวผลรูปภาพอิมเมจซาเลียนซีด้วยดีพเกซ

บทที่ 5
สรุปผลและข้อเสนอแนะ

5.1 สรุปผล

รหัสผ่านรูปภาพเป็นหนึ่งในวิธีการยืนยันตัวตนที่มีศักยภาพสูงและมีความปลอดภัยที่สูงกว่าการใช้รหัสผ่านตัวเลขและวิธีการปลดล็อคของแอนดรอยด์ โดยเฉพาะระบบรหัสผ่านแบบคิวด์รีคอลล์ซึ่งใช้องค์ประกอบของรูปภาพในการเรียกคืนความจำของผู้ใช้ อย่างไรก็ตามงานวิจัยของบิดเดิลและคณะ [5] พบว่ารหัสผ่านรูปภาพที่มีความปลอดภัยสูงมีความง่ายในการใช้งานต่ำจึงไม่เป็นที่นิยมในการนำมาประยุกต์ใช้งานจริงซึ่งอาจเกิดจากผู้ใช้ไม่คุ้นเคยกับรหัสผ่านรูปภาพ อีกปัญหาหนึ่งของรหัสภาพรูปภาพคือการโจมตีแบบโชลเดอร์เซิร์ฟฟิง งานวิจัยนี้จึงแบ่งเป็นสองส่วน ในส่วนแรกเป็นการทดสอบสมมติฐานเรื่องความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพจะเพิ่มมากขึ้นเมื่อทำการใช้งานต่อเนื่องบนสมาร์ทโฟนเป็นเวลาหนึ่งสัปดาห์ โดยทำการทดสอบกับรหัสผ่านรูปภาพพาสโก พาสเฟซ และพาสพอยท์ และส่วนที่สองคือการวิเคราะห์เลือกรหัสผ่านรูปภาพที่มีความปลอดภัย ความง่ายในการจำ และความง่ายในการใช้งานที่ดีที่สุดจากส่วนที่หนึ่งซึ่งคือระบบรหัสผ่านพาสพอยท์มาพัฒนาเพิ่มความปลอดภัยจากการโจมตีแบบโชสเดอร์เซิร์ฟฟิงโดยเพิ่มรหัสผ่านปลอมด้วยการสั่นแบบแฮปติกบนสมาร์ทโฟน และเพิ่มความปลอดภัยจากการโจมตีแบบฮอตสปอตโดยการใช้หลักการของอิมเมจซาเลียนซี่โดยใช้อัลกอริทึมดีฟเกซ

การทดสอบสมมติฐานในส่วนที่หนึ่งแบ่งการทำงานเป็น 3 ส่วนคือ 1. เลือกระบบรหัสผ่านที่ดีที่สุดของแต่ละประเภทของระบบรหัสผ่านรูปภาพ ซึ่งได้แก่ พาสโก พาสเฟซ และ พาสพอยท์ ตามลำดับ 2. นำทั้งสามรหัสที่เลือกมาปรับปรุงให้เหมาะสมกับการใช้งานบนสมาร์ทโฟน และมีการตั้งค่าเอนโทรปีในแต่ละระบบให้ใกล้เคียงกันเพื่อความง่ายในการทดสอบ 3. ทำการทดสอบการใช้งานของรหัสภาพรูปภาพทั้งสามประเภทและ ระบบรหัสผ่านตัวเลขแบบหกหลักกับผู้ใช้งาน 40 คน ระหว่างอายุ 23 – 35 ปี ในระยะเวลาหนึ่งสัปดาห์ ผลการทดสอบความง่ายในการใช้งานเชิงปริมาณประกอบด้วย อัตราความผิดพลาดซึ่งเกิดจากการเลือกรหัสผ่านผิดจุด จำนวนครั้งของการพยายามล็อกอินจนเข้าสู่ระบบสำเร็จ ระยะเวลาในการล็อกอินจนเข้าสู่ระบบ ส่วนผลการทดสอบเชิงคุณภาพใช้แบบทดสอบความง่ายในการใช้งานหลังการใช้งานระบบพีเอสเอสยูคิว มีเกณฑ์การให้คะแนนจากหนึ่งถึงเจ็ด โดยหนึ่งคือไม่เห็นด้วยที่สุดและเจ็ดคือเห็นด้วยที่สุด โดยมีพารามิเตอร์ในการทดสอบคือประโยชน์ในการใช้งานของระบบ คุณภาพในการแสดงผลข้อมูลของระบบ ส่วนติดต่อระหว่างผู้ใช้และระบบ และ ความพึงพอใจโดยรวมต่อระบบ และนำมาเปรียบเทียบกับผลการทดสอบความง่ายในการใช้งานของระบบรหัสผ่านสำรองที่เป็นที่นิยมในปัจจุบันคือระบบรหัสผ่านตัวเลขหกหลัก ผลการทดสอบพบว่าหลังจากใช้ระบบรหัสผ่านรูปภาพอย่างต่อเนื่องเป็นเวลาหนึ่งสัปดาห์ ความง่ายในการใช้

งานของทุกระบบรหัสผ่านมีประสิทธิภาพที่ดีขึ้น และมีความง่ายในการใช้งานต่างจากระบบรหัสผ่านตัวเลขหกอย่างไม่มีนัยสำคัญ ซึ่งสามารถพิสูจน์สมมติฐานเรื่องความง่ายในการใช้งานของระบบรหัสผ่านรูปภาพบนสมาร์ทโฟนจะเพิ่มมากขึ้นเมื่อใช้งานต่อเนื่องเป็นเวลาหนึ่งสัปดาห์นั้นเป็นจริง

จากผลการทดสอบถึงแม้ว่ารหัสผ่านรูปภาพพาสโกมีผลการทดสอบโดยรวมที่ดีกว่ารหัสผ่านรูปภาพพาสพอยท์เล็กน้อย แต่ปัญหาหลักของรหัสผ่านรูปภาพพาสโก คือปัญหาในการจำในระยะยาว [5] เนื่องจากรหัสผ่านรูปภาพพาสโกจัดอยู่ในระบบรหัสผ่านรูปภาพแบบรีคอลล์ การเรียกคืนความจำนั้นถูกกระทำโดยไม่มีตัวช่วยใดปรากฏอยู่บนรูปภาพ เป็นการจำแบบเดียวกันกับรหัสผ่านตัวอักษร ตรงกันข้ามรหัสผ่านรูปภาพพาสพอยท์ซึ่งเป็นระบบรหัสผ่านรูปภาพแบบคิวด์รีคอลล์ ซึ่งจะใช้องค์ประกอบของรูปภาพในรหัสผ่านเป็นตัวช่วยในการเรียกคืนความจำของผู้ใช้ ส่วนรหัสผ่านรูปภาพพาสเฟสนั้นมีข้อเสียที่ระยะเวลาในการล็อกอินจนเข้าสู่ระบบสำเร็จที่นานเกินไปเมื่อเทียบกับระบบอื่นถึงสามเท่าจึงไม่เหมาะสมกับการนำมาพัฒนาต่อ (รหัสผ่านตัวเลข 4.344 วินาที รหัสผ่านรูปภาพพาสโก 4.296 วินาที รหัสผ่านรูปภาพพาสพอยท์ 4.389 วินาที และ รหัสผ่านผ่านรูปภาพพาสเฟส 15.088 วินาที) จึงได้ทำการเลือกนำรหัสผ่านรูปภาพพาสพอยท์มาพัฒนา

รหัสผ่านรูปภาพพาสพอยท์เมื่อนำมาวิเคราะห์ความปลอดภัย พบว่ามีภัยคุกคามหลักคือ การโจมตีแบบโชลเดอร์เซิร์ฟฟิง และ การโจมตีแบบดิกชันนารีด้วยฮอตสปอตของรูปภาพ จึงทำการป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิงด้วยเทคนิคการเพิ่มรหัสผ่านปลอมด้วยการสั่นแบบแฮปติกบนสมาร์ทโฟน ซึ่งมีผลการทดสอบแสดงให้เห็นว่าสามารถป้องกันการโจมตีดังกล่าวได้ และการเพิ่มรหัสผ่านปลอมสามารถเพิ่มขนาดของรหัสผ่านมากกว่ารหัสผ่านรูปภาพพาสพอยท์อีกด้วย (จาก 23 บิต เป็น 35 บิต สำหรับจำนวนรหัสผ่าน 4 จุด จาก 29 บิต เป็น 47 บิต สำหรับจำนวนรหัสผ่าน 5 จุด และ จาก 35 บิต เป็น 53 บิต สำหรับจำนวนรหัสผ่าน 6 จุด) ส่วนการป้องกันการโจมตีแบบดิกชันนารีด้วยฮอตสปอตผู้วิจัยได้ใช้อิมเมจซาเลียนซีโดยอัลกอริทึมดีพเกซเพื่อเป็นการวิเคราะห์ความเสี่ยงของรูปภาพก่อนที่ผู้ใช้จะสร้างรหัสผ่าน ซึ่งจากงานวิจัย [35, 42] พบว่าเทคนิคนี้สามารถลดความเสี่ยงจากการโจมตีแบบดิกชันนารีได้จริง

หลังจากที่ผู้วิจัยได้เพิ่มประสิทธิภาพในความปลอดภัยของระบบรหัสผ่าน ผู้วิจัยได้นำรหัสผ่านรูปภาพแฮปติกพอยท์ มาทดสอบผลกระทดสอบความง่ายในการใช้งานอีกครั้งพบว่าความแตกต่างระหว่างความง่ายในการใช้งานของรหัสผ่านรูปภาพพาสพอยท์และแฮปติกพอยท์นั้นไม่มีนัยสำคัญ จากผลการทดลองสามารถสรุปได้ว่า รหัสผ่านรูปภาพแฮปติกพอยท์มีความง่ายในการใช้งานลดลงอย่างไม่มีนัยสำคัญเมื่อเทียบกับรหัสผ่านรูปภาพพาสพอยท์ และมีความสามารถในการป้องกันการภัยคุกคามของรหัสผ่านรูปภาพพาสพอยท์ได้ (การโจมตีแบบโชลเดอร์เซิร์ฟฟิง และการโจมตีแบบดิกชันรีด้วยฮอตสปอต) นอกจากนั้นยังมีเอนโทรปีของรหัสผ่านที่มากกว่ารหัสผ่านรูปภาพพาสพอยท์ และยังมีความเป็นไปได้ในการใช้งานในชีวิตประจำวันอีกด้วย

5.2 ข้อเสนอแนะ

1) รหัสผ่านรูปภาพแฮปติกพอยท์สามารถป้องกันการโจมตีแบบโชลเดอร์เซิร์ฟฟิงได้ แต่ถ้าผู้โจมตีสามารถบันทึกหน้าจอของสมาร์ทโฟนในระหว่างการใส่รหัสเป็นเวลามากกว่าหนึ่งครั้งผู้โจมตีอาจนำจุดรหัสผ่านทั้งหมดมาเปรียบเทียบเพื่อนำจุดที่เป็นจุดรหัสผ่านปลอมออก รหัสผ่านก็อาจจะถูกเปิดเผยได้ ดังนั้นในการใช้งานเพื่อป้องกันภัยคุกคามนี้ผู้ใช้ควรระมัดระวังในการกดรหัสผ่าน
2) การเลือกจุดรหัสผ่านของผู้ใช้นั้นมีพฤติกรรมที่แตกต่างกับการเลือกจุดรหัสผ่านจริง เนื่องจากจะมีความใส่ใจน้อยกว่าและอาจเลือกจุดที่ไม่ควรเลือกเป็นจุดของรหัสผ่าน เช่น เลือกพื้นที่ที่ไม่มีฮอตสปอตซึ่งอาจทำให้ผู้โจมตีสามารถจำแนกได้ว่าจุดใดเป็นรหัสผ่านปลอมและจุดใดเป็นจุดรหัสผ่านจริงได้ ในอนาคตควรมีระบบแจ้งเตือนผู้ใช้เมื่อป้อนจุดรหัสผ่านที่ไม่ควรเลือก
3) ระบบรหัสผ่านที่มีความปลอดภัยสูง เพื่อเพิ่มความง่ายในการใช้งานต้องให้เวลาผู้ใช้งานในการเรียนรู้ เป็นระยะเวลาหนึ่งจึงจะคุ้นเคยกับวิธีการใช้ของระบบรหัสผ่านนี้ แต่ระยะเวลานั้นไม่ควรนานเกินไป ในงานวิจัยนี้คือหนึ่งสัปดาห์
4) วิธีการสร้างจุดรหัสผ่านปลอมของรหัสผ่านรูปภาพแฮปติกพอยท์สามารถนำไปประยุกต์ใช้กับระบบรหัสผ่านที่ใช้การกดจุดในการยืนยันตัวตนได้เช่นกัน

เอกสารอ้างอิง

[1] Enso, B., “How Consumers Remember Passwords” *Forrester Research Report*, June 2, 2004.

[2] Florencio, D. and Herley, C.,“A large-scale study of web password habits”, *proc. of the International Conference on World Wide Web (WWW 2007)*, pp.657-666, 2007.

[3] Chiasson. S., Forget, A., Stobert, E., Van Oorschot, P. and Biddle, R., “Multiple password interference in text passwords and click-based graphical passwords”, *proc. of 16th ACM conference on Computer and communications security*, pp. 500–511, 2009.

[4] Nelson, D., Reed, U. and Walling, J., “Picture superiority effect”, *Journal of Experimental Psychology : Human Learning and Memory*, Vol.2, No. 5, pp.523-528, 1976.

[5] Biddle, R., Chiasson, S. and Van Oorschot, P., “Graphical Passwords: Learning from the First Twelve Years”, Carleton University, School of Computer Science, *Technical ReportTR-11-01* , January 4, 2011.

[6] De Angeli, A., Coventry, L., Johnson, G., and Renaud, K., “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems”, *International Journal of Human-Computer Studies*, 63(1-2):128–152, 2005.

[7] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D., “The Design and Analysis of Graphical Passwords”, *proc. of USENIX Security Symposium,* 1999.

[8] Backes, M., Durmuth, M., and Unruh, D., “Compromising reflections — or — how to read LCD monitors around the corner”, *IEEE Symposium on Security and Privacy*, 2008.

[9] Hai Tao. Pass-Go, “A New Graphical Password Scheme”, Master Thesis. University of Ottawa Canada, June, 2006.

[10] Nelson, D., Reed, V. and Walling, J. “Pictorial Superiority Effect”, *Journal of Experimental Psychology: Human Learning and Memory*, 2(5):523–528, 1976.

[11] Standing, L., Conezio, J., and Haber, R., “Perception and memory for pictures: Single-trial learning of 2500 visual stimuli”, *Psychonomic Science*, 19(2), 1970.

[12] Brostoff ,S and Sasse, M. A., “Are PassfacesTM more usable than passwords? A field trial investigation”, *proc. of Human Computer Interaction*, pp. 405-424, 2000.

[13] Valentine, T., “An evaluation of the Passface personal authentication system”, *Technical report*, Goldsmiths College Univ. of London, 1999.

[14] Davis, D., Monrose, F., and Reiter, M., “On user choice in graphical password schemes”, *13th USENIX Security Symposium*, 2004.

[15] Dhamija, R. and Perrig, A. “D´ej`a Vu: A user study using images for authentication*”, 9th USENIX Security Symposium*, 2000.

[16] Hollingworth, A. and Henderson, J., “Accurate visual memory for previously attended objects in natural scenes”, *Journal of Experimental Psychology: Human Perception and Performance*, 28(1):113–136, 2002.

[17] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. and Memon, N., “PassPoints: Design and longitudinal evaluation of a graphical password system”, *International Journal of Human-Computer Studies*, pp.102–127, 2005.

[18] Wiedenbeck, S., Waters, J., Birget, J., A. Brodskiy, and Memon, N., “Authentication using graphical passwords: Basic results”, *11th International Conference on Human-Computer Interaction (HCI International)*, July 2005.

[19] Chiasson, S., Biddle, R., and Van Oorschot, P. C., “A second look at the usability of click-based graphical passwords”, *ACM Symposium on Usable Privacy and Security (SOUPS)*, July 2007.

[20] Chiasson, S., Forget, A., Stobert, E., Van Oorschot, P.C., and Biddle, R., “Multiple password interference in text and click-based graphical passwords”, *ACM Computer and Communications.*

[21] Birget, J., Hong, D., and Memon, N., “Graphical passwords based on robust discretization”, *IEEE Transactions on Information Forensics and Security*, 1(3):395–399, 2006.

[22] Suo, X., “A design and analysis of graphical password” *Master’s thesis, College of Arts and Science, Georgia State University*, August 2006

[23] Chiasson, S., Van Oorschot, P. C., and Biddle, R., “Graphical password authentication using Cued Click Points”. E*uropean Symposium On Research In Computer Security (ESORICS)*, LNCS 4734, pages 359–374, September 2007.

[24] Chiasson, S., Forget, A., Biddle, R., and Van Oorschot, P. C., “Influencing users towards better passwords: Persuasive Cued Click-Points”, *Human Computer Interaction (HCI), The British Computer Society*, September 2008.

[25] Oechslin, P., “Making a faster cryptanalytic time-memory trade-off”, *Crypto’03*, August 2003.

[26] Van Oorschot, P. C. and Wan T., “TwoStep: An authentication method combining text and graphical passwords”, *4th International MCETECH Conference on eTechnologies*, 2009.

[27] Davis, D., Monrose, F., and Reiter, M., “On user choice in graphical password schemes”. *13th USENIX Security Symposium*, 2004.

[28] Thorpe J. and Van Oorschot P. C., “Graphical dictionaries and the memorable space of graphical passwords”, *13th USENIX Security Symposium*, August 2004

[29] Van Oorschot P. C. and Thorpe, J., “On predictive models and user-drawn graphical passwords”, *ACM Transactions on Information and System Security*, 10(4):1–33, 2008.

[30] Thorpe, .J., “On the Predictability and Security of User Choice in Passwords”, *PhD thesis, School of Computer Science, Carleton University*, January 2008.

[31] Dirik, A., Menon, N., and Birget, J., “Modeling user choice in the Passpoints graphical password scheme”, 3rd *ACM Symposium on Usable Privacy and Security (SOUPS),* July 2007.

[32] Laxton, B., Wang, K., and Savage, S., “Reconsidering physical key secrecy: Teleduplication via optical decoding”, *ACM Conference on Computer and Communications Security*, 2008.

[33] Backes, M., Durmuth, M., and Unruh, D., “Compromising reflections — or — how to read LCD monitors around the corner”, *IEEE Symposium on Security and Privacy*, 2008.

[34] Roth, V., Richter, K., and Freidinger, R., “A PIN-entry method resiliant against shoulder surfing”, *11th ACM Conference on Computer and Communications Security*, 2004.

[35] Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J., “Design and evaluation of a shoulder-surfing resistant graphical password scheme”, *International Working Conference on Advanced Visual Interfaces (AVI)*, May 2006.

[36] Provos, N., Mavrommatis, P., Abu Rajab, M., and Monrose, F., “All your iFrames point to us”, *17th USENIX Security Symposium*, 2008.

[37] Dhamija, R., Tygar, J., and Hearst, M., “Why phishing works”, *ACM Conference on Human Factors in Computing Systems (CHI),* 2006.

[38] Lewis, J.R., “IBM Computer Usability Satisfaction Questionnaires : Psychometric Evaluation and Instructions for Use”, *International Journal of Human-Computer Interaction*. pp.57-78, 1995.

[39] Sobrado, L., Birget, J.C., “Graphical passwords”, *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4 (2002).

[40] Thorpe, J., Van Oorschot, P., “Human-seeded attacks and exploiting hot-spots in graphical passwords”, *16th USENIX Security Symposium on USENIX Security Symposium*, pages 8:1–8:16. USENIX Association, 2007.

[41] Narayanan, A., Shmatikov, V., “Fast dictionary attacks on passwords using time-space tradeoff”. *ACM Conference on Computer and Communications Security (CCS)*, November 2005.

[42] Alshehri, Mohamed N., “Using image saliency and regions of interest to encourage stronger graphical passwords”, The 32nd Annual Conference on Computer Security Applications, pp.127-138, 5 December, 2018.

ภาคผนวก

ภาคผนวก ก

ผลงานวิจัยที่ตีพิมพ์

Acceptance Letter for Full Paper

2018 the 8th International Workshop on Computer Science and Engineering
Bangkok, Thailand, June 28-30, 2018
(WCSE 2018)

Paper ID: W024
Paper Title: A Study of Graphical Password Usability on Smartphones in a Week

Dear Trust Ratchasan and Rungrat Wiangsripanawan,

With heartiest congratulations I am pleased to inform you that based on the recommendations of the reviewers and the Technical Program Committees, your paper identified above has been accepted for publication and oral presentation by 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018).

WCSE 2018 conference received over 100 submissions from countries and regions so far, reviewed by international experts; the acceptance ratio is controlled below 55%. Your paper will be included in the WCSE 2018 conference proceedings after registration.

Herewith, the conference committee sincerely invites you to come to present your paper at WCSE 2018 to be held in Bangkok, Thailand, June 28-30, 2018.

For more information on the conference, please check the WCSE 2018 web site at: http://wcse.us/

Yours sincerely,

WCSE 2018 Organizing Committees
Bangkok, Thailand

wcse_general@zhconf.ac.cn

WCSE International Workshop on Computer Science and Engineering

HOME/主页 ORGANIZER/组委会 ABOUT WCSE/大会信息 TRACKS FOR ATTENDEES/参会指导
WCSE 2012-2018/历史回顾 CONTACT US/联系我们

You are here: Home » WCSE 2012-2018 » WCSE 2018

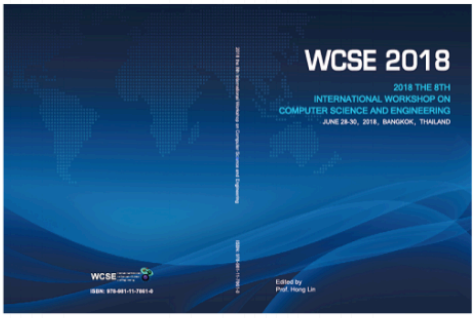
- HOME
- CALL FOR PAPERS
- ORGANIZER
- SUBMISSION
- REGISTRATION
- PROGRAM
- SPEAKERS
- VENUE
- CONTACT
- INVITATION LETTERS&VISA
- PRESENTATION INSTRUCTIONS
- WCSE 2018
- WCSE 2017
- WCSE 2016
- WCSE 2015
- WCSE 2014
- WCSE 2013
- WCSE 2012

WCSE 2018 | June 28-30, Bangkok, Thailand

Group Photo

2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018) with workshop the 6th ICITS, the 3rd ICEEI and the 3rd ICOSE was held in Bangkok, Thailand successfully during June 28-30, 2018. This year, the conference was assisted by Science and Engineering Institute, USA, University of Houston-Downtown, USA, Shanghai Information Center for Life Sciences,Chinese Academy of Sciences, China, Southeast University, China etc. Special appreciation extends to all conference committees.

Conference Proceedings (ISBN: 978-981-11-7861-0) (EI, SCOPUS successfully)



ISBN 978-981-11-7861-0
Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018)
Bangkok, 28-30 June, 2018, pp. 610-617

A Study of Graphical Password Usability on Smartphones in a Week

Trust Ratchasan[1+], Rungrat Wiangsripanawan[1]

[1] Department of Computer Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

Abstract. Smartphone technology nowadays is very progressive. With a powerful camera, high-speed connectivity, touchscreen interface, millions of different applications development and also a biometrics authentication system such as fingerprint scanner, iris scanner and even face scanner but whenever biometrics authentication system accidentally failed a smartphone still uses text passwords, PINs or Android's Unlock Pattern as a secondary authentication system but users typically create week text passwords since strong text passwords are difficult to recall and memorise. PINs and Android's Unlock Pattern are easier to recall and memorise but also having the guessablity problem. Graphical password system is one of the approach which propose of solving the memorability problem. In this paper we implemented and optimised the selected existing graphical password systems to smartphones and conducted an experiment to study and compare a usability of graphical password to the current secondary authentication system on smartphones in a week.

Keywords: user authentication, passwords, graphical passwords, usable security, human computer interaction.

1. Introduction

Biometrics authentication system on a smartphone became widespread and easily accessible. Even with high accuracy and easy for authentication but whenever biometrics authentication system is failed or unexpectedly unusable such as user's hands are too wet or the user wears personal protective equipments for example goggles, sunglasses or gloves a smartphone provides a secondary authentication system such as text password, PINs or Android's Unlock Pattern.

Text passwords are a common approach for authentication, but users normally create weak passwords and face a problem to memorise strong ones [1], [2]. Alternatively most of users prefer to use PINs and Android's Unlock Pattern as a secondary authentication system. On the other hand these authentication systems are even less secure than text passwords. Four digit PINs has only 16 bits of password space but also has very high usability for users. Android's Unlock Pattern is even easier to authenticate but has lower password space and higher guessability comparing to text passwords and PINs [3].

Graphical passwords have been proposed to solve the memorability problem based on the studies which indicated that humans are better at recognising and recalling images than texts of text passwords[4], [5], Some graphical passwords provide a high password space and against password guessing attacks that is equal to or greater than typical alphanumeric passwords, but also difficult to use such as low success rate and taking too long login time [6], there is a trade-off between usability and cryptographic strength.

In this paper we conducted an experiment to compare and evaluate usability of selected graphical password systems and PINs which is the most popular secondary authentication system in a smartphone with similar level of password strength (entropy), our study was conducted with 40 participants in a week. We developed and optimised an android application for studying participants use of selected graphical password

+ Corresponding author. Tel.: +66922733035; fax: +6623298412..
E-mail address: 58605087@kmitl.ac.th.

systems and PINs. Participants downloaded and installed the application from an email, Each user created their personal account and created one password for each graphical password scheme and used them daily in a week.

2. Graphical Password Systems

Graphical passwords are image-based passwords which are an authentication system that works by having the user select images or points of the image. They are an alternative way of solving the problem of using alphanumeric passwords [1], [2]. Graphical passwords are easier than text passwords for most people to remember [4], [5]. A study by Robert Biddle *et al*. [6] classifies and compares stereotype of graphical passwords which are Recall-based System, Recognition-based System and Cued-recall System.

2.1. Recall-based graphical password systems

Recall-based graphical password systems are also known as drawmetric systems which allows users to create passwords from drawing lines or points on empty spaces or a grid. This type of graphical password is the most difficult system to memorise since users must remember all lines without any memorisation aid. Examples of recall-based graphical password systems are Draw-a-Secret (DAS) [7], BDAS [8] and YAGP [9].

2.2. Recognition-based graphical password systems

Recognition-based graphical password systems are also known as cognometric systems or searchmetric systems. The system require users to select a set of images to create a password, then user must recognise their images from among decoys to log in, The images used are mostly people's faces, pictures, artwork and biographies. Examples of recognition-based graphical password systems are Use Your Illusion (UYI) [10] and Déjà vu [11].

2.3. Recognition-based graphical password systems

Cued-recall graphical password systems are also known as locimetric which require user choose positions or points of an image during password creation and authentication, subjects are given hints (cues) at the time of recall. The cues are supposed to help the subject recalls the memorised items. Examples of cued-recall graphical password systems are PassPoints [12] and Inkblot Authentication[13].

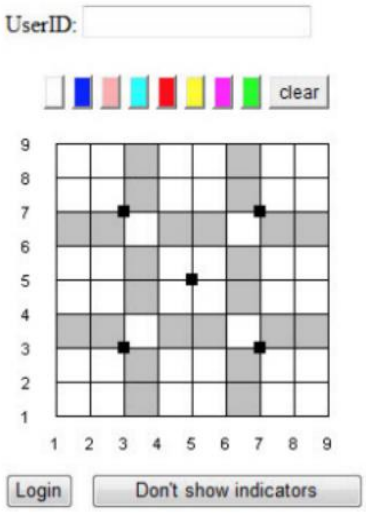


Fig. 1: User interface of PassGo

3. Related Work

3.1. PassGo

Pass-Go (Fig. 1) is a graphical password system proposed by Tao and Adams [14] which solves the Draw-a-Secret (DAS) [7] scheme issue: the difficulty of accurately duplicating sketches whose lines cross near grid lines or grid line intersections. It is named by the ancient board game Go, Pass-Go displays a grid of 9 x 9 dots and users draw their lines or points using grid intersection points. Each user's movements are snapped to gridlines and intersections, avoiding the effect of small variations in the trace. The theoretical password space of Pass-Go is larger than for DAS and PINs due to a finer grid (more squares); allowing diagonal movements (DAS encodes only horizontal and vertical movements); both resulting in greater password complexity than in DAS.

3.2. PassFaces

PassFaces is a graphical password system proposed by S.Brostoff, and M. A. Sasse [15]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognises and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. The previous studies [16], [17] have shown that PassFaces are very memorable over long period.

3.3. PassPoints

PassPoints is a cued-recall graphical password systems which proposed by S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon [12]. A password is a sequence of any n = 5 user selected click points (pixels) on a system-assigned image. The user selects points by clicking on them using a mouse. During login, re-entry of the click-points must be in the correct order, and accurate within a system-specified tolerance. The image acts as a memory cue to the location of the originally chosen click-points.

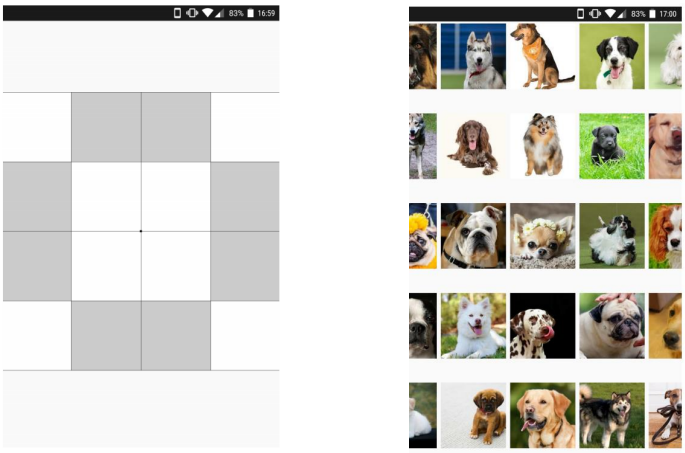
4. Experiment

4.1. Entropy Settings and Optimisations

We developed and optimised an android application as a prototype. In the following section we mentioned that we chose Pass-Go, PassFaces and PassPoints for the experiment. For PassGo it normally displays as 9 x 9 dots with multiple pen colours but for our optimisation to enhance the system more appropriate for a smartphone display size (typical smartphone display size is around 4.5" - 5.5") we scaled down a grid size to 5 x 5 (Fig. 2(a)) and remove an ability to select multiple pen colours, The theoretical password space of optimised Pass-Go is around 28 bits which is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters which is more secure than 6 digit PINs that has the theoretical password space around 20 bits.

PassFaces, The original PassFace settings had n = 4 rounds of P = 9 images per panel, with one image per panel from the set of images. The user portfolio contains exactly 4 faces, so all portfolio images are used during each login. The theoretical password space for PassFaces has cardinality P powered n, with P = 9, n = 4 yielding 6561, is around 13 bits. We optimised by increasing image per panel to 50, P = 50 and changed the number of rounds to 5, n = 5 (Fig. 2(b)) then the theoretical password space is increased to 28 bits which is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters and equivalent to optimised Pass-Go, We also did some optimisation to improve users recalling images and more user friendly by changing human faces to dog and puppy faces and for each image has its own uniqueness.

PassPoints, the original PassPoints uses click-based system and the theoretical password space was calculated by number of points(pixels) powered by a password is a sequence (n = 5) that is around 43 bits, but for a smartphone display which has smaller size than a computer display and it is also a touchscreen interface. Hence, we increased an area of tapping point on a smartphone display and the optimised theoretical password space is calculated by number of point which is 50, P = 50 and a sequence is 5, n = 5 then P powered by n is around 28 bits which is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters.



(a) (b)

Fig. 2: (a) User Interface of optimised Pass-Go (5 x 5 grid) on an android device. (b) User Interface of optimised PassFaces on an android device.

4.2. Experiment

We recruited 40 participants to involve the experiment, these participants (16 female and 24 male , age 23 - 35) are from the software development company where one of the researcher is currently working with. We assigned each participant to every optimised graphical password systems and 6 digits PINs. 83.33% of participants use pin as a secondary authentication system, 10% of participants use Android's Unlock Pattern as a secondary authentication system while the rest (6.66%) use text passwords as a secondary authentication system.

The experiment conducted at the company after working hour everyday during a week, initially at the first day users were introduced and well trained how to use the optimised graphical password systems. The participants were required to create the passwords at the first day. Afterwards, users were required to login with the initial passwords in each day. In the first day and the last day we also did the Lewis' Post-Study System Usability Questionnaire (PSSUQ) to participants [18] In the section 4.1 we set up and optimised password entropy and the selected graphical password systems have the similar theoretical password space which is 28 bits which make us easily compare and evaluate the data to 6 digits PINs.

We evaluate ease of graphical password systems access using four complimentary measures: (1) error rate of clicking incorrect points, (2) number of attempts required for successful authentication and (3) the login time required in a successful authentication.

5. Results

5.1. Error Rate

Error rate is the average rate of clicking incorrect points by all participants. Table 1 displays the distributions of error rate of each graphical password system and 6 digits PINs. Unsurprisingly, PINs has the lowest error rate between first day and last day (first day = 3.224 and last day = 0%, P = 0.0051) following by PassFaces (first day =18.98% and last day = 3.686%, P < 0.0001) then Pass-Go (first day = 24.444% and last day = 6.104%, P = 0.002) and PassPoints (first day =28.28% and last day = 13.855%, P = 0.006). The error rate is noticeably better comparing between the first day and the last day.

Table 1: Error rate result (percent)

	Day	Mean	t-test	S.d.	Min	Max
PINs	First day	3.224	t = 2.901 P = 0.0051	6.069	0	14.28
	Last day	0		0	0	0
Pass-Go	First day	24.444	t = 4.01 P = 0.002	23.428	0	70
	Last day	6.105		8.852	0	25
PassPoints	First day	28.28	t = 2.852 P = 0.006	23.93	0	73.33
	Last day	13.855		13.952	0	42.85
PassFaces	First day	18.98	t = 4.387 P < 0.0001	17.741	0	55.26
	Last day	3.686		7.708	0	20

5.2.Login Attempts

Table 2. displays the number of attempts required for successful authentication of each graphical password system. PINs has the lowest number of attempts (first day = 1.161 tries and last day = 1 try, P = 0.0425). PassGo has the most significant difference between the first day and the last day related to P value in t-test (first day = 2.355 tries and last day = 1.355 tries, P = 0.0013) following by PassFaces (first day = 1.709 tries and last day = 1.194 try, P = 0.0014) and PassPoints (first day = 1.935 tries and last day = 1.387 ties, P = 0.0075).

Table :. Login attempts result (tries)

	Day	Mean	t-test	S.d.	Min	Max
PINs	First day	1.161	t = 2.073 P = 0.0425	0.374	1	2
	Last day	1		0	1	1
Pass-Go	First day	2.355	t = 3.392 P = 0.0013	1.539	1	6
	Last day	1.355		0.486	1	2
PassPoints	First day	1.935	t = 2.772 P = 0.0075	0.964	1	5
	Last day	1.387		0.495	1	3
PassFaces	First day	1.709	t = 3.361 P = 0.0014	0.74	1	4
	Last day	1.194		0.401	1	2

5.3.Login Time

Table 3 displays the average login time required in a successful authentication of each graphical password system and 6 digits PINs in second time unit. PINs has the fastest login time (first day = 4.67 and last day = 4.344 sec, P = 0.5) and following by Pass-Go (first day = 19.305 sec and last day = 4.296 sec, P < 0.0001) then PassPoints (first day = 10.916 and last day = 4.389 sec, P < 0.0001) and PassFaces (first day = 28.755 and last day; μ = 15.088 sec, P < 0.0001). Login time on the selected graphical password systems after one week is also improved. Pass-Go and PassPoints login time in last day are similar to PINs.

5.4.Usability Results

We conducted user satisfaction experiment by using he Lewis' Post-Study System Usability Questionnaire (PSSUQ) which contains 19 usability questionnaire items and likert scale from 1 to 7. 1 means strongly disagree and 7 means strongly agree from Fig. 3 displays an average value for each graphical password system and 6 digits PINs comparing between the first day and the last day. The scores of PINs are slightly different between the first day and the last day but for the graphical password systems, the scores are significantly different and all of them are about the similar level. At the first day most of participants had negative comments for the graphical password systems for example some of them said that "why do I have to change from the current easy authentication system", "Graphical passwords are too complex" but at the last day 66.67% of participants said that they are willing to use the graphical password systems instead of 6

PINs, while 20% of participants said that they probably use the graphical password systems instead of 6 digits PINs and 13.33% of participants preferred to use 6 digits PINs than the graphical password systems.

Table :. Login time result (seconds)

	Day	Mean	t-test	S.d.	Min	Max
PINs	First day	4.67	t = 0.659 P = 0.5	1.911	1.78	9.93
	Last day	4.344		1.923	1.37	8.39
Pass-Go	First day	19.305	t = 6.612 P < 0.0001	12.258	5.14	48.51
	Last day	4.296		2.076	1.8	10.21
PassPoints	First day	10.916	t = 6.256 P < 0.0001	5.261	2.28	20.39
	Last day	4.389		2.0165	1.3	8.71
PassFaces	First day	28.755	t = 4.547 P < 0.0001	15.661	12.07	71.37
	Last day	15.088		5.074	7.51	25.74

6. Discussion and Limitations

The results from section 5 shows that after users used the graphical password systems in one week as a daily usage, error rate, login attempts, login time and usability are significantly improved and some of them are almost equivalent to 6 digits PINs with the higher theoretical password space and less guessability issue, Although the participants were well trained at the fist day but the error rate of graphical password systems are still very high.

Our findings regarding error rate and login attempts show that users could take just one week to improve. Once participants are familiar to the graphical password systems, the error rate for the selected graphical password systems PassGo and PassFaces are significantly improved. Error rate result in the last day are also comparable to 6 digits PINs. The error rate of PassPoints was slightly improved because users found that tapping at the same position on a smartphone display is a difficult task even though we already enlarged the tapping area.

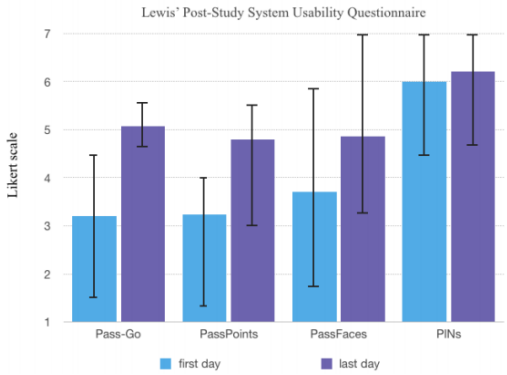


Fig. 3: PSSUQ result

Our findings regarding login time show that for each graphical password system were noticeably improved especially for PassGo. The results of Pass-Go and PassPoints at the last day are comparable to 6 digits PINs. Login time of PassFaces were about 50% improved but still taking long time compare to the others (PassFaces 14.927 sec, 6 digits PINs 4.606) because participants found that it was tough to find a password image on total 50 images per one panel.

In addition of usability, Each graphical password system has about the same likert score as we mentioned in section 5.4 most of participants are more satisfied comparing between the first day and the last

day and most of them are willing to change their secondary authentication system on a smartphone instead of 6 digits PINs.

From the experiment, although the result could show that error rate, login attempts, login time and usability were improved in a week but one of the main issue of graphical password system is shoulder surfing attack is still need to be prevented and improved, some of our selected may or may not have an ability to resist the attack.

7. Conclusions

We have presented the study of the graphical password usability on a smartphone can be significantly improved in a week with higher theoretical password space comparing to PINs and we found that there's possible to use graphical password systems as a secondary authentication system on a smartphone. In the future we would like to develop a better graphical password system on a smartphone which consists both acceptable usability and security.

8. Acknowledgement

We would like to thank F. Schaub, M. Walch, B. Könings, and M. Weber [19] for publishing an android open-source Pass-Go which can reduce huge of our application development time.

9. References

[1] B. Enso. How Consumers Remember Passwords. Forrester Research Report, June 2, 2004.

[2] D. Florencio and C. Herley. A large-scale study of web password habits. *proc. of the International Conference on World Wide Web (WWW 2007)*, pp. 657-666 (2007)

[3] S. Uellenbeck, M. Dürmuth, C. Wolf and T. Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. *proc. of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13),* pp.161-172. ACM, New York, NY, USA (2013)

[4] S. Chiasson, A. Forget, E. Stobert, P. Van Oorschot and R.Biddle. Multiple password interference in text passwords and click-based graphical passwords. *proc. of 16th ACM conference on Computer and communications security*, pp. 500–511, ACM (2009).

[5] D. Nelson, U. Reed and J. Walling. Picture superiority effect. *Journal of Experimental Psychology*, Human Learning and Memory (3), pp. 485–497 (1977).

[6] R. Biddle, S. Chiasson and P. van Oorschot. Graphical Passwords: Learning from the First Twelve Years, Carleton University - School of Computer Science, *Technical ReportTR-11-01*, January 4, 2011.

[7] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin. The Design and Analysis of Graphical Passwords. *proc. of USENIX Security Symposium* (1999).

[8] P. Dunph and J. Yan. Do Background Images Improve "Draw a Secret" Graphical Passwords? *proc. of 14th ACM Conference on Computer and Communications Security*, Virginia, USA. pp. 36-47, ACM Press, New York, October 28-31, 2007.

[9] H. C. Gao, X. W. Guo, X. P. Chen, L. M. Wang and X. Y. Liu. YAGP: Yet another graphical password strategy. *proc. of 24th Annual Computer Security Applications Conference (ACSAC 2008)*, California, USA. pp.121-129, August 8-12, 2008.

[10] E. Hayashi, R. Dhamija, N. Christin and A. Perrig. Use Your Illusion: secure authentication usable anywhere. *proc. of SOUPS '08*, ACM (2008).

[11] R. Dhamija and A. Perrig. Deja Vu: A User Study Using Images for Authentication. *proc. of 9th USENIX Security Symposium*(2000).

[12] S Wiedenbeck, J Waters, J. Birget, A. Brodskiy and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, pp.102–127 (2005).

[13] A. Stubblefield and D. R. Simon. Inkblot Authentication. Microsoft Technical Report MSR-TR-2004-85 (2004).

[14] Hai Tao. Pass-Go, a New Graphical Password Scheme, Master Thesis. University of Ottawa Canada, (June 2006).

Springer

springer.com

Springer

1st edition

Due 2019-07-06
1st ed. 2019, Approx. 200 p.

Printed book
Softcover

Printed book
Softcover
ISBN 978-3-030-17981-6
Ca. £ 59,99 | Ca. CHF 78,00 | Ca. 65,99 € | Ca. 72,59 € (A) | Ca. 70,61 € (D)
Planned

Discount group
Science (SC)

Product category
Proceedings

Series
Security and Cryptology

Computer Science : Systems and Data Security

Kang, Brent ByungHoon, Jang, JinSoo (Eds.), Korea Advanced Institute of Science and Technology, Daejeon, Korea (Republic of)

Information Security Applications

19th International Conference, WISA 2018, Jeju Island, Korea, August 23–24, 2018, Revised Selected Papers

This book constitutes the thoroughly refereed post-conference proceedingsof the 19th International Conference on Information Security Applications,WISA 2018, held on Jeju Island, Korea, in August 2018. The 11 revised full papers and 11 short papers presented in thisvolume were carefully reviewed and selected from 44 submissions. # The primary focus of WISA 2018 was on systems and network security including all other technical and practical aspects of security applications and alsoon the embedded, unmanned or autonomous systems and cyber physical systems in general.

Order online at springer.com/booksellers
Springer Nature Customer Service Center GmbH
Customer Service
Tiergartenstrasse 15-17
69121 Heidelberg
Germany
T: +49 (0)6221 345-4301
row-booksellers@springernature.com

CALL FOR PAPERS

OVERVIEW

WISA is one of the main security research venues hosted by the Korea Institute of Information Security and Cryptology (KIISC) and sponsored by the Ministry of Science, ICT and Future Planning (MSIP), and co-sponsored by the Electronics & Telecommunications Research Institute (ETRI), the Korea Internet & Security Agency (KISA), and the National Security Research Institute (NSRI).

The primary focus of WISA 2018 will be on systems and network security including all other technical and practical aspects of security applications. This year, in particular, we will be inviting participations from researchers working on vehicles, drones, and ships, who are keen on bringing open security challenges for their recent works on the embedded, unmanned or autonomous systems and cyber physical systems in general.

The areas of interest include, but are not limited to the following:

- Analysis of network and security protocols
- Anonymity and censorship-resistant technologies
- Applications of cryptographic techniques
- Authentication and authorization
- Automated tools for source code/binary analysis
- Automobile security
- Botnet defense
- Blockchain security
- Critical infrastructure security
- Denial-of-service attacks and countermeasures
- Digital Forensics
- Embedded systems security
- Exploit techniques and automation
- Hardware and physical security
- HCI security and privacy
- Intrusion detection and prevention
- Malware analysis
- Mobile/wireless/cellular system security
- Network-based attacks
- Network infrastructure security
- Operating system security
- Practical cryptanalysis (hardware, DRM, etc.)
- Side channel attacks and countermeasures
- Storage and file systems security
- Techniques for developing secure systems
- Trustworthy computing
- Trusted execution environments (Intel SGX, ARM Trustzone, etc.)
- Unmanned System Security for Vehicle/Drone/Ship Systems
- Vulnerability research
- Web security

WISA will be looking for original research papers that have not been published before. (A few selected papers will be recommended to SCIE journals). In addition, WISA will be accepting papers that report about experiences and recent enhancements of the prior works that had been published at top security conference venues. In the latter case, the papers are expected to contain new original materials, more than 30% beyond the prior works. The submission must be anonymous, with no author names, affiliations, acknowledgements, or obvious references.

ACCEPTED PAPERS

Short Session (Short Papers) : (Day1 10:00 ~ 12:00)

Track1: (Day1 10:00 ~ 12:00, Room : Crystal I)

Title:: Security Analysis of Mobile Web Browser Hardware Accessibility: Study with Ambient Light Sensors

Authors
---
1. Sanghak Lee <uzbu89@postech.ac.kr> (POSTECH)
2. Sangwoo Ji <sangwooji@postech.ac.kr> (POSTECH)
3. Jong Kim <jkim@postech.ac.kr> (POSTECH)

Abstract

Mobile web browsers are evolved to support the functionalities presented by HTML5. With the hardware accessibility of HTML5, it is now possible to access sensor hardwares of a mobile device through a web page regardless of the need for a mobile application. In this paper, we analyze the security impact of accessing sensor hardwares of a mobile device from mobile web page. First, we present the test results of hardware accessibility from mobile web browsers. Second, to raise awareness of the seriousness of hardware accessibility, we introduce a new POC attack LightTracker which infers the victim's location using light sensor. We also show the effectiveness of the attack in real world.

Title:: HapticPoints : The Extended PassPoints Graphical Password

Authors
---
1. Trust Ratchasan <trustrat@gmail.com> (KMITL)
2. Rungrat Wiangsripanawan (KMITL)

Abstract

The most common issue of alphanumeric passwords is users normal- ly create week passwords for the reason that strong passwords are difficult to recognise and memorise. Graphical password authentication system is one of the approach to address the issues of alphanumeric passwords memorability. Wiedenbeck et al. proposed PassPoints in which a password is a sequence of any 5 to 8 user-selected click points on a system-assigned image. Nevertheless PassPoints still faces the problem of predictable click points and shoulder surf- ing attack. In this paper, we purposed HapticPoints an alternative graphical password system on smartphones in which user does not need any additional memory task but be able to prevent the following problems by adding haptic feedback to PassPoints as additional decoy click points. We also conduct a user study to evaluate and compare the usability of HapticPoints and PassPoints.

HapticPoints : The Extended PassPoints Graphical Password

Trust Ratchasan and Rungrat Wiangsripanawan

Department of Computer Science, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

{58605087, rungrat.wi}@kmitl.ac.th

Abstract. The most common issue of alphanumeric passwords is users normally create weak passwords for the reason that strong passwords are difficult to recognise and memorise. Graphical password authentication system is one of the approach to address the issues of alphanumeric passwords memorability. Wiedenbeck et al. proposed PassPoints in which a password is a sequence of any 5 to 8 user-selected click points on a system-assigned image. Nevertheless PassPoints still faces the problem of predictable click points and shoulder surfing attack. In this paper, we purposed HapticPoints an alternative graphical password system on smartphones in which user does not need any additional memory task but be able to prevent the following problems by adding haptic feedback to PassPoints as additional decoy click points. We also conduct a user study to evaluate and compare the usability of HapticPoints and PassPoints.

Keywords: user authentication, passwords, graphical passwords, usable security, shoulder surfing attack, PassPoints.

1. Introduction

Alphanumeric passwords are the most common approach for authentication but users normally create weak passwords for the reason that strong passwords are difficult to recognise and memorise[1][2].

Graphical passwords have been proposed to solve the memorability problem based on the studies which indicated that humans are better at recognising and recalling images than alphanumeric passwords[2][3], Some graphical passwords provide a high password space and against password guessing attacks that is equal to or greater than typical alphanumeric passwords, but also difficult to use such as low success rate and taking too long login time[5], there is a trade-off between usability and cryptographic strength.

The previous studies[1,2] show that recognition-based graphical password systems are an easier memory task than recall-based graphical password systems. In cued-recall graphical password systems, an external cue is provided to help remember information. Tulving and Pearlstone explain that items in human memory may be available but not accessible for retrieval and show that previously inaccessible information in a pure recall situation can be retrieved with the aid of a retrieval cue[3].

PassPoints is a representative of cued-recall graphical password systems of particular interest and worthy of extensive study based on the previous study[6]. It extended

Blonder's[21] idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of the chosen pixels.

Even though, The primary security problem of PassPoints is hotspots, when users tend to select similar click points as part of their passwords. Attackers who are able to gather knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess PassPoints passwords [8, 9]. Another concern of PassPoints is a shoulder-surfing attack. When a user clicks at his/her password click points, nearby attackers can observe what points user is clicking.

In this paper, we purposed HapticPoints an alternative graphical password system on smartphones in which user does not need any additional memory task but be able to prevent the following problems by adding haptic feedback to PassPoints as additional decoy click points. We also conduct an user study to evaluate and compare the usability of HapticPoints and PassPoints.

2. Graphical Password Systems

Graphical passwords are image-based passwords which are an authentication system that works by having the user select images or points of the image. They are an alternative way of solving the problem of using alphanumeric passwords[1][2]. Graphical passwords are easier than text passwords for most people to remember[4][5]. A study by Robert Biddle et al.[6] classifies and compares stereotype of graphical passwords which are Recall-based System, Recognition-based System and Cued-recall System.

Recall-based graphical password systems. known as drawmetric systems which allows users to create passwords from drawing lines or points on empty spaces or a grid. This type of graphical password is the most difficult to memorize since users must remember all lines without any memorisation aid. Examples of recall-based graphical password systems are Draw-a-Secret (DAS)[10], BDAS[11], YAGP[12] and PassGo[15].

Recognition-based graphical password systems. known as cognometric systems or searchmetric systems, this system require users to select a set of images to create a password, then user must recognize their images from among decoys to log in, The images used are mostly people's faces, pictures, artwork, and biographies. Examples of recognition-based graphical password systems are Use Your Illusion (UYI)[13] and Deja vu[14].

Cued-recall graphical password systems. also known as locimetric which require user choose positions or points of an image during password creation and authentication, subjects are given hints (cues) at the time of recall. The cues are supposed to

help the subject recall the memorised items. Examples of cued-recall graphical password systems are PassPoints[19] and Inkblot Authentication[16].

3. PassPoints

PassPoints is a cued-recall graphical password systems which proposed by S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon[19]. A password is a sequence of any n = 5 user-selected click points (pixels) on a system-assigned image. The user selects points by clicking on them using a mouse. During login, re-entry of the click-points must be in the correct order, and accurate within a system-specified tolerance. The image acts as a memory cue to the location of the originally chosen click-points (see Fig. 1).

The underlying images of PassPoints for creating a password are not restricted to any types of images such as drawings, Perspective photos, Human face images can be used; users can even install their own images. Natural images help users remember complex passwords better. This suggests that in a human context, the (conditional) entropy of a password will depend on the underlying image, and leads to the question: Given an image, how can we predict the (conditional) entropy of a click point in that image, within the context of PassPoint passwords.

Based on the Ahmet Emir Dirik et al's study[8]. They analysed the password security of underlying images by computing the entropy of a click point by adding saliency points to the images, and they compared the predictions produced by their model with data consisting of roughly 100 actual passwords selected by users. In these (very small) images their model was able to predict 70- 80% of the user click positions. The results show that their model can be used to evaluate the suitability of an underlying image for the PassPoints system.

Fig. 1. User Interface of PassPoints.

4. Threat Model

Robert Biddle et al[6] elaborates standard threats to password-based authentication systems and how they relate to graphical passwords. Based on their study we model the threats faced in PassPoints. Attacks are classified as shoulder surfing attacks, brute force attacks, dictionary attacks and hotspots.

4.1. Shoulder Surfing Attack

Shoulder-surfing attack is a direct attack focused on the visual aspect of graphical passwords. When users are logging in or inputting passwords, attackers may directly observe or use external recording devices such as high resolution cameras and surveillance equipments to collect users' credentials.

Several existing graphical password systems tried to prevent from shoulder surfing attacks but turns out significant usability drawbacks[24], usually in the time and effort required to log in, making them less suitable for daily-usage authentication.

4.2. Brute Force Attack

Brute force attack is a trial and error method used to obtain information such as a user password by imitating the clicking on a password image. In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. An attack of this nature can be time and resource consuming. Success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

The advantage to do offline brute force attacks is that with enough time and computing power, all passwords will be found. However, full search of large password spaces is limited in practice by the time or processing power available.To minimise the threat of exhaustive attacks, the theoretical password space should be too large to search.

4.3. Dictionary Attack

The original idea involved guessing passwords from a relatively short pre-compiled list (dictionary) of high probability candidate passwords, based on assumptions about user behaviour. Massive dictionaries and powerful data structures have created a continuum from small dictionaries to prioritised brute force attacks, with smart dictionary attacks combining time-memory trade-offs of brute force attacks with higher success probabilities of prioritised dictionaries, in some cases algorithmically generated [25].

Many users' uses weak passwords which make it is easier for attackers to guess the password using the graphical dictionary attack[7].

Previous studies[8, 9] show that users' choices are predictable in most cued-recall based systems, so attackers can make use of this property. Attackers first collect images used by authentication systems, then processes and analyses the images to obtain the hotspots and patterns.

4.4. Hotspots

Hotspots[22] are remarkable points or areas of a password image with higher probability of being chosen by users as password click points. The attacks below target PassPoints itself, as opposed to evolved systems like PCCP[23].

Success in exploiting hotspots with automated image processing tools has been reported (see Fig. 2)[8]. The most efficient hotspot attacks to date [9] harvest from different users a small sample of passwords for target images, using the component click-points to build "human-seeded" attack dictionaries. One such attack uses a first-order Markov attack, a second, based on an independent probability model, assumes click-points are independent of their predecessors.

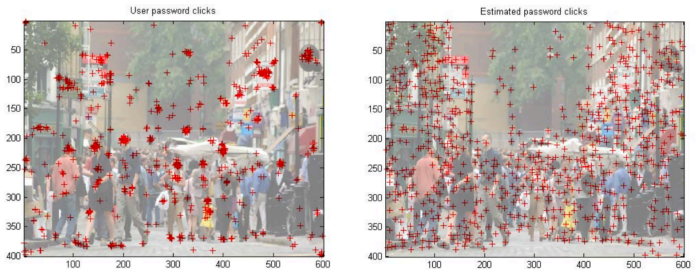


Fig. 2 A. Dirik et el. exploited hotspots with automated image processing

5. HapticPoints

We propose a graphical password authentication system on smartphones which extended from PassPoints called "HapticPoints" to enhance and prevent attacks of PassPoints which we describe in section 3. In HapticPoints we added haptic feedback randomly after a user click on a password click point to notify users that they need to create additional decoy click points.

The reason behind adding haptic feedback is when the haptic feedback vibrates, it can neither be observed by eyes nor eavesdropped by ears which means attackers may not be noticed that which click points are actual click points and which click points are decoy points. We generate the number of decoy click points (p) by:

$$decoyPoints = ciel(actualPoints/2)$$

In HapticPoints graphical password authentication system, there are two usage phases: the registration phase and the login phase.

5.1. Registration Phase

The previous study[17]. shows that their model can be used to guide suitable image selection for graphical passwords before the user selects their first click point and without requiring additional user effort by proposing a measurement for guiding images that is based on overall image saliency and contents (see Fig.2). They found that the more salient regions on an image, the higher the entropy of click points, and thus the higher the theoretical and practical password space.

In the registration phase we let users choose their own images to create passwords then we show image saliency by using Deep Gaze[18] algorithm to inform the suitability of the image to prevent dictionary attacks. The following is the complete procedure:

1. User selects his/her password image from the phone, the password image can be any types of images.
2. The selected password image will be analysed and showed overall image saliency (see Fig.3). At this step we will inform user that the more salient regions on the image, the stronger password that it could be.
3. If user confirms to use the current image as a password, Create a password by clicking on the password image in the range from 4 to 6 points in sequence (Similar to the original PassPoints)
4. Confirm the password by re-entering it correctly. Users incorrectly confirming their password could retry the confirmation or return to Step 3 or Step 1.

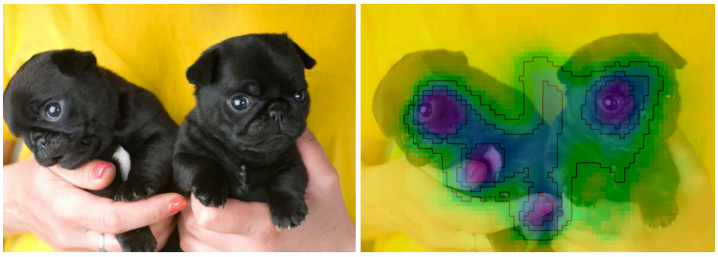


Fig. 3 An example of saliency map

Actual Password : Point A > Point B > Point C > Point D

Decoy Password : Point A > **Decoy Point** >Point B > Point C > **Decoy Point** > Point D

Or

Decoy Password : Point A > Point B > **Decoy Point** > **Decoy Point** > Point C > Point D

Fig. 4 Examples of HapticPoints password input.

5.2. Login Phase

In login phase, users use passwords created during the registration phase to log into HapticPoints (see Fig.4-5). The following is the complete procedure:

1. User starts clicking the first password click point of a password image.
2. If the haptic feedback vibrates, user needs to create a decoy click point by clicking any area in the password image and If the haptic feedback doesn't vibrate, user needs to click on the actual click point of the current password sequence.
3. Continue following Step1 and Step 2 until user finished inputting password.
4. If users noticed an error during login, they could cancel their login attempt and try again in Step 1.

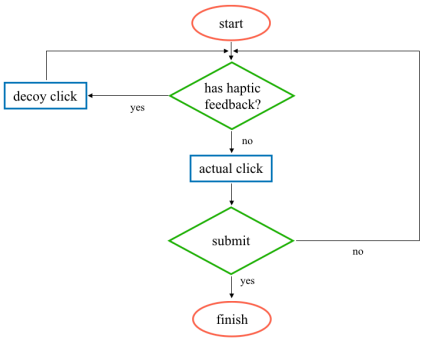


Fig. 5 HapticPoints login flow

6. Usability Evaluation

We developed a prototype on android operating system as an application and we also recruited 20 participants to involve the experiment, these participants (8 female and 12 male , age 24 - 32) are from the software development company where one of the researcher is currently working with.

The experiment started with a tutorial phase, in which participants had to enter a PassPoints password followed by HapticPoints password on the smartphone. The application continued to challenge the participants as soon as both passwords had been entered successfully. Then, each participant had to create their own passwords.

We assessed usability with a combination of quantitative and qualitative metrics. A scheme's efficiency is measured by number of attempts required for successful login and the entry time required for a login, effectiveness is assessed with the recall success rate. The usability questionnaire provides qualitative data on user satisfaction based on participant ratings onLewis' Post- Study System Usability Questionnaire (PSSUQ) to participants[20].

6.1. Login Attempts

Table 1 displays the number of attempts required for successful authentication of each graphical. HapticPoints was taken slightly more attempts than PassPoints (PassPoints = 1.645 tries, HapticPoints = 1.709 tries and P = 0.759). A T-test analysis for PassPoints and HapticPoints password revealed no significant difference.

Scheme	Mean	S.d.	Min	Max	t-test
Original PassPoints	1.645	0.797	1	4	t = 0.308 P = 0.759
HapticPoints	1.709	0.824	1	4	

Table 1. Login attempts result (tries)

6.2. Login Time

Table 2 displays the average login time required in a successful authentication of PassPoints and HapticPoints, Login time is also no significant difference between PassPoints and HapticPoints from a T-test analysis (PassPoints = 8.421 seconds, HapticPoints = 10.278 seconds, P = 0.0782).

Scheme	Mean	S.d.	Min	Max	t-test
Original PassPoints	8.421	3.838	3.35	15.52	t = 1.793 P = 0.0782
HapticPoints	10.278	4.178	4.01	17.37	

Table 2. Login time result (seconds)

6.3. Recall Success Rate

In PassPoints scheme, the nature of many recall success rate was down to either forgetting the password length or clicking points outside the tolerance region. We conducted an experiment to compare recall success rate between PassPoints and Haptic Points. We separated the time range of the experiment to two groups which are one hour and one week.

Table compares the recall success rate for one hour test and one week test. From a T-test analysis shows that the recall success rate of both HapticPoints is similar to PassPoints.

	Scheme	Mean	S.d.	Min	Max	t-test
One hour test	PassPoints	95.97	9.347	75	100	t = 0.912 P = 0.365
	HapticPoints	93.548	11.12	75	100	
One week test	PassPoints	67.741	29.006	0	100	t = 0.2002 P = 0.842
	HapticPoints	66.129	33.259	0	100	

Table 3. Recall success rate result (seconds)

6.4. Usability Questionnaire (PSSUQ)

We conducted user usability experiment by using he Lewis' Post-Study System Usability Questionnaire (PSSUQ)[20] which contains 19 usability questionnaire items perceived usefulness of the scheme in completing the given tasks (SysUse), perceived quality of displayed information (InfoQual) and interface elements (InterQual). and overall satisfaction with the scheme (Overall). Likert scale from "1" to "7". "1" means strongly disagree and "7" means strongly agree. Fig. 6 shows the results for each scheme. A T-test found no significant differences between PassPoints and HapticPoints for any of the scores ($t = 0.4412$, $P = 0.634$).

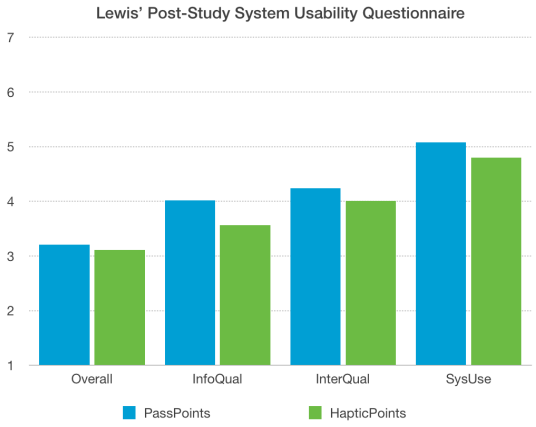


Fig. 6 PSSUQ Result.

7. Security Evaluation

7.1. Brute Force Attack

We calculate the entropy of haptic points password to quantify the security of haptic points against brute force attacks. Entropy means the quantity of information inside the password space, i.e., all possible passwords, in bits.

We implement a prototype to a smartphone which has 5 inches display size, and the number of total tolerance squares is 60 (6 in horizontal and 10 in vertical). Table 4 shows and compares the calculated password entropy between the original PassPoints and HapticPoints. We can find that the password strength of HapticPoints 4 click points password is similar to PassPoints 6 click points password which also is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters. From the result, it shows that our proposed scheme is more secure than PassPoints in practice against brute force attacks.

7.2. Shoulder Surfing Attack

We followed the common approach of having participants act as shoulder surfers [26, 27, 28, 29]. Participants acted as shoulder surfers and the experimenter acted the victim. This setup has the advantage that the experimenter could train password entry in advance, to ensure consistent entry speed and body posture for all participants. Thus, we evaluated a casual observer's ability to recognise a password entered by a trained user, compared to evaluating an expert shoulder surfer with a beginner user in the reverse setup. The average age of the participants was 29 years old. The youngest

participant was 23 years old and the oldest was 44 years old.

The shoulder surfing experiment was conducted after the usability experiment. The right-handed experimenter sat at a table holding a smartphone as if entering a password and the participant could position herself left, right, or behind the experimenter. We also limited the number of login attempts for shoulder surfers to 4 times.

The shoulder surfing result of PassPoints is 12 out of 20 (60%) shoulder surfers could crack the password but the result of HapticPoints is 1 out of 20 (5%) shoulder.

	Number of click point(s)		
	4	5	6
Orignal PassPoints Entropy	23 bits	29 bits	35 bits
HapticPoints Entropy	35 bits	47 bits	53 bits

Table 4. The entropy in bits of the original PassPoints compared with HapticPoints.

7.3. Dictionary Attack and Hotspots

In general graphical password systems are vulnerable to the threat of dictionary attacks. Attackers can collect the image of PassPoints and perform an automated image processing [8] to obtain hotspots and patterns. However we enhanced an ability to avoid dictionary attacks by adding image saliency [17, 18]. A more complex image can provide more possible click points that users actually select, thus potentially encouraging the user to create a less guessable password, or at least one that is more computationally intensive and time consuming for an attacker. This also has the effect of spreading potential user password click points, and thus potential hotspots, over an image, which may make dictionary attacks that need to consider all hotspots less feasible.

8. Limitation

We can only increase the cost of shoulder surfing attack. If the attacker is able to observe multiple login sessions then clicking points may be revealed based on the intersection and correlation among the observations. HapticPoints is not fully resistant to shoulder surfing attack, but still stronger than PassPoints because if PassPoints passwords are being screen recorded or observed, attackers could possibly crack passwords in only one time.

9. Conclusion

In order to solve the security problems of PassPoints (shoulder surfing attack, brute force attack and dictionary attack), we propose a PassPoints based graphical-password authentication system called HapticPoints. By adding haptic feedback to create decoy click points and a sequence of 4-6 click-points that user selects in the password image. We implemented a prototype as an android application of HapticPoints and conducted a user study. The experiment results shows that the password becomes stronger and be able to prevent the attacks while the usability is slightly decreased.

HapticPoints provides 47 bits entropy (with 5 click points) against brute force attacks which is higher than PassPoints (29 bits). Moreover, we enhanced an ability to prevent dictionary attacks by adding image saliency at the registration phase to inform the suitability of the user's password image.

References

1. J. Li, Y. Jiang, R. Fan. Recognition of Biological Signal Mixed Based on Wavelet Analysis. In: Y. Jiang, et al (eds.). *Proc. of UK-China Sports Engineering Workshop*. Liverpool: World Academic Union. 2007, pp. 1-8.
2. R. Dewri, and N. Chakraborti. Simulating recrystallization through cellular automata and genetic algorithms. *Modelling Simul. Mater. Sci. Eng*. 2005, **13** (3): 173-183.
3. A. Gray. *Modern Differential Geometry*. CRE Press, 1998.
4. B. Enso. How Consumers Remember Passwords. *Forrester Research Report*, June 2, 2004.
5. D. Florencio and C. Herley. A large-scale study of web password habits. Proceedings of the International Conference on World Wide Web, (WWW 2007), 657-666.
6. R. Biddle, S. Chiasson and P. van Oorschot. Graphical Passwords: Learning from the First Twelve Years, Carleton University - School of Computer Science, *Technical ReportTR-11-01* , January 4, 2011.
7. S.Chiasson, et al. Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. ACM, 2009.
8. A. Dirik, N. Memon, and J. Birget. Modeling user choice in the passpoints graphical password scheme. In Proceedings of the 3rd symposium on Usable privacy and security, pages 20–28. ACM, 2007.
9. J. Thorpe and P. van Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, pages 8:1–8:16. USENIX Association, 2007.
10. I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin. The Design and Analysis of Graphical Passwords. *proc*. *of USENIX Security Symposium* (1999).
11. P. Dunph and J. Yan. Do Background Images Improve "Draw a Secret" Graphical Passwords?. p*roc*. *of 14th ACM Conference on Computer and Communications Security*, Virginia, USA. pp.36-47, ACM Press, New York, October 28-31, 2007.

12. H. C. Gao, X. W. Guo, X. P. Chen, L. M. Wang and X. Y. Liu. YAGP: Yet another graphical password strategy. *proc. of 24th Annual Computer Security Applications Conference (ACSAC 2008)*, California, USA. pp.121-129, August 8-12, 2008.
13. E. Hayashi, R. Dhamija, N. Christin and A. Perrig. Use Your Illusion: secure authentication usable anywhere. *proc. of SOUPS '08*, ACM (2008).
14. R. Dhamija and A. Perrig. Deja Vu: A User Study Using Images for Authentication. *proc. of 9th USENIX Security Symposium*(2000).
15. Hai Tao. Pass-Go, a New Graphical Password Scheme, Master Thesis. University of Ottawa Canada, (June 2006).
16. A. Stubblefield and D. R. Simon. Inkblot Authentication. Microsoft Technical Report MSR-TR-2004-85 (2004)
17. Mohammad N. Alshehri and C. Heather. Using Image Saliency and Regions of Interest to Encourage Stronger Graphical Passwords. ACSAC '16, Los Angeles, CA, USA. (December 2016)
18. M. Kummerer, L. Theis, and M. Bethge, "Deep Gaze I: Boosting ¨ saliency prediction with feature maps trained on ImageNet," arXiv preprint arXiv:1411.1045, 2014.
19. S Wiedenbeck, J Waters, J. Birget, A. Brodskiy and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, pp.102–127 (2005)
20. J.R. Lewis. IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use, *International Journal of Human-Computer Interaction*. pp. 57–78 (1995)
21. G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.
22. K. Golofit. Click passwords under investigation. In 12th European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007.
23. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. Influencing users towards better passwords: Persuasive Cued Click-Points. In Human Computer Interaction (HCI), The British Computer Society, September 2008.
24. S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In International Working Conference on Advanced Visual Interfaces (AVI), May 2006.
25. A. Narayanan and V. Shmatikov. Fast dictionary attacks on passwords using time-space tradeoff. In ACM Conference on Computer and Communications Security (CCS), November 2005.
26. J. Nicholson. Design of a Multi-Touch Shoulder Surfing Resilient Graphical Password. Dissertation, Newcastle University, 2009.
27. F. Tari, A. A. Ozok, and S. H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In SOUPS'06. ACM, 2006.
28. D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier. Multi-touch authentication on tabletops. In CHI '10. ACM, 2010.
29. N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan. Shoulder surfing defence for recall-based graphical passwords. In SOUPS'11. ACM, 2011.

ประวัติผู้เขียน

ชื่อ	นายธรรศ รัชสัน
วัน เดือน ปีเกิด	27 กรกฎาคม พ.ศ. 2536
ที่อยู่	143/5 หมู่ 1 ตำบลบางคูวัด อำเภอเมือง จังหวัดปทุมธานี 12000
ประวัติการศึกษา	2558 วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ 2561 วิทยาศาสตรมหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ
ผลงานวิชาการ	Trust Ratchasan and Rungrat Wiangsripanawan, "Study of Graphical Password Usability on Smartphones in a Week," Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018), 28-30 June, 2018, Bangkok, pp. 610-617. Trust Ratchasan and Rungrat Wiangsripanawan, "HapticPoints : The Extended PassPoints Graphical Password" Lecture Notes in Engineering and Computer Science: Proceedings of 19th World Conference on Information Security Applications (WISA 2018), 23-25 August, 2018, Jeju Island, South Korea.