อิทธิพลของวิธีการนำเสนอรูปภาพใบหน้าบุคคล และจำนวนรอบในการตั้งรหัสผ่านที่มีผลต่อการระลึกได้ของรหัสผ่าน

โดย

นายนิพัทธิ์ ภัทรโสภณกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2557

อิทธิพลของวิธีการนำเสนอรูปภาพใบหน้าบุคคล และจำนวนรอบในการตั้งรหัสผ่านที่มีผลต่อการระลึกได้ของรหัสผ่าน

โดย

นายนิพัทธิ์ ภัทรโสภณกุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2557

EFFECTS OF FACIAL IMAGE DISPLAYS AND PASSWORD SETTING TURNS ON PASSWORD RECALL

BY

MR. NIPAT PATTARASOPHONKUL

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE PROGRAM IN COMPUTER SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
FACULTY OF SCIENCE AND TECHNOLOGY
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2014

มหาวิทยาลัยธรรมศาสตร์
คณะวิทยาศาสตร์และเทคโนโลยี

วิทยานิพนธ์

ของ

นายนิพัทธิ์ ภัทรโสภณกุล

เรื่อง

อิทธิพลของวิธีการนำเสนอรูปภาพใบหน้าบุคคล
และจำนวนรอบในการตั้งรหัสผ่านที่มีผลต่อการระลึกได้ของรหัสผ่าน

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต

เมื่อ วันที่ 10 สิงหาคม พ.ศ. 2558

ประธานกรรมการสอบวิทยานิพนธ์ _____
(อาจารย์ ดร. รัชต พีชวณิชย์)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร. ณัฐธนนท์ หงส์วริทธิ์ธร)

กรรมการสอบวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร. เสาวลักษณ์ วรรธนาภา)

กรรมการสอบวิทยานิพนธ์ _____
(ดร. มารุต บูรณรัช)

คณบดี _____
(รองศาสตราจารย์ ปกรณ์ เสริมสุข)

หัวข้อวิทยานิพนธ์	อิทธิพลของรูปภาพใบหน้าบุคคลที่มีผลต่อการระลึกได้ของรหัสผ่าน
ชื่อผู้เขียน	นายนิพัทธิ์ ภัทรโสภณกุล
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผู้ช่วยศาสตราจารย์ ดร. ณัฐธนนท์ หงส์วริทธิ์ธร
ปีการศึกษา	2557

บทคัดย่อ

ระบบคอมพิวเตอร์ส่วนใหญ่จำเป็นต้องมีการพิสูจน์ตัวตนด้วยรหัสผ่านเพื่อเข้าใช้ระบบ รหัสผ่านที่นิยมใช้คือรหัสผ่านแบบตัวอักษรที่ถูกผู้ใช้สร้างขึ้นมาในขั้นตอนการลงทะเบียน หากผู้ใช้ไม่สามารถยืนยันรหัสผ่านได้อย่างถูกต้องจะไม่สามารถเข้าใช้งานระบบได้ ฉะนั้นผู้ใช้จึงเลือกใช้รหัสผ่านที่จำง่าย หรือคำที่มีความหมายสามารถเดารหัสผ่านได้ง่าย จึงทำให้มีผู้ไม่หวังดีพยายามโจรกรรมรหัสผ่านด้วยวิธีการต่างๆ ระบบต่างๆจึงเพิ่มความปลอดภัยด้วยการบังคับให้ผู้ใช้สร้างรหัสผ่านตามกฎเกณฑ์ที่วางไว้เพื่อไม่ให้ผู้ไม่หวังดีสามารถเดารหัสผ่านได้ง่าย ปัญหาจึงเกิดกับผู้ใช้คือยากต่อการจดจำรหัสผ่าน หนึ่งในกระบวนการพิสูจน์ตัวตนที่นำมาแก้ปัญหานี้คือ การพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ จากการศึกษาเกี่ยวกับความจำของมนุษย์พบว่ามนุษย์สามารถจดจำภาพบุคคลได้ดีกว่าวัตถุอื่น จึงได้มีการนำรูปภาพใบหน้าบุคคลมาเป็นปัจจัยในการศึกษาเกี่ยวกับรหัสผ่านรูปภาพ โดยที่งานวิจัยนี้ได้นำรูปภาพใบหน้าบุคคลแบ่งเป็น 4 ประเภท คือ ผู้ชาย ผู้หญิง เด็ก และการ์ตูน มาให้ผู้ใช้เลือกเป็นรหัสผ่านและให้ผู้ใช้พิมพ์ตัวอักษรภาษาอังกฤษที่ถูกสุ่มขึ้นมาใต้รูปภาพเพื่อเพิ่มความยากในการโจรกรรมรหัสผ่าน ใช้รูปแบบการทดลองแบบ 2x2 Between Subjects Design มีผู้เข้าร่วมการทดลองจำนวน 80 คน แบ่งออกเป็น 4 กลุ่มการทดลอง กลุ่มการทดลองละ 20 คน ศึกษา 2 ปัจจัย คือ ลักษณะของรูปภาพใบหน้าบุคคล ระหว่างการใช้รูปภาพใหญ่แบ่งเป็น 9 ส่วนย่อยกับการใช้รูปภาพเล็ก และปัจจัยจำนวนรอบของการสร้างรหัสผ่าน ระหว่างจำนวนรอบในการสร้างรหัสผ่าน 1 รอบ กับจำนวนรอบในการสร้างรหัสผ่าน 2 รอบ โดยมีการวิเคราะห์ผลการทดลองด้านประสิทธิภาพการใช้งาน ความปลอดภัย และความพึงพอใจต่อรหัสผ่านรูปภาพ

ผลการทดลองด้านการใช้งานแสดงให้เห็นว่า ปัจจัยลักษณะของรูปภาพใบหน้าบุคคลมีอิทธิพลต่อการระลึกได้ของรหัสผ่านอย่างมีนัยสำคัญ โดยลักษณะรูปภาพใบหน้าใหญ่แบ่งเป็นส่วนๆ สามารถทำให้ผู้ใช้จำรหัสผ่านได้ดีกว่ารูปภาพย่อย ซึ่งสอดคล้องกับทฤษฎีทางจิตวิทยาเกี่ยวกับการจดจำใบหน้า ส่วนผลการทดลองด้านความปลอดภัย พบว่า การโจรกรรมรหัสผ่านด้วยวิธีการแอบมอง (Shoulder Surfing) ไม่สามารถพิสูจน์ตัวตนได้สำเร็จ สำหรับผลการวิเคราะห์ความพึงพอใจของผู้เข้าร่วมการทดลองสามารถสรุปโดยรวมได้ว่า ผู้เข้าร่วมการทดลองมีความพึงพอใจต่อโปรแกรมการพิสูจน์ตัวตน

คำสำคัญ: การพิสูจน์ตัวตน, รหัสผ่าน, การโจรกรรมรหัสผ่านด้วยวิธีการแอบมอง

Thesis Title	EFFECTS OF FACIAL IMAGE DISPLAYS AND PASSWORD SETTING TURNS ON PASSWORD RECALL
Author	Mr. Nipat Pattarasophonkul
Degree	Degree of Master of Science Program in Computer Science
Department/Faculty/University	Department of Computer Science Faculty of Science and Technology Thammasat University
Thesis Advisor	Asst. Prof. Dr. Nuttanont Hongwarittorrn
Academic Years	2014

ABSTRACT

Most of the computer systems nowadays require users to verify themselves before logging into the system. The widely used verification system is an alphabetical logging in system which users create for registration process. If users cannot verify themselves, they cannot log in. For this reason, most users tend to set password that either too general or easy to guess which can be easily hacked. Hence, computer systems try to protect users by setting up the rules & regulations for creating the password so that it will not be hacked easily, however, to remember the complicated password that users are not familiar with is quite difficult, so image verification has been applied as the solution. According to the study of human memory, it indicates that humans can memorize image better than other objects, therefore, humans' faces are taken into account as one of the factor to study image verification. Humans' faces are categorizes into 4 groups, some of which are men, women, children, and cartoon for users to select as the password. Then users must type English letters that will randomly appear under the images to strengthen the verification process. The test applies 2x2 Between Subject Design method with the sample size of 80 person and classify into 4 groups, each group contain 20 persons.

The research would like to study 2 topics which are the shape of humans' faces between big image sizes that separates into 9 sections and small image size and the differences between creating the password for 1 time and 2 times test which based on efficiency, security, and satisfaction of image verification.

The research findings indicate that the shape of humans' faces is the significant factor because users recognize password better with big size images of humans' faces that separates into 9 sections compared to small size image. The reason is because to memorize images that are separated into parts is easier than memorize the whole face. The findings also matche the face recognition of psychological theory For security, the research indicates that hacking password by Shoulder Surfing cannot verify users successfully. For satisfaction of people who participate in the test, the research found that overall they are satisfied with the user verification program.

Keywords: Authentication, Password, Shoulder Surfing

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไกได้ดี ด้วยความกรุณาจาก อาจารย์ ดร.รัชต พีชวณิชย์ ประธานกรรมการสอบวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.เสาวลักษณ์ วรรธนาภา และ ดร.มารุต บูรณรัช กรรมการสอบวิทยานิพนธ์ ที่เสียสละเวลาในการเป็นกรรมการสอบและให้ข้อเสนอแนะในการแก้ไขวิทยานิพนธ์ โดยเฉพาะอย่างยิ่งผู้ช่วยศาสตราจารย์ ดร.ณัฐธนนท์ หงส์วริทธิ์ธร กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ให้ความอนุเคราะห์แนะนำแนวคิด แนวทางการทำงานวิจัย การแก้ปัญหาที่เกิดขึ้นในการดำเนินงานวิจัยตลอดจนตรวจสอบข้อบกพร่องของงานวิจัย เพื่อให้วิทยานิพนธ์มีความถูกต้องและสมบูรณ์ ข้าพเจ้ามีความรู้สึกซาบซึ้งในความกรุณาและขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอกราบขอบพระคุณคณาจารย์ทุกท่านที่มีส่วนในการประสิทธิ์ประสาทวิชาให้แก่ข้าพเจ้า และขอขอบพระคุณเจ้าหน้าที่ประจำภาควิชาวิทยาการคอมพิวเตอร์ทุกท่านที่ให้ความช่วยเหลือและอำนวยความสะดวกในทุกเรื่อง ตลอดระยะเวลาของการศึกษาอละดำเนินการวิจัย

ขอขอบพระคุณพนักงานการประปาส่วนภูมิภาคสาขาในสังกัดการประปาส่วนภูมิภาค เขต 2 ที่สละเวลาในการทำการทดลองของวิทยานิพนธ์ฉบับนี้

ขอขอบคุณเพื่อนๆทุกคน ในมิตรภาพ และคำปรึกษาในด้านต่างๆ ท้ายที่สุดขอขอบพระคุณครอบครัวที่คอยห่วงใย สนับสนุนและเป็นกำลังใจตลอดมา

นายนิพัทธิ์ ภัทรโสภณกุล

สารบัญ

สารบัญตาราง

สารบัญภาพประกอบ

บทที่ 1

บทนำ

1.1 ความเป็นมา และความสำคัญของงานวิจัย

ระบบคอมพิวเตอร์เข้ามามีบทบาทในชีวิตประจำวันของผู้คนมากขึ้นทั้งเรื่องการงาน การเรียน และเรื่องส่วนตัว ทำให้ระบบคอมพิวเตอร์ต่างๆต้องมีกระบวนการพิสูจน์ตัวตน (Authentication) เพื่อเป็นการยืนยันตัวบุคคลหรือเป็นการตรวจสอบสิทธิ์ก่อนการเข้าใช้งานหรือการเข้าถึงทรัพยากรต่างๆในระบบ เทคนิคหนึ่งที่นิยมใช้กันอย่างแพร่หลายในระบบคอมพิวเตอร์สำหรับกระบวนการพิสูจน์ตัวตน คือการพิสูจน์ตัวตนด้วยรหัสผ่าน(Password) ซึ่งรหัสผ่านนั้นเริ่มมีการใช้งานมาตั้งแต่ปี 1960 เป็นชุดของตัวอักษรที่ผู้ใช้ได้สร้างขึ้นจากขั้นตอนของการลงทะเบียนเข้าใช้งานระบบในครั้งแรก เมื่อผู้ใช้ต้องการเข้าใช้งานระบบจะต้องยืนยันรหัสผ่านที่ได้สร้างขึ้นให้ถูกต้องจึงจะสามารถเข้าใช้งานระบบหรือบริการต่างๆได้ตามสิทธิ์ที่ได้รับ หากไม่สามารถยืนยันรหัสผ่านของตนเองได้อย่างถูกต้องก็จะไม่สามารถเข้าใช้งานระบบได้ ทำให้ผู้ใช้พยายามที่จะสร้างรหัสผ่านที่ตนเองสามารถจำได้ (Memorability) ในเว็บไซต์ (gizmodo.com,2012) ได้นำเสนอรหัสผ่านที่ผู้ใช้นิยมสร้างมากที่สุด 25 อันดับ ในปี 2012 พบว่า รหัสผ่านที่ผู้ใช้นิยมมากที่สุดได้แก่ “password” , “123456” , “qwerty” , “iloveyou” , “football” เป็นต้น สังเกตว่า รหัสผ่านที่ได้รับความนิยมจะถูกสร้างขึ้นมาจากชุดตัวอักษรหรือตัวเลขที่เรียงลำดับกันบนแป้นพิมพ์ รวมทั้งเป็นประโยคหรือคำศัพท์ต่างๆที่คุ้นเคยหรือเป็นที่ชื่นชอบของผู้ใช้ ซึ่งสอดคล้องตามหลักการจำของมนุษย์ หากรหัสผ่านที่ถูกสร้างขึ้นนั้นสอดคล้องกับประสบการณ์เก่าหรือสิ่งที่ผู้ใช้เคยประสบมาก่อนจะส่งผลให้ผู้ใช้สามารถจำรหัสผ่านที่สร้างได้ง่ายขึ้น แต่การสร้างรหัสผ่านในลักษณะเช่นนี้จะเกิดปัญหาด้านความปลอดภัย (Security) อาจทำให้ผู้ที่ไม่หวังดีสามารถขโมยหรือคาดเดารหัสผ่านได้โดยอาศัยหลักการที่เรียกว่า Dictionary Attack เป็นการสุ่มเดารหัสผ่านจากคำศัพท์ต่างๆที่ได้มีการรวบรวมไว้ หากรหัสผ่านที่ผู้ใช้สร้างขึ้นมีลักษณะเป็นคำหรือประโยคสั้นๆจะส่งผลให้ผู้ไม่หวังดีสามารถสุ่มเดารหัสผ่านได้ ทำให้เกิดความเสียหายต่อผู้ใช้และระบบคอมพิวเตอร์ ระบบต่างๆในปัจจุบันจึงจำเป็นต้องออกกฎเกณฑ์เพื่อไม่ให้ผู้ใช้สร้างรหัสผ่านที่ง่ายต่อการคาดเดา ถือเป็นมาตรการสร้างความปลอดภัยให้แก่ระบบและผู้ใช้งาน เช่น เว็บไซต์ (appleid.apple.com) ได้กำหนดกฎในการสมัคร Apple ID ว่ารหัสผ่านที่สร้างขึ้นจะต้องประกอบด้วย อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ อักษรภาษาอังกฤษตัวพิมพ์เล็ก และตัวเลข รวมทั้งต้องมีความยาวของรหัสผ่าน 8 ตัวขึ้นไป หรือ เว็บไซต์ (outlook.com)

กำหนดว่ารหัสผ่านที่ถูกสร้างขึ้นต้องมีความยาวอย่างน้อย 8 ตัว และประกอบไปด้วยอย่างน้อย 2 อย่างจาก อักษรภาษาอังกฤษตัวพิมพ์ใหญ่, ตัวพิมพ์เล็ก, ตัวเลข และอักขระพิเศษ เป็นต้น การออกกฎเกณฑ์ต่างๆเหล่านี้ ถึงแม้จะเป็นการเพิ่มความปลอดภัย แต่กลับก่อให้เกิดปัญหาที่ผู้ใช้งานไม่สามารถจำรหัสผ่านของตนเองได้ เนื่องจากรหัสผ่านที่ถูกสร้างขึ้นไม่ได้ถูกเชื่อมโยงในลักษณะของความหมาย จากปัญหาดังที่ได้กล่าวมาในข้างต้น ทำให้สิ่งที่ควรคำนึงถึงในการค้นหาเทคนิควิธีในการสร้างรหัสผ่านที่ส่งผลให้ผู้ใช้จำได้ง่าย และมีความปลอดภัยสูง รวมทั้งต้องมีความง่ายต่อการใช้งาน (Usability) ของผู้ใช้

รหัสผ่านแบบรูปภาพ (Graphical Password) เป็นรหัสผ่านอีกรูปแบบหนึ่ง โดยเปลี่ยนจากการสร้างรหัสผ่านจากชุดอักขระบนแป้นพิมพ์เป็นการสร้างรหัสผ่านจากการเลือกรูปภาพหรือนำภาพมามาสร้างเป็นรหัสผ่านแทน ซึ่งเป็นวิธีที่ดีเพื่อรองรับการขโมยหรือสุ่มเดาจากผู้ไม่หวังดีที่อาศัยเทคนิค Dictionary Attack ได้ ทั้งนี้รหัสผ่านแบบรูปภาพยังสอดคล้องกับหลักการรับรู้ของมนุษย์ที่สามารถรับรู้รูปภาพได้ดีกว่าตัวอักษร จากงานวิจัยทางด้านจิตวิทยาพบว่ามนุษย์สามารถจำรูปภาพและระลึกถึงภาพที่เคยได้เห็นมาก่อนได้ดีกว่าแบบตัวอักษร (Kristin & Heather, 2004) ซึ่งหากผู้ใช้งานสามารถจำรูปภาพจำนวนมากๆได้ จะเพิ่มความยากในการขโมยรหัสผ่านจากผู้ที่ไม่หวังดี

กระบวนการจำของมนุษย์ตามหลักทางจิตวิทยาเริ่มจากการรับรู้สิ่งเร้าเข้าสู่สมอง ต้องอาศัยการฝึกทบทวนซ้ำจึงจะสามารถจำได้ แต่ถ้ามีการนำประสบการณ์หรือความรู้เก่ามาใช้ร่วมกับสิ่งเร้า จะทำให้เกิดการระลึกได้ (Recall) (อุบลวรรณ ภวกานันท์, 2555) เช่น หากเราเคยไปเที่ยวทะเลแห่งหนึ่ง เมื่อเวลาผ่านไปแล้วได้เห็นรูปภาพทะเล อาจทำให้เราระลึกได้ว่าเคยไปมาแล้วเมื่อไหร่ และไปกับใคร เป็นต้น หากมีการนำรูปภาพหนึ่งมาช่วยในขั้นตอนการสร้างรหัสผ่าน น่าจะช่วยให้ผู้ใช้สามารถระลึกรหัสผ่านที่ตนเองสร้างขึ้นได้หากเห็นรูปภาพนั้นอีกครั้ง

ในปี 2005 (www.realuser.com,2005) ได้นำเสนอวิธีการที่เรียกว่า Passface วิธีนี้ผู้ใช้งานเลือกรูปภาพหน้าบุคคลมา 4 รูปภาพโดยระบบจะแสดงรูปภาพบุคคลมาให้เลือกซึ่งมีรูปภาพหน้าบุคคลที่ไม่ใช่รูปภาพที่ใช้งานเลือกแสดงด้วยเพื่อเป็นรูปภาพหลอก รูปภาพบุคคลทั้ง 4 รูปนั้นจะนำมาเป็นรหัสผ่านรูปภาพให้กับผู้ใช้งานต่อไป ในขั้นตอนการพิสูจน์ตัวตน (Authentication) ระบบจะแสดงรูปภาพหน้าบุคคล 9 รูปในแบบกริดซึ่งจะมีรูปภาพบุคคลเพียงหน้าเดียวที่ผู้ใช้งานต้องเลือกรูปภาพที่เป็นรหัสผ่านของผู้ใช้งาน ระบบจะแสดงรูปขึ้นมาหลายชุดจนผู้ใช้งานเลือกรูปภาพที่เป็นรหัสผ่านของตนเองจนครบ 4 รูป และมีความถูกต้องจึงจะสามารถผ่านการพิสูจน์ตัวตนเข้าระบบได้ โดยรูปภาพบุคคลที่เหลือในแต่ละชุดเป็นเพียงภาพหลอกเท่านั้นเขาได้ใช้เทคนิคที่ว่าบุคคลจะสามารถระลึกถึงหน้าบุคคลได้ง่ายมากกว่ารูปภาพชนิดอื่นๆ ซึ่งจะมีข้อเสียที่ว่าเมื่อรูปภาพที่ระบบแสดงมาในแต่ละรอบไม่มีรูปภาพที่ผู้ใช้งานต้องการเลือกเพื่อใช้เป็นรหัสผ่านเข้าสู่ระบบได้

ต่อมาในปี 2013 นักวิจัย (Farnaz, Maslin & Azizah, 2013) ได้นำรหัสผ่านแบบ Passface มาเพิ่มความปลอดภัยขึ้น เรียกว่า Secure Passface (S-Passface) โดยทำการเปลี่ยนจากการใช้เมาส์คลิกที่รูปภาพใบหน้าบุคคลมาเป็นการใช้แป้นพิมพ์ทำการพิมพ์ตัวอักษรที่กำกับอยู่ใต้รูปภาพใบหน้าบุคคลแทน เนื่องจากการคลิกที่รูปภาพใบหน้าบุคคลนั้น อาจทำให้ผู้ไม่หวังดีสามารถขโมยรหัสผ่านโดยใช้เทคนิคที่เรียกว่า shoulder surfing นั่นคือ การแอบมองอยู่ด้านหลังเพื่อจดจำรหัสผ่านของผู้ใช้ รหัสผ่านแบบ S-Passface จะใช้ตัวอักษรกำกับใต้รูปภาพใบหน้าบุคคล มาต่อกันเป็นรหัสผ่านแทนการคลิก ทำให้ผู้ไม่หวังดีขโมยรหัสได้ยากขึ้น แต่การใช้รูปภาพใบหน้าบุคคลซึ่งผู้ใช้อาจจะไม่รู้จัก ทำให้มีข้อเสียในการจดจำรูปภาพใบหน้าบุคคลเหล่านั้นซึ่งจะส่งผลให้ผู้ใช้จำรหัสผ่านไม่ได้ การเปลี่ยนเปลี่ยนรูปภาพใบหน้าบุคคลไปเปลี่ยนรูปภาพของวัตถุต่างๆที่พบเห็นชีวิตประจำวันอาจทำให้ผู้ใช้นำไปเชื่อมโยงกับประสบการณ์ของแต่ละคนทำให้สามารถจดจำรหัสผ่านได้ดีขึ้น

งานวิจัยนี้ได้นำแนวคิดมาจากรหัสผ่านรูปภาพแบบ S-Passface โดยนำเสนอระบบแสดงรูปภาพใบหน้าของบุคคลในแต่ละช่องของกริด และมีตัวอักขระกำกับไว้ในกริดแต่ละช่อง โดยเป็นตัวอักษรภาษาอังกฤษที่ถูกสุ่มขึ้นมาเพื่อป้องกันการโจมตีในรูปแบบของ dictionary attack ผู้ใช้จะเลือกรูปภาพวัตถุที่ต้องการ แล้วพิมพ์อักขระที่กำกับไว้เพื่อใช้เป็นรหัสผ่าน การที่ให้ผู้ใช้มองรูปภาพแล้วพิมพ์อักขระที่กำกับในแต่ละช่องนี้ เพื่อเป็นการเพิ่มความปลอดภัยจากการขโมยรหัสผ่านที่เรียกว่า Shoulder Surfing สำหรับการใช้รูปภาพของวัตถุ เพื่อให้ผู้ใช้งานเกิดกระบวนการเชื่อมโยงรูปภาพประกอบกับเหตุการณ์หรือประสบการณ์ส่วนตัวของผู้ใช้งานแล้วสร้างออกมาเป็นรหัสผ่าน ส่งผลให้ผู้ใช้งานสามารถจดจำและระลึกถึงรหัสผ่านที่เคยได้สร้างไว้ในครั้งที่แล้วเมื่อเห็นรูปภาพประกอบเดิมอีกในครั้งต่อไป (Kristin & Heather, 2004) เนื่องจากผู้ใช้งานแต่ละคนจะมีประสบการณ์ต่อรูปภาพประกอบแตกต่างกันออกไป ทำให้การใช้กระบวนการเช่นนี้จะมีเพียงแต่ผู้ใช้งานเพียงคนเดียวที่ทราบว่าเมื่อเห็นรูปภาพประกอบนี้แล้วควรทำอย่างไร นอกจากนี้จะเกิดผลดีต่อความปลอดภัยของรหัสผ่านของผู้ใช้งานแต่ละคนด้วย

1.2 ปัญหานำวิจัย

งานวิจัยนี้ทำการเปรียบเทียบเพื่อศึกษาปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านแบบรูปภาพ โดยทำการศึกษาเปรียบเทียบใน 2 ปัจจัย ได้แก่ วิธีการนำเสนอรูปภาพใบหน้าบุคคลระหว่างรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วนและรูปภาพใบหน้าบุคคลย่อย กับจำนวนรอบที่ใช้ในการสร้างรหัสผ่านรูปภาพระหว่างจำนวนรอบในการสร้างรหัสผ่านรูปภาพ 1 รอบและจำนวนรอบในการสร้างรหัสผ่านรูปภาพ 2 รอบ

1.3 วัตถุประสงค์ของงานวิจัย

1. เพื่อเปรียบเทียบประสิทธิภาพด้านการใช้งาน (Usability) ประสิทธิภาพด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ในแต่ละกลุ่มการทดลองที่มีผลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ ระหว่างการจำนวนรอบในการสร้างรหัสผ่าน 1 รอบ กับการใช้จำนวนรอบในการสร้างรหัสผ่าน 2 รอบ

2. เพื่อเปรียบเทียบประสิทธิภาพด้านการใช้งาน (Usability) ประสิทธิภาพด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ที่มีผลต่อการพิสูจน์ตัวตนด้วยรหัสผ่าน ระหว่างวิธีการนำเสนอรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วน กับวิธีการนำเสนอรูปภาพใบหน้าบุคคลย่อย

3. เพื่อเปรียบเทียบประสิทธิภาพด้านการใช้งาน (Usability) ประสิทธิภาพด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ที่มีผลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ ระหว่างวิธีการนำเสนอรูปภาพใบหน้าบุคคล กับจำนวนรอบในการตั้งรหัสผ่าน

1.4 สมมติฐาน

ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยรูปแบบการนำเสนอรูปภาพใบหน้าบุคคล มีผลต่อด้านการใช้งาน (Usability) และด้านความปลอดภัย (Security) ของรหัสผ่านรูปภาพ

1. การเปรียบเทียบประสิทธิภาพด้านการใช้งาน และด้านความปลอดภัย ระหว่างจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

H_0 : จำนวนรอบในการตั้งรหัสผ่าน ไม่ส่งผลต่อ การใช้งานรหัสรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่าน ส่งผลต่อ การใช้รหัสผ่านรูปภาพ

H_0 : จำนวนรอบในการตั้งรหัสผ่าน ไม่ส่งผลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่าน ส่งผลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

2. การเปรียบเทียบประสิทธิภาพด้านการใช้งาน และประสิทธิภาพด้านความปลอดภัย ระหว่างระหว่างวิธีการนำเสนอรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วน กับวิธีการนำเสนอรูปภาพใบหน้าบุคคลย่อย

H_0 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ การใช้งานรหัสรูปภาพ

H_1 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ การใช้งานรหัสผ่านรูปภาพ

H_0 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

H_1 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

3. การเปรียบเทียบการมีอิทธิพลร่วมกัน ระห่วงจำนวนรอบในการตั้งรหัสผ่าน กับวิธีการนำเสนอรูปภาพใบหน้าบุคคล ที่มีผลต่อด้านการใช้งาน และด้วยความปลอดภัย

H_0 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ การใช้งานรหัสรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ การใช้รหัสผ่านรูปภาพ

H_0 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

1.5 ขอบเขตงานวิจัย

งานวิจัยนี้จึงได้กำหนดขอบเขตการวิจัยเพื่อให้เป็นไปตามวัตถุประสงค์ ดังต่อไปนี้

1. กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ เป็นพนักงานของการประปาส่วนภูมิภาคเขต 2 โดยมุ่งเน้นศึกษาเฉพาะกลุ่มตัวอย่าง ที่เคยใช้งานระบบพิสูจน์ตัวตนและใช้งานคอมพิวเตอร์มาแล้วอย่างน้อย 1 ปี ทั้งเพศชาย และเพศหญิง จำนวนทั้งหมด 80 คน โดยได้แบ่งออกเป็น 4 กลุ่มทดลอง กลุ่มทดลองละ 20 คน

2. การทดลองด้านประสิทธิภาพการใช้งาน (Usability) จะดำเนินการทดลองการพิสูจน์ตัวตนทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 หลังจากการลงทะเบียนทันที ครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 7 วัน และ ครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน

3. การทดลองด้านประสิทธิภาพความปลอดภัย (Security) จะดำเนินการทดลองการโจรกรรมรหัสผ่านโดยวิธีการแอบมอง (Shoulder surfing) หลังจากผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนในครั้งแรกทันที โดยให้ทดลองโจรกรรมได้ไม่เกิน 3 ครั้ง

4. การทดสอบประสิทธิภาพของวิธีการพิสูจน์ตัวตนที่ได้ออกแบบไว้ในงานวิจัย โดยการวัดประสิทธิภาพด้านการใช้งานซึ่งประกอบไปด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ และความสำเร็จในการพิสูจน์ตัวตน และการวัดประสิทธิภาพด้านความปลอดภัยจะประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมพิสูจน์ตัวตน และวัดความพึงพอใจที่ผู้ใช้มี

ต่อระบบพิสูจน์ตัวตนด้วยแบบสอบถาม และสุดท้ายจะนำข้อมูลเหล่านี้มาเปรียบเทียบตามปัจจัยที่ศึกษาเพื่อวิเคราะห์ผลการวิจัยว่ามีความแตกต่างกันอย่างไร

1.6 นิยามคำศัพท์ที่เกี่ยวข้อง

1. รหัสผ่านแบบรูปภาพ (Graphical Passwords) หมายถึง การใช้งานเกี่ยวกับภาพ การเขียนภาพ หรือการวาดภาพ เป็นรหัสผ่านส่วนบุคคลสำหรับการพิสูจน์ตัวตนเข้าสู่ระบบ

2. การระลึกความจำ หมายถึง การรวบรวมความคิดหรือพยายามฟื้นความจำ การที่มีบางสิ่งบางอย่างที่ทำให้นึกถึงสิ่งนั้นได้

3. ผู้สังเกตการณ์ หมายถึง ผู้ทดลองอีกกลุ่มการทดลองที่ยืนสังเกตการณ์ในการสร้างรหัสผ่านแบบรูปภาพ อยู่ด้านหลังผู้ที่กำลังทำการทดลองสร้างรหัสผ่านรูปภาพอยู่ในขณะนั้น จนถึงสิ้นสุดการล็อคอินเข้าสู่ระบบ

4. ความพึงพอใจต่อระบบ หมายถึง ผู้ทดลองเข้าใจการทำงานของระบบ การจัดวางปุ่มกดต่างๆ และรูปภาพวัตถุต่างๆ ที่มีในระบบเพียงพอต่อการใช้งาน

5. การลักลอบขโมยรหัสผ่าน หมายถึง การรับรู้รหัสผ่านของผู้อื่นมากระทำการใดๆ โดยที่บุคคลนั้นไม่ยินยอมให้ข้อมูลดังกล่าว

1.7 ประโยชน์ที่คาดว่าจะได้รับ

งานวิจัยนี้ คาดหวังว่าจะได้รับประโยชน์จากงานวิจัย ดังต่อไปนี้

1. เพื่อทราบถึงความแตกต่างของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ แบบมีปัจจัยจำนวนรอบในการสร้างรหัสผ่าน และวิธีการนำเสนอรูปภาพใบหน้าบุคคล ในด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจ

2. เพื่อทราบถึงรูปแบบที่ใช้ในการออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่เหมาะสม นำไปใช้งานได้ให้มีการใช้งานที่ง่าย (Usability) และมีความปลอดภัย (Security)

3. เพื่อนำข้อมูลจากการศึกษาวิจัยนี้ ไปศึกษาวิจัยสำหรับงานวิจัยในนอนาคต หรือนำไปเป็นแนวทางสำหรับประยุกต์ใช้กับงานวิจัยอื่นๆที่เกี่ยวข้องกับการออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านแบบรูปภาพ

1.8 รายละเอียดงานวิจัย

วิทยานิพนธ์ฉบับนี้มีรายละเอียดต่างๆ แบ่งออกได้เป็น 5 บท ดังนี้

บทที่ 1 บทนำ ประกอบด้วย ความเป็นมาและความสำคัญของงานวิจัย ปัญหานำวิจัย วัตถุประสงค์งานวิจัย สมมติฐาน ขอบเขตงานวิจัย ประโยชน์ที่คาดว่าจะได้รับ และรายละเอียดงานวิจัย

บทที่ 2 ทฤษฎีละงานวิจัยที่เกี่ยวข้อง ประกอบด้วย ทฤษฎีที่เกี่ยวกับความจำของมนุษย์ การจำรูปภาพใบหน้าบุคคล ความหมายของรหัสผ่านแบบตัวอักษร และงานวิจัยที่เกี่ยวข้องกับการออกแบบระบบพิสูจน์ตัวตน

บทที่ 3 วิธีการดำเนินงานวิจัย ประกอบไปด้วย ระเบียบวิธีการทดลอง ตัวแปรและสมมติฐานที่ใช้ในงานวิจัย โครงสร้างและขั้นตอนการทำงานของระบบที่ได้ออกแบบ รูปแบบการทดลอง และการวัดและประเมินผลการทดลอง

บทที่ 4 ผลการทดลอง ประกอบด้วย ผลการทดลองด้านประสิทธิภาพการใช้งาน (Usability) ด้านประสิทธิภาพความปลอดภัย(Security) ความพึงพอใจของผู้ใช้งานที่มีต่อระบบพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ และการวิเคราะห์ผลการทดลองเพิ่มเติม

บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ ประกอบไปด้วย สรุปผลการทดลองที่ได้จากการวิเคราะห์ผลการวิจัย การอภิปรายผลและข้อเสนอแนะ และแนวทางสำหรับการศึกษาวิจัยต่อไปในอนาคต

บทต่อไป จะอธิบายถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง เพื่อนำมาเป็นแนวทางในการทำงานวิจัยนี้

บทที่ 2

ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในบทนี้ จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง โดยทฤษฎีที่เกี่ยวข้องกับงานวิจัยนี้ประกอบด้วย การรับรู้ทางสายตา (Visual Perception) และระบบความจำของมนุษย์ (Memory System) เพื่อนำมาใช้ออกแบบรหัสผ่านที่ช่วยให้ผู้ใช้สามารถจดจำได้ง่าย โดยทฤษฎีและงานวิจัยที่เกี่ยวข้องต่างๆ มีดังนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

การออกแบบรหัสผ่านเพื่อให้เป็นเครื่องมือสำหรับการจำรหัสผ่านนั้น จำเป็นต้องศึกษาเกี่ยวกับหลักการรับรู้ของมนุษย์และระบบความจำของมนุษย์เสียก่อน เพื่อให้เข้าใจและนำมาประยุกต์ใช้ในการออกแบบรหัสผ่านได้

2.1.1 การรับรู้ทางสายตา (Visual Perception)

หลักการมองเห็นของตา จะมีการมองเห็นคล้ายกับการทำงานของกล้องถ่ายภาพ เพราะการทำงานของกล้องถ่ายภาพก็นำมาจากหลักการทำงานของตา เริ่มต้นจากแสงตกกระทบวัตถุและสะท้อนเข้าสู่นัยน์ตา ผ่านกระจกตา ม่านตาเข้าไปยังเลนส์ตา เพื่อปรับแสงให้ตก ไปยังจอรับภาพ โดยที่จอรับภาพนั้นจะมีเซลล์ประสาทรับแสงอยู่เป็นจำนวนมาก ประมาณ 70% ของเซลล์รับความรู้สึกทั้งหมดของร่างกาย ภาพที่เกิดขึ้นบนจอรับภาพนั้นจะเป็นภาพหัวกลับ และ กลับซ้าย-ขวา ของวัตถุจริง การทำงานของกล้องถ่ายภาพก็ทำงานเช่นเดียวกันจนถึงกระบวนการนี้ กล้องจะสร้างภาพที่ได้ลงไปบนฟิล์มเกิดเป็นภาพแฝง ซึ่งสามารถมองเห็นได้เมื่อไปผ่าน กระบวนการ ล้าง-อัดภาพ แต่การมองเห็นของมนุษย์นั้น แสงจากวัตถุที่เข้าสู่นัยน์ตาจะถูกใส่รหัส เป็นข้อมูลส่งไปยังสมอง ซึ่งสมองจะทำการถอดรหัสข้อมูลนั้น โดยการกลับภาพหัวกลับนั้นให้เป็น ภาพที่ถูกต้อง และนำไปเทียบกับประสบการณ์ที่มีอยู่เดิม ก่อนจะแปลออกมาเป็นความหมายใน ที่สุด จากข้างต้นแม้ว่าหลักการมองเห็นของมนุษย์และกล้องมีความคล้ายคลึงกันอย่างมาก แต่ การรับรู้และแปลความหมายของคนกับกล้องจะแตกต่างกัน เพราะการรับรู้ด้วยตาของคนจะ เกี่ยวเนื่องกับประสบการณ์ แม้ว่าคนส่วนใหญ่เชื่อกันว่าสิ่งที่มองเห็นจะต้องเหมือนกับรูปร่างจริง ของวัตถุ เพราะภาพที่เกิดขึ้นเกิดจากแสงจาก

วัตถุนั้นกระตุ้นนัยน์ตาเกิดเป็นกระแสประสาทขึ้นสู่ สมอง แต่โดยความเป็นจริงแล้วการรับรู้ของมนุษย์ไม่ใช่การคัดลอกลักษณะทางกายภาพเข้าสู่ สมองอย่างตรงไปตรงมา ต้องผ่านกระบวนการต่างๆ หลายขั้นตอน หรือแม้กระทั่งคนสองคนที่ ได้รับสิ่งเร้าเดียวกัน อาจแปลความหมายของภาพที่เห็นไม่เหมือนกัน (ชัยชนะ จารุวรรณากร, 2548, น.15)

มนุษย์รับรู้ภาพ โดยเริ่มจากการมองภาพหรือสิ่งเร้าที่สนใจ แล้วจะถูกส่งมาเก็บในระบบความจำในลักษณะของตัวแทนข้อมูล หรือที่เรียกว่า รหัสภาพ ถึงแม้ว่าสิ่งเร้าที่รับรู้เป็นตัวษร ก็จะถูกแปลงให้อยู่ในรูปของรหัสภาพเช่นกัน หากกระบวนการรับรู้ที่เกิดขึ้นมีการเชื่อมโยงสิ่งเร้าเข้ากับความรู้หรือประสบการณ์ที่ผ่านมา จะส่งผลให้เกิดกระบวนการระลึกได้ที่ไม่ใช่ข้อมูลความจำที่ถูกเก็บไว้ แต่เป็นการสร้างข้อมูลและสถานการณ์ขึ้นมาใหม่ จากสิ่งที่ผู้ใช้รู้อยู่แล้ว หากในกระบวนการสร้างรหัสผ่านได้มีการนำประสบการณ์หรือความรู้มาใช้ร่วมด้วย ก็จะทำให้ผู้ใช้สามารถที่จะระลึกถึงรหัสผ่านได้ อย่างไรก็ตามหากผู้ใช้สร้างรหัสผ่านโดยไม่มีความสัมพันธ์กับรูปภาพประกอบ ซึ่งจะส่งผลต่อการระลึกถึงรหัสผ่านได้เช่นกัน

2.1.2 ระบบความจำ (Memory System)

ความจำ เป็นกระบวนการเก็บรักษา(storage) การระลึก(recall) การทบทวน (rehearsal) และการค้นคืน(retrieval) ข้อมูลจากประสบการณ์ในอดีตและพึ่งจะมีอยู่ในขณะนั้นชั่วคราว โดยมีกระบวนการสำคัญ 3 แบบ คือ

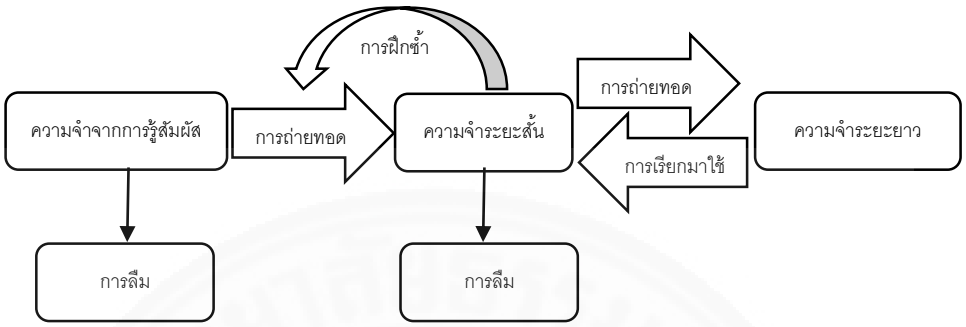
1. การเข้ารหัส (encoding) คือ การรับสิ่งกระตุ้นเข้ามาและแปลรหัสข้อมูลจากการรับสัมผัสเพื่อไปสร้างเป็นตัวแทนทางสมอง

2. การเก็บ (storage) คือ การเก็บรักษาข้อมูลหรือรหัสความจำเพื่อเตรียมพร้อมสำหรับการนำออกมาใช้

3. การเรียกเอาขึ้นมาใช้ (retrieval) คือ การเข้าถึงข้อมูลและการนำข้อมูลที่เก็บไว้ออกมาใช้

นอกจากนี้ ยังมีกระบวนการอื่นๆอีก เช่น การทบทวน การลืม และการควบคุม ระบบความจำทั้ง 3 หน่วย ได้แก่ ความจำจากการรู้สัมผัส (Sensory Memory - SM) ความจำระยะสั้น (Short-Term Memory - STM) และความจำระยะยาว (Long-Term Memory - LTM) กระบวนการทั้งหลายเหล่านี้จะทำงานร่วมกันเป็นระบบโครงสร้างของการจำจึงเรียกว่า “โครงสร้างความจำ” โดยคำว่า รหัส จะหมายถึงการแปลงข้อมูลจากลลักษณะหนึ่งไปแฝงไว้ในข้อมูลอีกลักษณะหนึ่ง ซึ่งข้อมูลใหม่นั้นจะยังมีความหมายเดิมอยู่ ในปัจจุบันกระบวนการที่ข้อมูลจะดำเนินการผ่าน

ระบบความจำทั้ง 3 ชนิดนี้ถูกมองเป็นแบบจำลองการจัดการข้อมูล หรือการประมวลผลข้อมูล (The Information Processing Model) สรุปได้ดังภาพที่ 2.1



ภาพที่ 2.1 การประมวลผลข้อมูล
ที่มา : *"ระบบความจำ"*, โดย อุบลวรรณ ภวกานันท์, 2555, จิตวิทยาการรู้ คิด และปัญญา, หน้า.147.

2.1.3 ความสัมพันธ์ระหว่างการเข้ารหัส (Encoding) และการเรียกข้อมูลมาใช้ (Retrieval)

ในแต่ละวันเราจะรับรู้สิ่งต่างๆมากมายในรูปแบบต่างๆ ทั้งภาพและเสียง เราสามารถจะจำข้อมูลเหล่านั้นได้อย่างถูกต้องด้วยองค์ประกอบ 3 ชนิด ได้แก่

1. ความตั้งใจ (attention) ถ้าเราให้ความสำคัญกับสิ่งใด เรามักจะให้ความตั้งใจเป็นพิเศษกับสิ่งนั้นซึ่งจะช่วยให้เราสามารถจำข้อมูลนั้นได้ดีและได้นาน

2. ความลุ่มลึกของการประมวลผล (deep of processing) การแปลงข้อมูลนั้นมีหลายวิธี แต่ละวิธีจะมีความซับซ้อนแตกต่างกันออกไป

3. ความเหมาะสมในการถ่ายโยงของกระบวนการ (transfer-appropriate process) ที่ทำให้เห็นถึงความสามารถของความจำและยังแสดงถึงความสัมพันธ์ระหว่างการเข้ารหัสเบื้องต้นของข้อมูลและการเรียกข้อมูลกลับคืนมาใช้ ตัวอย่างเช่น เมื่อมองเห็นภาพที่มีความสัมพันธ์กับข้อมูลที่มีอยู่ในความจำ ก็จะทำให้ระลึกได้ดีขึ้น

2.1.6 การจำใบหน้า (Face Recognition)

มีวัตถุที่มีรูปแบบซับซ้อนมากกว่าแบบที่เรียบง่ายเช่น ความหลากหลายของรูปร่างของสัตว์ โดยเฉพาะเมื่อมีการเคลื่อนไหว หนึ่งในความหลากหลายของรูปร่างสิ่งมีชีวิตคือใบหน้ามนุษย์เราสามารถเห็นความแตกต่างของใบหน้านับพันหน้าได้ จดจำการแสดงสีหน้าได้ และตัดสินอายุหรือเพศจากใบหน้าได้ ความจำต่อตัวเร้าที่มีการเคลื่อนที่ยังไม่ได้ถูกจัดในรูปทรงเรขาคณิต 24 แบบของบีทเดอร์แมน ใบหน้ามีความพิเศษจากความได้สัดส่วนที่พัฒนาขึ้น เด็กจะแยกจำความแตกต่างของใบหน้าได้ตั้งแต่เป็นทารกและรับรู้ถึงความเปลี่ยนแปลงบนใบหน้าด้วย เด็กทารกอายุ 1-3 เดือนจดจำใบหน้าได้โดยเฉพาะใบหน้าของแม่และพ่อ ถ้าให้เลือกเด็กทารกอายุ 3 เดือนจะชอบจ้องมองใบหน้ามากกว่าที่อื่น และทารกก็ชอบมองรูปถ่ายของแม่มากกว่ารูปถ่ายผู้หญิงอื่น (Siegler, 1991) ทารกจะชอบมองใบหน้าผู้ใหญ่ที่มีความดึงดูดคือมีความได้ส่วนกัน กระบวนการเจริญเติบโตจะเปลี่ยนรูปศีรษะและใบหน้าของมนุษย์ให้มีลักษณะเฉพาะของแต่ละคน โดยสัดส่วนจะเปลี่ยนแปลงคือความนูนของหน้าผากจะลดน้อยลง มุมมองของใบหน้าก็จะเปลี่ยนไปด้วย (e.g. Pittenger & Shaw, 1975) การเปลี่ยนแปลงเหล่านั้นเป็นผลของกระบวนการพัฒนาไปตามลำดับขั้นของอายุ การรับรู้เรื่องเหล่านี่จะถูกรวบรวมด้วยข้อจำกัดซึ่งในการพัฒนาทางสมองเช่นกัน วิทคี บรูซ (Vicki Bruce, 1986; 2000) ได้ทดลองให้ผู้ถูกทดลองรูปใบหน้าที่ไม่รู้จัก 24 รูปจากทั้งหมด 48 รูป อีก 24 รูปเป็นภาพเป้าหมายที่ใช้กระตุ้นซึ่งเป็นรูปที่ได้เห็นมาแล้ว ในรูปทั้ง 24 นั้นจะมี 8 รูปเป็นรูปเดียวกันยกเว้นท่าทางหรือหารแสดงสีหน้าที่เปลี่ยนแปลงไปและอีก 8 รูปจะเหมือนเดิม ส่วนอีก 8 รูปทั้งท่าทางและการแสดงสีหน้าเปลี่ยนแปลงไป ผลพบว่ามีความถูกต้องของการจำใบหน้าที่ไม่เปลี่ยนแปลงเลยเท่ากับ 90% และ 76% สำหรับใบหน้าที่เปลี่ยนแลงท่าทางหรือการแสดงสีหน้า และ 60.5% สำหรับใบหน้าที่เปลี่ยนแปลงทั้งท่าทางและกางแสดงสีหน้า การเปลี่ยนแปลงทรงผมหรือสีผมหรือการไว้หนวด หรือการโกนหนวด จะทำให้การจำใบหน้าได้ลดน้อยลง การใส่ถุงน่องครอบศีรษะไว้เป็นการปลอมตัวได้ผลดีมากซึ่งพวกโจรใช้วิธีนี้มานานแล้ว ใบหน้าที่ปรากฏให้มองจากข้างบนลงมาจะจำได้น้อยกว่าแบบอื่น ตัวอย่างเช่น บ้านที่มองจากที่สูง การค้นพบนี้สนับสนุนว่าใบหน้าทีความพิเศษการจำใบหน้าอาจจะผิดพลาดได้ถ้าถูกบิดเบือนจากความจริง อย่างไรก็ตามเราก็ยังคงจำใบหน้าได้แม้เมื่อรายละเอียดจะถูกเคลื่อนย้าย มีการพบว่ามนุษย์จำรูปการ์ตูนได้ดีกว่าภาพอื่นๆ เช่นรูปการ์ตูนนักการเมืองผู้เคยโด่งดังบนหน้าหนังสือพิมพ์รายวันหรือนิตยสาร โดยปกติผู้อ่านไม่มีปัญหาในหารจำใบหน้าของแต่ละบุคคลเมื่อถูกนำมาทดสอบ ผู้ถูกทดสอบจะจำรูปภาพล้อเลียนของบุคคลได้ดีกว่ารูปวาดธรรมดา ใบปี ค.ศ. 1987 โรธเดสและคณะ (Rhodes, Brennan & Carey) จากมหาวิทยาลัยสแตนฟอร์ด (Stantord University) ได้ทำรูปวาดล้อเลียนและรูปการ์ตูนจากรูปถ่าย 60 รูปแล้วนำไปถามนักศึกษา 20 คนที่คุ้นเคยกับใบหน้าเหล่านั้นให้บอกลักษณะของบุคคลนั้น ผลพบว่าความ

แม่นยำในการจำรูปล้อเลียนและรูปการ์ตูนไม่มีความแตกต่างกัน แต่รูปล้อเลียนจะถูกจำได้ในเวลาเพียงครึ่งเดียว (3.2 วินาที) ของเวลาในการจำรูปการ์ตูนปกติเดียวกัน (6.4 วินาที) รูปล้อเลียนถูกจำได้ดีกว่าเพราะลักษณะหน้าตาจะถูกเขียนให้เกินความจริงซึ่งทำให้เห็นความแตกต่างระหว่างลักษณะที่ถูกล้อเลียนกับลักษณะปกติของบุคคลนั้น เหตุผลนี้เองที่สนับสนุนว่าความจำใบหน้ายู่บนพื้นฐานของใบหน้าที่มีความโดดเด่นเหมือนกับการจำวัตถุอื่น แต่ใบหน้าไม่ได้เป็นเพียงลักษณะที่ถูกประกอบขึ้นมาเท่านั้นแต่ยังนำไปสู่ความจำได้เหมือนเป็นตัวกระตุ้นที่สำคัญแบบหนึ่ง (ดูใน Bruce, 1988; Klatzky & Forrest, 1984) อย่างไรก็ดีการจำใบหน้าได้ยังคงเป็นปริศนาอยู่ เพราะในบางประเด็นคล้ายกับการจำตัวเร้าอื่นๆ แต่อีกประเด็นก็แตกต่างกันมากเพราะเราเห็นใบหน้านับพันที่ต่างกันแต่เราก็ยังจำเอกลักษณ์ของแต่ละใบหน้าได้ และเราก็สามารถให้ความรู้สึกที่เหมาะสมกับแต่ละใบหน้าได้โดยทั่วไปการจำใบหน้าของเราจะดีมากและไม่บ่อยครั้งที่จะผิดพลาด แต่ก็มีกรณีที่พบได้ในโรค Prosopagnosia ที่ผู้ป่วยสูญเสียความจำใบหน้าที่คุ้นเคยโดยผู้ป่วยสามารถมองเห็นและอธิบายใบหน้าของคนแต่ไม่สามารถจำใบหน้านั้นได้ (ดูใน Tranel, Damasio, & Damasio, 1988; Sergent & Poncet, 1990) ซึ่งเป็นแบบหนึ่งของกลุ่มโรค agnosig ที่ผู้ป่วยจะไม่สามารถจำความหมายของวัตถุหรือสิ่งที่เคยเห็นได้ การมองเห็นไม่ทำงานตามเซลล์ประสาทบนพื้นที่เฉพาะใยสมอง โรค Prosopagnosia เกิดจากสมองถูกกระทบกระเทือนหรือถูกทำลาย ส่วนมากจะพบในบริเวณสมองขวาด้านล่างแต่ไม่สามารถระบุถึงตำแหน่งและเส้นใยต่างๆ ได้เราจึงเรียกบริเวณนั้นโดยรวมว่า “face areas” ซึ่งพบว่าเมื่ออายุมากขึ้นสามารถเกิด Prosopagnosia จากการไม่สมบูรณ์หรือการทำงานขาดหายไป จากการศึกษาทางแพทย์ต่อมาสรุปผลว่าอาการ Prosopagnosia นั้นเกิดจากการบกพร่องของการรับรู้ใบหน้า (face perception) และความจำเชิงประจักษ์ (explicit memory)

2.1.7 ความรู้พื้นฐานเกี่ยวกับรหัสผ่าน (Password)

รหัสผ่าน (password) คือ ชุดของตัวอักษรภาษาอังกฤษที่ผู้ใช้งานระบบจะต้องสร้างขึ้นมาในขั้นตอนการลงทะเบียน แล้วนำไปใช้สำหรับการพิสูจน์ตัวตน เพื่อยืนยันสิทธิ์การเข้าถึงแหล่งข้อมูล ผู้ใช้ควรเก็บรักษารหัสผ่านไว้เป็นความลับไม่ให้ผู้อื่นรับรู้ หากผู้อื่นสามารถล่วงรู้ถึงรหัสผ่าน จะทำให้สามารถเข้าสู่ข้อมูลในระบบได้ (http://th.wikipedia.org, 2556)

รหัสผ่านนั้นเริ่มมีการใช้งานมาตั้งแต่ปี 1960 เป็นชุดของตัวอักษรที่ผู้ใช้ได้สร้างขึ้นจากขั้นตอนของการลงทะเบียนเข้าใช้งานระบบในครั้งแรก เมื่อผู้ใช้ต้องการเข้าใช้งานระบบจะต้องยืนยันรหัสผ่านที่ได้สร้างขึ้นให้ถูกต้องจึงจะสามารถเข้าใช้งานระบบหรือบริการต่างๆได้ตามสิทธิ์ที่ได้รับ หากไม่สามารถยืนยันรหัสผ่านของตนเองได้อย่างถูกต้องก็จะไม่สามารถเข้าใช้งานระบบได้ สำหรับรหัสผ่านในคอมพิวเตอร์ถูกนำไปใช้ในหลายจุดประสงค์ เช่น เพื่อยืนยันการเข้าใช้งาน

คอมพิวเตอร์ การเข้าใช้งานระบบอีเมล์ต่างๆ การเข้าใช้ฐานข้อมูล เครือข่าย หรือการเข้าใช้เครือข่ายสังคมออนไลน์ต่างๆ

รหัสผ่านอาจเป็นกลุ่มของอักขระที่ไม่มีความหมาย หรืออาจเป็นชุดของตัวอักษรผสมกับตัวเลขและสัญลักษณ์พิเศษต่างๆ เพื่อให้ยากต่อการโจรกรรมรหัสผ่าน รหัสผ่านยังมีอีกประเภทที่เรียกว่า พาสโค้ด (passcode) เป็นรหัสผ่านที่เป็นเพียงแต่ตัวเลขอย่างเดียว อย่างเช่น รหัสลับบุคคล (PIN) ที่ใช้ในการเข้าถึงเอทีเอ็ม ที่ต้องใช้ประกอบกับบัตรเอทีเอ็ม จึงจะสามารถยืนยันเข้าใช้งานได้

การโจรกรรมรหัสผ่านสามารถทำได้หลากหลายวิธีเช่น การสุ่มเดารหัสผ่านจากคำศัพท์ต่างๆที่ได้มีการรวบรวมไว้ นอกจากนี้ รหัสผ่านอาจถูกโจรกรรมได้ด้วยการเดาสุ่มตัวอักษรทีละตัว ซึ่งถ้าหากสามารถสุ่มจนตรงกับรหัสผ่านที่สร้างไว้ ผู้ไม่หวังดีก็จะสามารถโจรกรรมรหัสผ่านได้สำเร็จ

นอกจากนี้ หากมีผู้ไม่หวังดีทราบข้อมูลส่วนตัวของผู้ตั้งรหัสผ่านก็อาจนำข้อมูลดังกว่ามาใช้ประกอบการเจาะรหัสผ่านได้ด้วย

OTP (One-time password) เป็นรหัสผ่านที่สามารถใช้ได้เพียงครั้งเดียวในการเข้าสู่ระบบ ซึ่งมีความแตกต่างจากรหัสผ่านทั่วไป คือสามารถป้องกันภัยคุกคามเกี่ยวกับการกรอกรหัสผ่านซ้ำ (Replay Attack) กล่าวคือ หากผู้ประสงค์ร้ายทำการจดจำรหัสผ่านเดิมที่ผู้ใช้งานเคยเข้าสู่ระบบ เพื่อจะนำกลับมาใช้ซ้ำ จะไม่สามารถกระทำได้เนื่องจากรหัสผ่านจะถูกเปลี่ยนไปในแต่ละครั้งที่เข้าสู่ระบบ แต่อย่างไรก็ตามการใช้งานรหัสผ่าน OTP มีข้อเสียคือ ผู้ใช้งานอาจจดจำรหัสผ่านดังกล่าวได้ยาก ดังนั้นจึงมักพบเห็นการใช้รหัสผ่านแบบ OTP ร่วมกับเทคโนโลยีอื่น ทั้งนี้ เทคโนโลยีที่ใช้ในการสร้างรหัสผ่านแบบ OTP ได้แก่ การคำนวณจากเวลา การคำนวณจากรหัสผ่านเดิม หรือค่าสุ่มอื่นๆ เป็นต้น (https://www.etda.or.th/etda_website/mains/display
/1257, 2555)

อย่างไรก็ตาม การใช้รหัสผ่านที่เป็นอักขระ ส่งผลให้ผู้ใช้เกิดความยากในการจดจำ เนื่องจากไม่สอดคล้องกับหลักการจำของมนุษย์ จึงได้มีรหัสผ่านอีกประเภทหนึ่งที่สอดคล้องกับหลักการรับรู้และการจำของมนุษย์ เรียกว่า รหัสผ่านแบบรูปภาพ (Graphical Password)

2.2 งานวิจัยที่เกี่ยวข้อง

งานวิจัยที่เกี่ยวข้องในการพัฒนารหัสผ่านแบบรูปภาพแบ่งออกเป็น 2 ประเภท คือ Recognition-based คือ รหัสผ่านแบบรูปภาพที่ให้ผู้ใช้เลือกชุดของรูปภาพเพื่อนำมาเป็นรหัสผ่านในขั้นตอนการลงทะเบียนผู้ใช้จะต้องระบุรูปภาพที่ได้เลือกไว้ให้ถูกต้อง ส่วนรหัสผ่านแบบรูปภาพอีก

ประเภท คือ Recall-based เป็นรหัสผ่านแบบรูปภาพอีกประเภทหนึ่งที่ผู้ใช้ต้องวาดหรือเลือกจุดให้ถูกต้องตามที่สร้างไว้ในการลงทะเบียน

ในเว็บไซต์ www.realuser.com (2005) ได้นำเสนอวิธีการที่เรียกว่า Passface วิธีนี้ผู้ใช้งานเลือกรูปภาพหน้าบุคคลมา 4 รูปภาพโดยระบบจะแสดงรูปภาพบุคคลมาให้เลือกซึ่งมีรูปภาพหน้าบุคคลที่ไม่ใช่รูปภาพที่ใช้งานเลือกแสดงด้วยเพื่อเป็นรูปภาพหลอก รูปภาพบุคคลทั้ง 4 รูปนั้นจะนำมาเป็นรหัสผ่านรูปภาพให้กับผู้ใช้งานต่อไปในอนาคต ในขั้นตอนการพิสูจน์ตัวตน (Authentication) ระบบจะแสดงรูปภาพหน้าบุคคล 9 รูปในแบบกริดซึ่งจะมีรูปภาพบุคคลเพียงหน้าเดียวที่ผู้ใช้งานต้องเลือกรูปภาพที่เป็นรหัสผ่านของผู้ใช้งาน ระบบจะแสดงรูปขึ้นมาหลายชุดจนผู้ใช้งานเลือกรูปภาพที่เป็นรหัสผ่านของตนเองจนครบ 4 รูป และมีความถูกต้องจึงจะสามารถผ่านการพิสูจน์ตัวตนเข้าระบบได้ โดยรูปภาพบุคคลที่เหลือในแต่ละชุดเป็นเพียงภาพหลอกเท่านั้นเขาได้ใช้เทคนิคที่ว่าบุคคลจะสามารถระลึกถึงหน้าบุคคลได้ง่ายมากกว่ารูปภาพชนิดอื่นๆ ซึ่งจะมีข้อเสียที่ว่าเมื่อรูปภาพที่ระบบแสดงมาในแต่ละรอบไม่มีรูปภาพที่ผู้ใช้งานต้องการเลือกเพื่อใช้เป็นรหัสผ่านเข้าสู่ระบบได้ ก็จะต้องทำกระบวนการเลือกรูปภาพนี้อยู่หลายรอบเช่นกัน ดังภาพที่ 2.2

ภาพที่ 2.2 วิธีระบบ Passface

ที่มา : *"Passfaces"* โดย Passfaces Corporation, 2005, www.realuser.com .

Sobrado and Birget (2002) ได้พัฒนาแนวคิดของรหัสผ่านแบบรูปภาพที่นำมาแก้ปัญหา Shoulder Surfing ในขั้นตอนแรกระบบจะแสดงรูปภาพที่เป็นวัตถุต่างๆจำนวนมากเพื่อให้ผู้ใช้งานได้เลือกวัตถุที่ต้องการก่อน หลังจากนั้นเป็นขั้นตอนของการพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบ ผู้ใช้งานจะต้องจดจำวัตถุที่ตนเองได้เลือกไว้ในขั้นตอนแรก และคลิกเลือกให้ถูกต้อง โดยใช้หลักการว่าเมื่อผู้ใช้งานได้เลือกรูปที่ตนเลือกถูกต้องแล้วจะเกิดเป็นรูปเหลี่ยม (Convex Hull) รูปทรงต่างๆ ซึ่งแต่ละครั้งก็จะวางตำแหน่งที่แตกต่างกันออกไป หลังจากนั้นให้ผู้ใช้งานเลือกรูปภาพตามจำนวนที่กำหนดภายในรูปเหลี่ยมที่เกิดขึ้นจากการล้อมรอบด้วยวัตถุที่ผู้ใช้งานเลือกไว้ โดยรูปภาพวัตถุที่เขาได้ใช้มีประมาณ 1,000 กว่าวัตถุ ซึ่งมีจำนวนมากและไม่มีความเกี่ยวข้องกัน และในทางกลับกันหากมีรูปภาพวัตถุจำนวนน้อยๆ ก็จะส่งผลต่อความเป็นไปได้ของรหัสผ่านที่จะเป็นไปได้ (Password Space) เนื่องจากมีวัตถุจำนวนมากและตำแหน่งไม่มีความแน่นอน จึงสามารถใช้เป็นรูปภาพหลอกกับผู้ไม่หวังดีได้ ประกอบกับวิธีการคิดในการเลือกวัตถุภายในรูปเหลี่ยมจึงจะสามารถพิสูจน์ตัวตนได้ถูกต้อง จึงสามารถป้องกันการขโมยรหัสผ่านที่เรียกว่า Shoulder Surfing ได้ แต่เมื่อกำหนดให้มีจำนวนวัตถุที่ผู้ใช้งานต้องเลือกมากขึ้น จะส่งผลให้ผู้ใช้งานไม่สามารถจดจำรหัสผ่านที่สร้างขึ้นได้อย่างแม่นยำ

ภาพที่ 2.3 แนวคิดของ Sobrado and Birget
ที่มา : *"Graphical passwords"* โดย Sobrado and Birget, 2002, An Electronic Bulletin for Undergraduate Research.

Man, Hong, and Mathews (2003) ได้เสนอวิธีการรองรับ shoulder-surfing อีกวิธีหนึ่งที่ว่า ผู้ใช้งานต้องเลือกอ๊อบเจ็ครูปภาพตามจำนวนที่กำหนอดโดยอ๊อบเจ็คเหล่านั้นมีความหลากหลายแตกต่างกันออกไปโดยมาจากการสุ่มขึ้นมาจากระบบ พร้อมกันนั้นผู้ใช้งานต้องกำหนดรหัสตัวอักษรกำกับให้กับแต่ละอ๊อบเจ็คด้วยไม่ซ้ำกัน สถานะต่อไปคือเมื่อผู้ใช้งานจะเข้าระบบผู้ใช้งาน

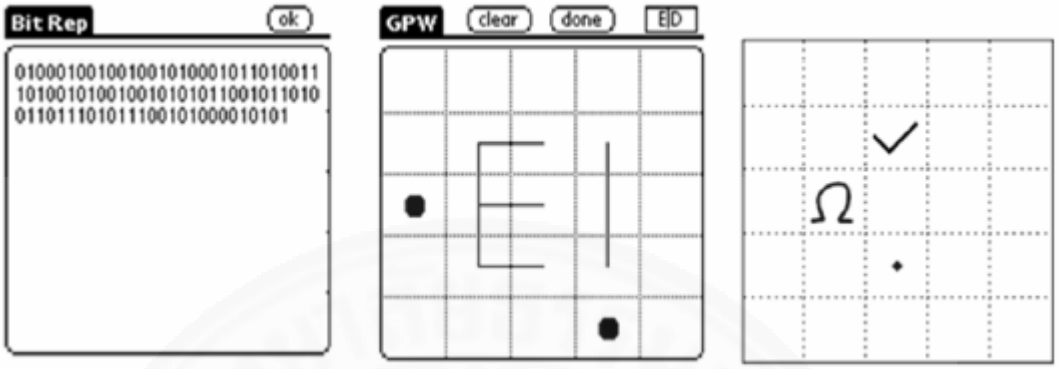
ต้องเลือกอ๊อบเจ็คที่ตนเองได้เลือกไว้ตอนแรก ซึ่งระบบจะทำการสุ่มภาพขึ้นมาแสดงเป็นอ๊อบเจ็ครูปภาพหลอก (Decoy-object) มาจำนวนมาก และทุกอ๊อบเจ็คที่เลือกผู้ใช้งานจะต้องพิมพ์ตัวอักษรกำกับให้ถูกต้องเหมือนเดิมตามที่ได้กำหนดไว้ทุกอ๊อบเจ็คจนครบจำนวนผู้ใช้งานได้เลือก มีข้อดีคือระบบนี้จะไม่มีเมาส์เลื่อนไปตามผู้ใช้งานเคลื่อนไหวจะเป็นควบคุมจากคีย์บอร์ดแทนทั้งหมด แต่อย่างไรก็ตามวิธีการนี้ผู้ใช้งานยังคงต้องจำตัวอักษรที่ตนเองได้กำกับไว้ในแต่ละ อ๊อบเจ็ครูปภาพของตนไม่ซ้ำกันเลย ส่งผลให้ผู้ใช้งานยังคงต้องจดจำตัวอักษรจำนวนมากเพื่อเข้าใช้ระบบนี้

ภาพที่ 2.4 วิธีการของ Man, Hong, and Mathews

ที่มา : *"A shoulder-surfing resistant graphical password scheme"* โดย Man, Hong, and Mathews, 2003, Proceedings of International conference on security and management

Takada and Koike ได้วิเคราะห์เทคนิควิธีสำหรับรหัสผ่านรูปภาพบนโทรศัพท์มือถือโดยสามารถให้ผู้ใช้งานเลือกรูป (Pass-image) ที่ตนเองชอบไว้สำหรับใช้พิสูจน์ตัวตน อันดับแรกผู้ใช้งานจะต้องลงทะเบียนกับระบบเพื่อนำรูปที่ตนเองชอบให้ระบบได้เรียนรู้ หลังจากนั้นกระบวนการพิสูจน์ตัวตนผู้ใช้งานจะต้องเลือกรูปภาพที่ตนเองได้เลือกเข้าระบบไว้ ตามรอบแต่ละครั้งที่ระบบแสดงรูปภาพหลากหลายแกผู้ใช้ เช่นเดียวกันถ้านั้นรอบนั้นๆ ไม่มีรูปภาพที่เป็นของรหัสผ่านตนเองก็จะต้องรอให้ระบบสุ่มขึ้นมาจนสามารถที่จะเลือกได้ถูกต้องซึ่งอาจจะนานกว่ารหัสผ่านแบบตัวอักษรในบางครั้ง เข้าได้ใช้แนวความคิดที่ว่าผู้ใช้งานสามารถจำรูปภาพที่ตนเองชอบได้มากกว่ารูปภาพชนิด

อื่นๆ แต่ระบบนี้อนุญาตให้ผู้ใช้งานนำรูปภาพที่เป็นของตนเองนำมาเข้าลงทะเบียนเป็นรหัสผ่านรูปภาพได้ซึ่งเป็นข้อดีอย่างหนึ่งเช่นกัน



ภาพที่ 2.5 Draw a secret

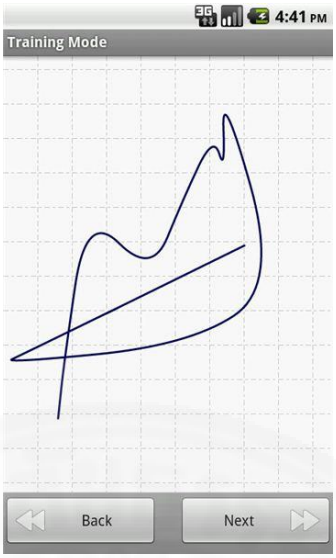
ที่มา : *"Image-based Authentication for Mobile Phones using user's Favorite Image_in Human-Computer Interaction with Mobile"* โดย Takada and Koike

Farnaz, Maslin & Azizah (2013) ได้นำรหัสผ่านแบบ Passface มาเพิ่มความปลอดภัยขึ้น เรียกว่า Secure Passface (S-Passface) โดยทำการเปลี่ยนจากการใช้เมาส์คลิกที่รูปภาพใบหน้าบุคคลมาเป็นการใช้แป้นพิมพ์ทำการพิมพ์ตัวอักษรที่กำกับอยู่ใต้รูปภาพใบหน้าบุคคลแทน เนื่องจากการคลิกที่รูปภาพใบหน้าบุคคลนั้น อาจทำให้ผู้ไม่หวังดีสามารถขโมยรหัสผ่านโดยใช้เทคนิคที่เรียกว่า shoulder surfing นั่นคือ การแอบมองอยู่ด้านหลังเพื่อจดจำรหัสผ่านของผู้ใช้

การที่รหัสผ่านแบบ S-Passface จะใช้ตัวอักษรกำกับใต้รูปภาพใบหน้าบุคคล มาต่อกันเป็นรหัสผ่านแทนการคลิก ทำให้ผู้ไม่หวังดีขโมยรหัสได้ยากขึ้น แต่การใช้รูปภาพใบหน้าบุคคลซึ่งผู้ใช้อาจจะไม่รู้จัก ทำให้มีข้อเสียในการจดจำรูปภาพใบหน้าบุคคลเหล่านั้นซึ่งจะส่งผลให้ผู้ใช้จำรหัสผ่านไม่ได้

ภาพที่ 2.6 S-Passface

จากงานวิจัย ที่ใช้ตารางกริด Jermyn, Monrose, Reiter, and Rubin (1999) ได้นำเสนอวิธีการที่เรียกว่า Draw a secret (DAS) ให้ผู้ใช้งานลากเส้นวาดรูปที่มีความเฉพาะของตนเองที่รู้ ผู้ใช้งานจะต้องวาดภาพ 2 มิติ ลงบนระบบกริดพื้นที่ว่าง โดยแค่ละช่องกริดจะเป็นคู่อันดับที่จะเก็บตำแหน่งของรูปภาพที่ผู้ใช้งานลากเส้นผ่านไว้ ระบบจะเก็บเป็นลำดับก่อนหลังในการลาดเส้นของผู้ใช้งานด้วย ซึ่งจะเป็นข้อเสียเปรียบด้วยเพราะผู้ใช้งานจะต้องจดจำลำดับการลกเส้นก่อนหลังของตนเองให้ถูกต้องด้วย ในสถานการณ์พิสูจน์ตัวตนระบบจะให้ผู้ใช้งานลากเส้นวาดรูปภาพที่เป็นรหัสผ่านของตนเอง ถ้าลากเส้นผ่านช่องกริดแลลำดับก่อนหลังได้ถูกต้องตามที่ได้ลงทะเบียนไว้ในขั้นตอนแรกจะสามารถผ่านเข้าสู่ระบบได้ เขาได้กล่าวว่าเหตุที่เลือกใช้งานเป็นระบบกริดขนาด 5×5 ก็เพียงพอแล้ว ว่าเมื่อลากเส้นวาดรูปเต็มพื้นที่แล้วความเป็นไปได้ของรหัสผ่านมากกว่าแบบรหัสผ่านตัวอักษรในความยาวของรหัสผ่านเท่าๆ กันแล้วระบบนี้มีข้อจำกัดที่ว่าช่องกริดที่ใช้งานตะต้องมีความใหญ่พอดีไม่เล็กจนเกินไป เพราะถ้าช่องกริดเล็กจนเกินไปผู้ใช้งานจะลอกเส้นให้ผ่านบริเวณช่องกริดเดิมที่เป็นช่องรหัสผ่านของตนเองได้ยากยิ่งขึ้น และเพื่อประหยัดพื้นที่จอแสดงผลบน PDA ด้วยเหตุผลนี้จึงได้ทำบนกริดแบบ 5×5 ระบบนี้อาจจะถูกการขโมยข้อมูลที่เรียกว่า Dictionary attack เพื่อเดาการลากเส้นวาดรูปภาพเป็นคำศัพท์ที่มีความหมายก็เป็นได้ รวมถึงการขโมยข้อมูลแบบ Shoulder surfing อีกด้วย (Xiaoyuan, 2006)

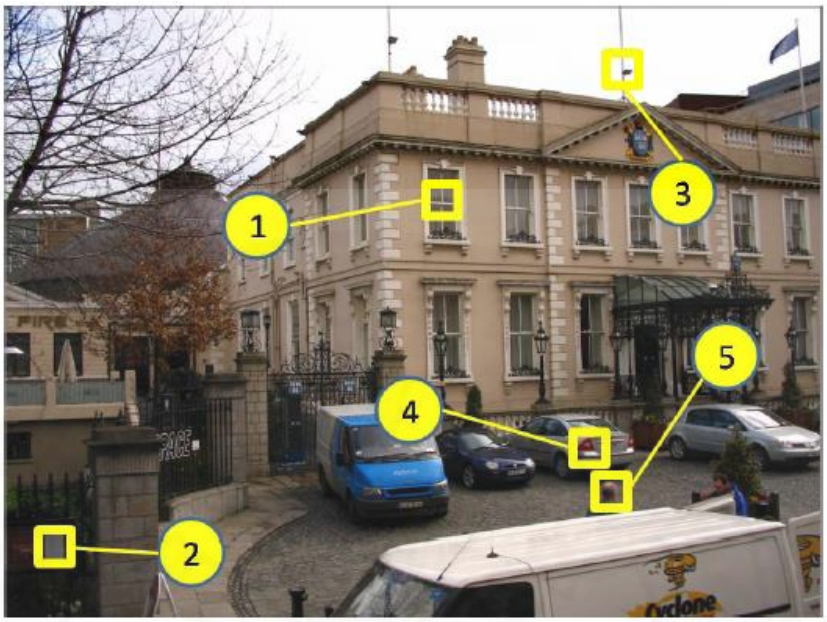


ภาพที่ 2.7 การลากเส้นวาดลายเซ็น

จากการคิดทฤษฎีในงานวิจัยของ Jermyn, Monrose, Reiter, and Rubin (1998) ได้นำเสนอระบบการพิสูจน์ตัวตนโดยให้ผู้ใช้เขียนลายเซ็นของตนเอโดนใช้เมาส์ควบคุม โดยระบบนี้จะแบ่งเป็น 2 ขั้นตอนคือการลงทะเบียนเข้าระบบและการพิสูจน์ตัวตน ในขั้นตอนการละทำเบียนเข้าระบบผู้ใช้งานจะต้องลากเส้นวาดเขียนลายเซ็นของตัวเองด้วยเมาส์ถอดรหัสออกมาเป็นพื้นที่ช่องของลายเซ็นนั้นได้ลากผ่านไปยังระบบกริด และเก็บลงฐานข้อมูลในส่วนของขั้นตอนการพิสูจน์ตัวตนขั้นแรกให้ผู้ใช้งานลากเส้นวาดลายเซ็นของตัวเองและทำการยืนยันข้อมูลที่ใส่อีกครั้ง ระบบทำการตรวจสอบความถูกต้อง และนำมาเปรียบเทียบกับฐานข้อมูลข้อดีของวิธีนี้คือผู้ใช้งานไม่ต้องจำข้อมูลใดมาก แค่เพียงลากเส้นวาดเป็นลายเซ็นของตนเองเท่านั้น ซึ่งยากต่อการปลอมแปลงจากบุคคลอื่น อย่างไรก็ตามไม่ใช่ทุกคนที่จะใช้เมาส์ควบคุมการลากเส้นได้อย่างดีเยี่ยม ดังนั้นความยากจ่อให้ผู้ใช้งานในวิธีนี้จึงอยู่ที่เรื่องการใช้เมาส์ควบคุมการลากเส้นวาดลายเซ็นของตนเอง ปัญหาส่วนนี้จะเป็นที่ผู้ใช้งานไม่สามารถบังคับให้เมาส์ลากเส้นวาดไปยังช่องที่ถูกลงทะเบียนเป็นรหัสผ่านของตนเอง ทางเลือกที่เป็นไปได้คือการใช้ปากกาอิเล็กทรอนิคส์แต่ก็ไม่แพร่หลายที่ต้องเสียค่าใช้จ่ายกับอุปกรณ์เสริมที่ราคาสูง พวกเข้าให้เสนอให้ใช้งานบน PDA ที่เป็นอุปกรณ์เล็กๆ จะได้ประโยชน์สูงสุด

Blonder (1996) ได้ออกแบบระบบรหัสผ่านรูปภาพที่เรียกว่า Pass-point ที่ผู้ใช้งานใช้เมาส์คลิกที่รูปภาพสถานที่รูปหนึ่ง ให้ได้จุดของรูปภาพที่ต้องการและลำดับก่อนหลังให้ถูกต้องทั้งหมด จุดเหล่านั้นได้กำหนดไว้แล้วในระบบว่าเป็นจุดใดบ้าง ไม่ได้ให้ผู้ใช้งานเป็นคนกำหนดรหัสผ่านเองด้วยตนเอง โดยการพิสูจน์ตัวตนผู้ใช้งานต้องคลิกเมาส์เลือกบริเวณที่ใกล้เคียงกับพื้นที่ของรูปภาพที่ได้ลงทะเบียนไว้ ได้อาศัยหลักการที่ว่าเมื่อเห็นรูปภาพแล้วผู้ใช้งานจะสามารถระลึกถึงจุดที่ได้เลือกมากกว่าการระลึกถึงตัวอักษร ซึ่งอาจเป็นข้อเสียที่ผู้ใช้งานไม่สามารถจำจุดที่ต้องทำเครื่องหมายเลือก

ตำแหน่งอย่างถูกต้องแม่นยำ ในรูปภาพหนึ่งที่มีรายละเอียดพิกเซลของรูปภาพมากกมายอาจจะเป็นเพียงจุดเล็กๆ ทำให้ผู้ใช้งานสับสนในการคลิกเลือกจุดบนภาพได้ (Xiaoyuan, 2006)

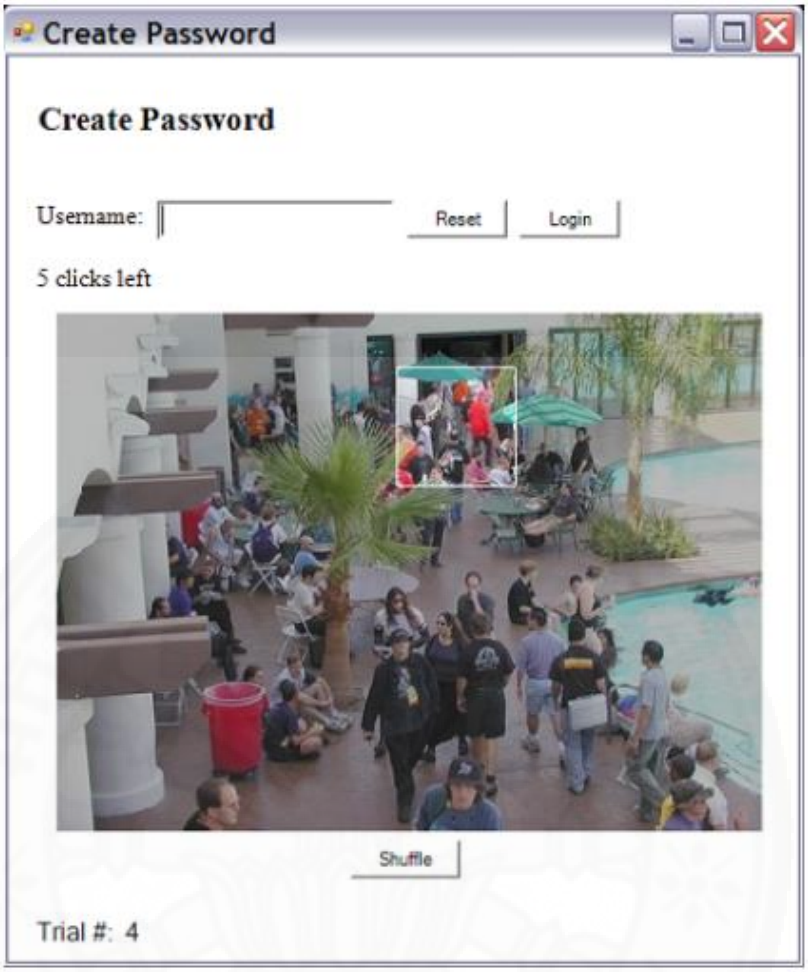


ภาพที่ 2.8 วิธีของ Blonder

ในงานวิจัยเกี่ยวกับรหัสผ่านรูปภาพอีกแบบหนึ่งของ Wiedenbeck, Waters, Birget, and Memon (1998) เป็นความคิดของ Pass-point เช่นกันโดนนำแนวคิดของ (Blonder, 1996) มาเพิ่มเติม ผู้ใช้งานสามารถใช้เมาส์คลิกลงบนภาพสถานที่นั้น ในตำแหน่งใดๆ ก็ได้ตามที่ผู้ใช้งานต้องการเพื่อลงทะเบียนเป็นรหัสผ่านรูปภาพของผู้ใช้งานเอง และเมื่อจุดนั้นบนภาพได้ถูกเลือกระบบจะสร้างพื้นที่ขยายเพิ่มขึ้นเพื่อรองรับผู้ใช้งานสามารถคลิกบริเวณพิกเซลใกล้เคียงกับจุดที่เลือกจริงมากที่สุดและตามลำดับก่อนหลังได้อย่างถูกต้อง ได้อาศัยข้อมูลที่ว่ารูปภาพใดๆ ก็สามารถใช้งานได้ทั้งหมดเพราะรูปอาจจะมีจุดที่น่าจดจำอยู่มากมายหลายจุด และทำให้ความเป็นไปได้ของรหัสผ่านรูปภาพสูงตามไปด้วย เขาได้ทดลองในกลุ่มตัวอย่างของเขาโดยแบ่งเป็น 2 กลุ่มคือ กลุ่มแรกให้ใช้งานรหัสผ่านแบบตัวอักษร อีกกลุ่มให้ใช้รหัสผ่านรูปภาพที่เขาได้เสนอแนวคิดไว้ ผลการทดลองพบว่าผู้ใช้งานสามารใช้งานและมีความอยากใช้งานรหัสผ่านรูปภาพมากกว่ารหัสผ่าตัวอักษร อย่างไรก็ตามเขาได้กล่าวไว้ว่า ผู้ใช้งานรหัสผ่านรูปภาพจะต้องเสียเวลาในการเรียนรู้ในการทำงานของระบบมากกว่ารหัสผ่านแบบตัวอักษร และแต่ปัญหาที่เกิดก็เป็นเรื่องเดิมคือความคลาดเคลื่อนการเลือกจุดบริเวณพิกเซลที่กำหนดไว้บนรูปภาพของตนเอง ซึ่งทำให้เสียเวลามากจะเหมาะสมกับภาพที่มีจุดน่าจดจำใหญ่ๆ เท่านั้น (Xiaoyuan, 2006)

ภาพที่ 2.9 PassPoint

Narender, Babu, Rao (2010) ได้เสนอว่าโดยระบบคอมพิวเตอร์ส่วยใหญ่ใช้งานรหัสผ่านเป็นแบบตัวอักษร ซึ่งผู้ใช้งานยากต่อการจดจำ ส่งผลให้ผู้ใช้งานสร้างรหัสผ่านแบบง่ายสั้นๆ ไม่ปลอกภัย รหัสผ่านรูปภาพจึงได้ถูกออกแบบมาเพื่อง่ายต่อผู้ใช้งานยิ่งขึ้น ได้เสนอวิธี DAS (Draw-A-Secret) ในระบบของเขาใช้สื่อกลางที่ในการช่วยจำและระลึกถึง โดยการแสดงภาพขึ้นมาหรือภาพช่วย เพื่อหาจุดที่ผู้ใช้งานได้ใช้เมาส์คลิกในครั้งแรก ในทางจิตวิทยาจะเป็นการช่วยระลึกถึงของการกระทำ ภาพจำได้ง่ายกว่าเป็นคำพูด ในระบบนี้ต้องการใช้งานรหัสผ่านที่รวดเร็วฉะนั้นเวลาจึงเป็นสิ่งสำคัญในการทดสอบ โดยวาดรหัสผ่านลงไปโดยจะเก็บตามคู่อันดับของการลาอกเส้นรหัสผ่าน ระยะก็จะเป็นผลรวมของจำนวนช่องที่ลากเส้นรูปภาพลงไป ยิ่งเพิ่มจำนวน สโต๊คของการใส่รหัสผ่านมากเท่าไหร่ยิ่งทำให้การแก้รหัสผ่านได้ยากขึ้นไปด้วย และหมายถึงการขโมยข้อมูลที่ยากขึ้น แต่ก็ทำให้ยากต่อการจำกับผู้ใช้งาน เขาได้ทดลองกับกลุ่มการทดลองที่ใช้รหัสผ่านตัวอีกษรปละรหัสผ่ายรูปภาพแบบ DAS ที่เขาได้เสนอไว้พบว่าหลังจากผ่านไป 5 สัปดาห์ กลุ่มทดลองที่ใช้งานรหัสผ่านรูปภาพ DAS ยังสามารถจดจำรหัสผ่านของตนเองได้อยู่



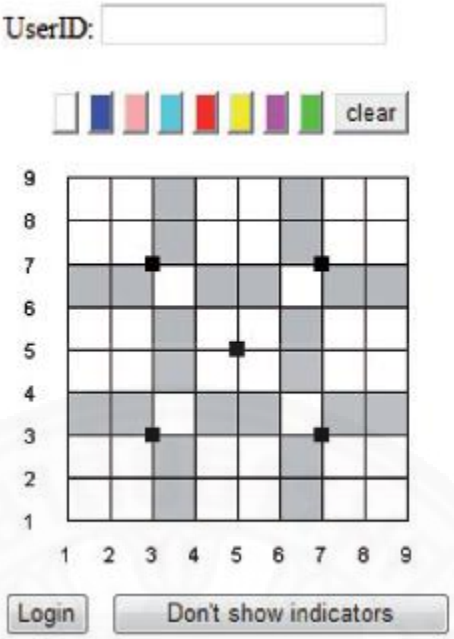
ภาพที่ 2.10 ระบบ Persuasive Cued Click-Point (PCCP) ของ Elizabeth

Elizabeth (2010) การคลิกเลือกพื้นที่บนรูปภาพทีประโยชน์มากทั้งการช่วยระลึกถึงและความจำ อย่างไรก็ตาม ขนาดรูปภาพและจำนวนครั้งในการคลิกเลือกแต่ละครั้งก็จะส่งผลโดยตรงกับความปลอดภัยของการใช้รหัสผ่านนั้นๆ ที่ดีกว่ารหัสผ่านตัวอักษร ถึงแม้ว่าตัวอักษรที่สามารถจดจำได้แต่ก็มีความปลอดภัยต่ำสามารถเดาได้ง่าย หรือถ้ายากต่อการเดาได้ผู้ใช้งานก็ไม่สามารถจดจำได้อีกเช่นกัน รหัสผ่านรูปภาพจึงเข้ามาแทนที่รหัสผ่านตัวอักษร รหัสผ่านรูปภาพมีข้อแตกต่างจากแบบอักษร 2 ข้อคือประการแรกรูปภาพใช้เป็นสัญลักษณ์ที่ทำให้มนุษย์เก็บในความทรงจำได้ดีกว่าตัวอักษร ฉะนั้นรหัสผ่านจึงเป็นข้อได้เปรียบในเรื่องความจำ ประการที่สองบางอย่างเป็นเครื่องช่วยเรียกคืนความจำที่ทำให้คนสามารถจำได้และจำแนกรหัสผ่านประจำของพวกเขา โดยจะสนใจที่ขนาดของรูปภาพจำนวนจุดบนภาพที่ได้คลิกเลือกไป ขึ้นอยู่กับอุปกรณ์ของผู้ใช้งานสามารถรองรับขนาดภาพได้แค่ไหน

ระบบนี้จะแสดงถึงลำดับการคลิกลงบนรูป และระบบจะถามให้คลิกบนรูปที่ 1 ตำแหน่งในแต่ละภาพด้วย โดยที่รูปแรกระบบจะกำหนดมาให้เอง แต่รูปต่อๆมานั้นจะเป็นรูปที่ได้รับการพิจารณาเลือกจากผู้ใช้งานคลิก นั้นหมายถึงการคลิกนั้นก็จะได้ตำแหน่งที่แตกต่างกันในแต่ละครั้งที่เป็นภาพใดๆ ในส่วนนี้ก็จะเป็นตัวช่วยความจำให้กับผู้ใช้งานที่จะพยายามคลิกเลือกตำแหน่งที่ถูกต้อง ถ้าพวกเขาเห็นรูป พวกเขาก็จะรู้ว่าเขาได้เลือกคลิกลงบนตำแหน่งใดไป ในการใส่รหัสผ่านแบบคลิกนี้ก็ต้องรับว่าผู้ใช้งานอาจจะไม่สามารถคลิกลงบนตำแหน่งเดิมอย่างแม่นยำได้ อาจจะมีการคลาดเคลื่อนด้วยที่ต้องกำหนดอยู่รอบจุดๆ ที่ผู้ใช้งานได้เลือกตำแหน่งนั้น และยอมรับจุดเหล่านั้นได้ด้วย โดยระบบ PCCP นี้จะทำ viewport ที่ทำสัญลักษณ์ไว้ที่ส่วนประกอบของรูปภาพและถามผู้ใช้งานให้คลิกจุดที่ต้องการเสือกภายใน viewport ที่ให้มาเท่านั้นด้วย ดังนั้นผลลัพธ์ก็จะหลากหลายมาก ถ้าผู้ใช้งานไม่สามารถที่จะจำจุดๆที่ทำมา viewport มาให้ได้ผู้ใช้งานสามารถกดปุ่ม shuffle เพื่อให้ทำการสุ่มจุด viewport ให้แสดงกับผู้ใช้งานในตำแหน่งใหม่อีกครั้งได้ ปุ่มนี้จะทำให้แน่ใจได้ว่าจุดที่ได้จะเป็นความหลากหลายจริงๆโดยระบบ PCCP นี้มีความปลอดภัยที่มากกว่าระบบอื่นๆ คือจะไปเปรียบเทียบกับตัวอักษรที่ได้กรอกเป็นข้อมูลควบคู่ไปด้วย โดยแค่จะเก็บคุณลักษณะของความปลอดภัยแบบตัวอักษรไว้รวมด้วยในระบบนี้ซึ่งจะต้องคิดความเป็นไปได้ทั้งหมด (password space) ของหัสผ่านตัวอักษร

Tao & Carlisle (2007) ได้นำเสนอความคิดในระบบรหัสผ่านรูปภาพ จากหมากรุกจีน (GO) มาใช้ในการออกแบบ เป็นวิธีที่เรียกว่า Pass-Go ออกแบบเป็นระบบกริด (Grid based) ที่ให้ผู้ใช้งานเลือกจุดตัดบนกริดลากเส้นเชื่อมระหว่างจุดตัดถึงกันหรือจะทำเป็นจุดเครื่องหมายไว้เหมือนเป็นการวางหมาก โดยดังเดิมรหัสผ่านใช้เป็นแบบตัวอักษรเพื่อระบุตัวตนของผู้ใช้งาน ซึ่งสามารถถูกโจมตีจากวิธี dictionary attack อีกทั้งความจำกัดด้านความจำของมนุษย์ บ่อยครั้งที่ผู้ใช้งานใช้รหัสผ่านที่ง่ายต่อการจำและสามารถเดาได้ง่าย จึงได้เสนอวิธีนี้เพื่อช่วยให้จำง่ายและกันการโจมจีแบบ dictionary โดยวิธี Pass-Go รี้ได้รวมข้อดีของ DAS (Draw-A-Secret ของ Jermyn, 1999) ทั้งทางความปลอดภัยที่ดีด้วย

วิธีนี้ต่างจากวิธี DAS ที่ต้องการให้ผู้ใช้งานเลือกตรงจุดที่เป็นจุดตัดของเส้นแบ่งกริดเพื่อใส่รหัสผ่าน และระบบคู่อันดับเป็นการอ้างอิงถึงจุดตัดของเส้นแบ่งกริดไม่ได้อ้างอิงถึงช่องเซลล์เหมือนในวิธี DAS โดยจุดตัดนี้เสมือนเป็นจุดอ้างอิงที่ไม่ใช่พื้นที่ช่องเซลล์ และเป็นจุดอ้างอิงที่ผู้ใช้งานเลือกได้เลยไม่ต้องมีการคิดความคลาดเคลื่อนของพิกเซลเพื่อไว้ ข้อดีของการเปลี่ยนจากเซลล์มาเป็นการคลิกบนจุดตัด อีกประการคือสามารถลากเส้นตรงได้ง่ายขึ้นปละใน PASS-Go มีขนาด G×G แต่ในระบบวิธี DAS จะเป็นแบบ (G-1)×(G-1) บนพื้นที่การแสดงรูปภาพเดียวกัน



ภาพที่ 2.11 การออกแบบ Pass-Go

ในขณะที่วิธี DAS เป็นการแสดงผลจริงที่ผู้ใช้งานได้ลอกเส้นวาดรูปลงบนกริด แต่ Pass-Go จะแสดงบนจุดตัดที่เป็นรูปแบบแน่นอนทำให้ผู้ใช้งานไม่สับสนในการทำงานของตนเอง ในการเข้ารหัสตำแหน่งที่ผู้ใช้งานลากเส้นจะเก็บเป็นคู่อันดับเหมือนกันกับวิธี DAS เป็นแบบกริด 2 มิติเหมือนกัน ในแนวคิดของการมีจุดอ้างอิงที่เลียนแบบมาจากหมากรุกโกะที่รียกว่าจุดดาว (Star) ใน Pass-Gow ได้นำมาใส่ไว้ด้วยกัน 5 จุดเล็กๆ ในขนาดกริดทั้งหมดเป็น 19×19 เพื่อช่วยในการใช้งานที่ง่ายขึ้นของผู้ใช้งานในการเริ่มจะสิ้นสุดการคิดรหัสผ่านของตนเอง ทั้งยังเป็นจุดอ้างอิงที่สามารถช่วยให้ผู้ใช้งานสามารถช่วยจำว่าได้ลากเส้นรอบๆ จุดนั้นไว้อย่างไร การออกแบบขนาดของกริดเขาได้ออกแบบเป็น 9×9 ใช้พื้นที่เพียง 25 ตารางเซนติเมตร ซึ่งสามารถติดตั้งบน PDA ได้

ในส่วนของการแสดงผลที่เป็นสี เขาได้เลือกสีที่ใช้ 8 สี คือ สีดำ สีแดง สีน้ำเงิน สีเหลือง สีเขียว สีชมพู สีเขียวเข้ม สีม่วง โดยได้ออกแบบวางไว้รอบกริด สีของเส้นหรือจุดสามารถเปลี่ยนได้โดนการคลิกปุ่มและสีที่เป็นค่าเริ่มต้นคือสีดำ โดยเขาได้เก็บข้อมูลผู้ใช้งานในการเลือกสีทำเป็นรหัสป่านของตนเองด้วย จะเห็นว่า สีแดง สีน้ำเงิน สีเขียว เป็นสีที่ผู้ใช้งานนิยมใช้มากที่สุด 3 อันดับแรก ซึ่งต่อมาเป็นสีดำที่เป็นค่าสีเริ่มต้น ในเรื่องของการรองรับการขโมยข้อมูลแบบ Shoulder surfing เขาได้เสนอ 2 แนวทาง คือ ไม่ให้แสดงผลรูปภาพเส้นหรือจุดที่ผู้ใช้งานได้สร้างไว้เลย ให้เห็นแค่การเคลื่อนที่ของเมาส์เท่านั้น ซึ่งเป็นจะเป็นการยากต่อการจดจำและเข้าใจของผู้ใช้งานอย่างแน่นอน ประที่ 2 ให้เกิดภาพที่สุ่มให้เกิดขึ้นบนกริดที่ผู้ใช้งานกำลังสร้างรหัสผ่านของตนเองอยู่ โดยผู้ใช้งานกดปุ่มคลิกขวาที่เมาส์ รูปภาพที่สุ่มให้แสดงในตำแหน่งที่ไม่แน่นอนก็จะแสดงขึ้น วิธีนี้ก็จะส่งผลให้งานยาก

ต่อการจำและสับสนว่าส่วนใดเป็นรหัสผ่านที่แท้จริงของตนเอง จึงต้องหาวิธีที่ได้ผลในทางที่ดีมากกว่านี้

ในทางจิตวิทยา Kristin, Heather (2004) ได้ทำกรณีศึกษาคนจะระลึกถึงภาพ คำพูด หรือทั้งภาพและคำพูดที่อยู่ด้วยกันในความจำส่วน short term memory วิธีการทดลองของผู้วิจัยมี 3 กลุ่มๆละ 10 คนคละเพศ อายุเฉลี่ยประมาณ 25.3 ปีทั้งชายหญิง กลุ่มแรกดูรายชื่อคำ 18 คำ กลุ่มสองดูรูปภาพ 18 รูปที่มีความเชื่อมโยงกับคำพูดด้วย และกลุ่มสาม ดูทั้งภาพและคำพูดอยู่ด้วยกัน มีเวลาให้ 1 นาทีมรการจำหลังจากนั้นทิ้งระยะ 30 วินาทีให้พัก หลังจากนั้นให้การะลึก (Recall) ถึงสิ่งเหล่านั้นเวลา 1 นาทีเท่าที่จำได้ แล้วบอกให้ผู้วิจัยเขียนลงไปและตรวจสอบว่าถูกต้องหรือไม่ ในการบันทึกผลจะบันทึกเพศและอายุ ในการทดลองทางสถิติพบว่าการจำรูปภาพและคำพูดอยู่ด้วยกันจะดีที่สุด ว่ามีคำพูดตัวอักษรเพียงอย่างเดียว ดังนั้นจึงสนับสนุนสมมุติฐานที่ว่ามีภาพและคำพูดอยู่ด้วยกันจะช่วยจำได้ง่ายกว่ามีเพียงคำพูดอย่างเดียว แต่รูปภาพและคำพูดที่อยู่ด้วยกันยังไม่ดีกว่าอย่างมีนัยสำคัญกับกลุ่มที่มีรูปภาพอย่างเดียว

บทที่ 3

วิธีดำเนินงานวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อเป็นการศึกษาเกี่ยวกับการใช้งานง่าย (Usability) และความปลอดภัย (Security) ของรหัสผ่านรูปภาพแบบกริด ที่มีการใช้รูปภาพใบหน้าบุคคลปรากฏอยู่แต่ละช่องของกริดในการสร้างรหัสผ่าน โดยจะส่งผลให้เกิดกระบวนการระลึกได้ (Recall) ของรหัสผ่านรูปภาพที่ผู้ใช้งานได้มีการสร้างไว้ ซึ่งในบทนี้เป็นการกล่าวถึงวิธีดำเนินงานวิจัย โดยประกอบไปด้วย ระเบียบวิธีการดำเนินงานวิจัย โครงสร้างและขั้นตอนการทำงานของระบบ และการออกแบบการวัดผลการทดลองเพื่อประเมินประสิทธิภาพของระบบที่ได้ออกแบบ

3.1 ระเบียบวิธีการทดลอง

ขั้นตอนการศึกษาและออกแบบรหัสผ่านได้นำรูปภาพของใบหน้าบุคคล 4 ประเภท คือ ผู้ชาย ผู้หญิง เด็ก และการ์ตูน เนื่องจากมีงานวิจัยที่ระบุว่ามนุษย์สามารถจดจำใบหน้าบุคคลได้ดีกว่าวัตถุอื่น ประกอบกับตัวอักษรภาษาอังกฤษที่ถูกสุ่มขึ้นมา เพื่อการป้องกันการขโมยรหัสผ่านด้วยเทคนิค Shoulder surfing โดยไม่ให้ผู้ใช้คลิกที่ช่องกริด แต่ให้มองตัวอักขระที่กำกับไว้ในแต่ละช่องและพิมพ์แทน ด้วยวิธีการนี้จะทำให้ผู้ไม่หวังดีขโมยรหัสผ่านได้ยากขึ้น งานวิจัยนี้ได้สุ่มตัวอักษรภาษาอังกฤษ 2 ตัว เพื่อไม่ให้ถูกโจมตีด้วยเทคนิค Dictionary attack

3.1.1 ตัวแปรและสมมติฐาน

งานวิจัยศึกษาและออกแบบรหัสผ่านที่ช่วยให้ผู้ใช้จดจำรหัสผ่านได้ง่ายขึ้น มีตัวแปรที่ใช้ในการศึกษาและสมมติฐาน ดังนี้

3.1.1.1 ตัวแปรอิสระ (Independent Variable)

งานวิจัยนี้มีตัวแปรอิสระที่ใช้ในการศึกษา 2 ตัวแปร คือ

1. จำนวนรอบในการตั้งรหัสผ่าน คือ จำนวนรอบที่ใช้ในการสร้างรหัสผ่านรูปภาพในขั้นตอนการลงทะเบียนและการพิสูจน์ตัวตน จำแนกค่าของตัวแปรได้ 2 ระดับ คือ การใช้

จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ โดยตั้งรหัสผ่านทั้งหมด 8 รูปภาพ และการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ โดยตั้งรหัสผ่านรอบละ 4 รูปภาพ รวมทั้งหมด 8 รูปภาพ

2. การนำเสนอรูปแบบใบหน้าบุคคล คือ การนำเสนอรูปแบบใบหน้าบุคคลที่มีลักษณะการใช้รูปภาพใบหน้าบุคคลสำหรับรหัสผ่าน 4 ประเภท ได้แก่ รูปภาพใบหน้าผู้ชาย รูปภาพใบหน้าผู้หญิง รูปภาพใบหน้าเด็ก และรูปภาพใบหน้าการ์ตูน โดยจำแนกค่าของตัวแปรได้ 2 ระดับ คือ การนำเสนอรูปแบบใบหน้าบุคคลที่มีลักษณะการใช้รูปภาพใบหน้าบุคคลขนาดใหญ่ประเภทละ 1 รูปภาพรวม 4 รูปภาพ แล้วตัดแบ่งแต่ละรูปภาพออกเป็นส่วนๆ เท่าๆกัน รูปภาพละ 9 ส่วน รวมทั้งหมด 36 ส่วน และ การนำเสนอรูปแบบใบหน้าบุคคลที่มีลักษณะการใช้รูปภาพใบหน้าบุคคลขนาดเล็กประเภทละ 9 รูปภาพ จำนวน 4 ประเภท รวมทั้งหมด 36 รูปภาพ

3.1.1.2 ตัวแปรตาม (Dependent Variable)

1. ประสิทธิภาพการใช้งานของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ ประกอบด้วย คะแนนการพิสูจน์ตัวตนด้วยรหัสผ่าน และความสำเร็จในการพิสูจน์ตัวตน

2. ประสิทธิภาพความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ ประกอบด้วย คะแนนการโจรกรรมรหัสผ่านของวิธีการพิสูจน์ตัวตนด้วยรหัสผ่าน และความสำเร็จในการโจรกรรมรหัสผ่านรูปภาพ

3. ความพึงพอใจที่ผู้ใช้มีต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านที่ได้ออกแบบในงานวิจัย โดยที่ผู้เข้าร่วมการทดลองจะได้ทำแบบสอบถามความพึงพอใจหลังการทดลองการพิสูจน์ตัวตนด้วยรหัสผ่านเสร็จสิ้นในครั้งสุดท้าย

3.1.1.3 สมมติฐานในการทดลอง

ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน มีผลต่อด้านการใช้งาน (Usability) และด้านความปลอดภัย (Security) ของรหัสผ่านรูปภาพ

1. การเปรียบเทียบประสิทธิภาพด้านการใช้งาน และด้านความปลอดภัยระหว่างจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

H_0 : จำนวนรอบในการตั้งรหัสผ่าน ไม่มีอิทธิพลต่อ การใช้งานรหัสรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่าน มีอิทธิพลต่อ การใช้รหัสผ่านรูปภาพ

H_0 : จำนวนรอบในการตั้งรหัสผ่าน ไม่มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่าน มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

2. การเปรียบเทียบประสิทธิภาพด้านการใช้งาน และด้านความปลอดภัย ระหว่างระหว่างวิธีการนำเสนอรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วน กับวิธีการนำเสนอรูปภาพใบหน้าบุคคลย่อย

H_0 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ การใช้งานรหัสรูปภาพ

H_1 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ การใช้รหัสผ่านรูปภาพ

H_0 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

H_1 : วิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

3. การเปรียบเทียบการมีอิทธิพลร่วมกัน ระห่วงจำนวนรอบในการตั้งรหัสผ่าน กับวิธีการนำเสนอรูปภาพใบหน้าบุคคล ที่มีผลต่อด้านการใช้งาน และด้วยความปลอดภัย

H_0 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ การใช้งานรหัสรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ การใช้รหัสผ่านรูปภาพ

H_0 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล ไม่มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

H_1 : จำนวนรอบในการตั้งรหัสผ่านร่วมกับวิธีการนำเสนอรูปภาพใบหน้าบุคคล มีอิทธิพลต่อ ความปลอดภัยของรหัสผ่านรูปภาพ

3.1.2 รูปแบบการวิจัย

การศึกษาปัจจัยที่มีผลต่อการนำรูปภาพใบหน้าบุคคลมาช่วยสร้างเป็นรหัสผ่าน และการมีการสุ่มตัวอักษรภาษาอังกฤษกำกับใต้รูปภาพเพื่อนำมาเป็นรหัสผ่าน ขั้นตอนการทดลองมี 2 ส่วน คือ ขั้นตอนการสร้างรหัสผ่าน(register) และขั้นตอนการเข้าสู่ระบบ(login) ผู้เข้าร่วมทดลองจะถูกแบ่งออกเป็น 4 กลุ่ม ได้แก่ รูปภาพใหญ่แบ่งเป็นส่วนๆ ประกอบกับสร้างรหัสผ่าน 1 รอบ รูปภาพใหญ่แบ่งเป็นส่วนๆ ประกอบกับสร้างรหัสผ่าน 2 รอบ รูปภาพย่อยในแต่ละกริด ประกอบกับสร้างรหัสผ่าน 1 รอบ และรูปภาพย่อยในแต่ละกริด ประกอบกับสร้างรหัสผ่าน 2 รอบ ซึ่งแสดงได้ดังตาราง 3.1

ตารางที่ 3.1

การออกแบบการทดลองการใช้งานระบบรหัสผ่าน

รูปแบบการทดลอง	รูปภาพใหญ่ตัดแบ่งเป็นส่วนๆ	รูปภาพย่อยในแต่ละกริด
1 รอบ	กลุ่มที่ 1	กลุ่มที่ 3
2 รอบ	กลุ่มที่ 2	กลุ่มที่ 4

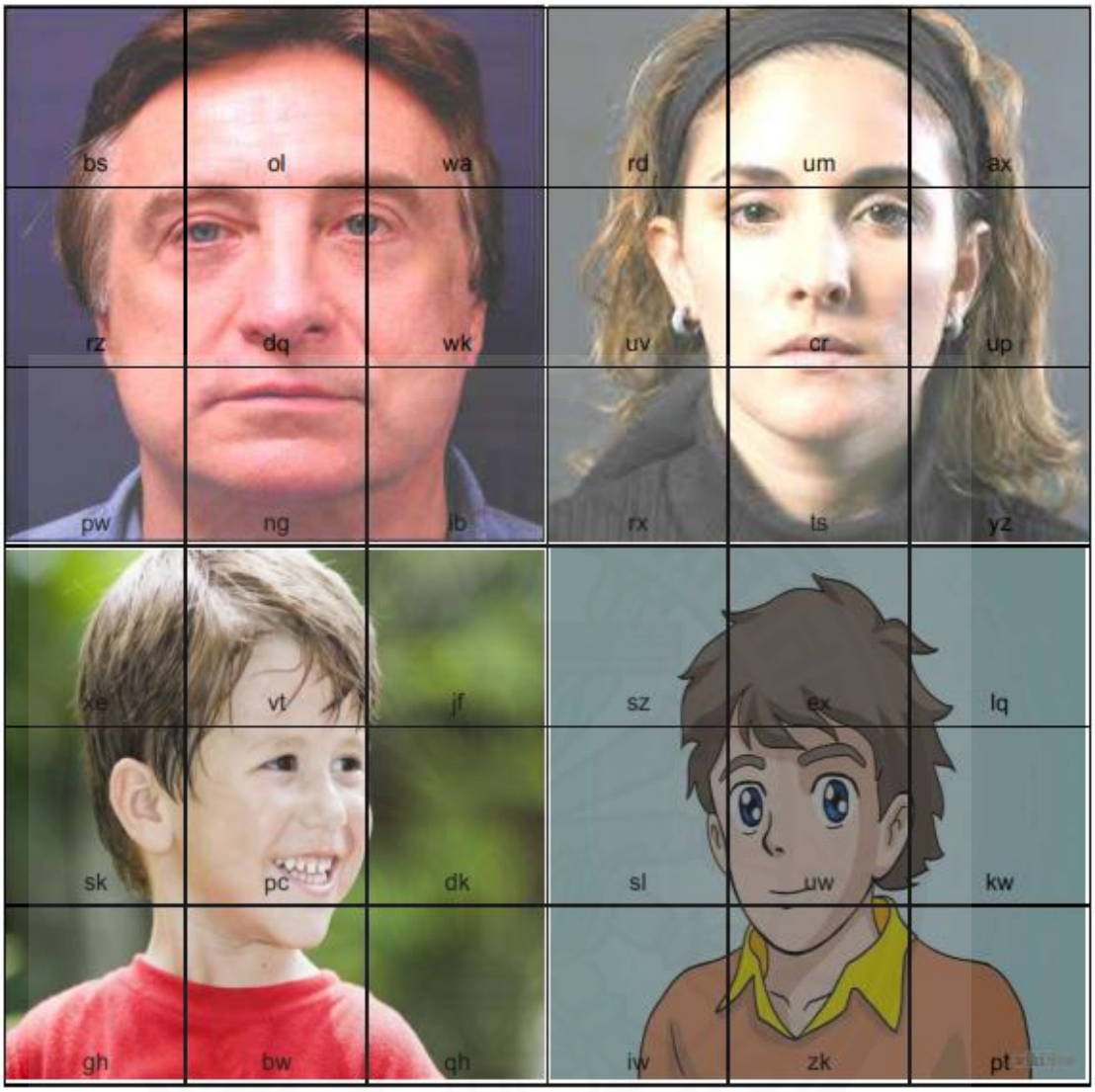
งานวิจัยนี้เป็นการวิจัยเชิงทดลอง (Experimental Research) ใช้รูปแบบการทดลองแบบ 2x2 Between Subject Design การทดลองแบ่งกลุ่มทดลองตามปัจจัยที่ศึกษา ซึ่งแบ่งเป็น 4 กลุ่มการทดลอง โดยให้แต่ละกลุ่มการทดลองทำการทดลองเพียงกลุ่มละ 1 รูปแบบ

ผู้เข้าร่วมทดลองจะถูกแบ่งออกเป็น 4 กลุ่ม ได้แก่ การสร้างและพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ 1 รอบร่วมกับการนำเสนอรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนๆ การสร้างและพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ 2 รอบร่วมกับการนำเสนอรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนๆ การสร้างและพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ 1 รอบ ร่วมกับการนำเสนอรูปภาพใบหน้าบุคคลขนาดเล็กในแต่ละช่องกริด และการสร้างและพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ 2 รอบร่วมกับการนำเสนอรูปภาพใบหน้าบุคคลขนาดเล็กในแต่ละช่องกริด

การทดลองด้านการใช้งาน (Usability) จะทำการทดลองการพิสูจน์ตัวตนทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 หลังจากการลงทะเบียนทันที ครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 7 วัน และครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน

การทดลองด้านความปลอดภัย (Security) จะทำการทดลองการโจรกรรมรหัสผ่านโดยวิธีการแอบมอง (Shoulder surfing) หลังจากผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนในครั้งแรกทันที โดยใหเทดลองโจรกรรมได้ไม่เกิน 3 ครั้ง

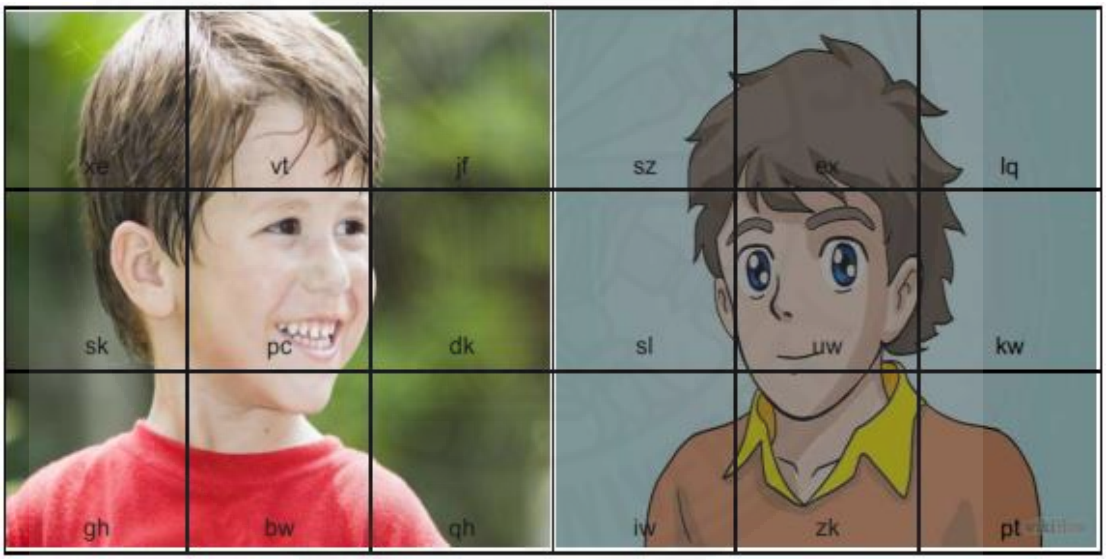
การประเมินประสิทธิภาพของวิธีการพิสูจน์ตัวตนที่ออกแบบ โดยการวัดประสิทธิภาพด้านการใช้งานซึ่งประกอบไปด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ และความสำเร็จในการพิสูจน์ตัวตน และการวัดประสิทธิภาพด้านความปลอดภัยจะประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมพิสูจน์ตัวตน และวัดความพึงพอใจที่ผู้ใช้มีต่อระบบพิสูจน์ตัวตนด้วยแบบสอบถาม



ภาพที่ 3.1 ตัวอย่างรูปแบบการทดลองของกลุ่มที่ 1

กลุ่มการทดลองที่ 1 จะใช้การนำเสนอรูปแบบของรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าบุคคลขนาดใหญ่ จาก 4 ประเภท ได้แก่ ใบหน้าผู้ชาย ใบหน้าผู้หญิง ใบหน้าเด็ก และใบหน้าการ์ตูน โดยใช้รูปภาพใบหน้าบุคคลประเภทละ 1 รูปภาพ แล้วเป็นส่วนในแต่ละรูปภาพเป็น 9 ส่วน รวมทั้งหมด 36 ส่วน การปรากฏของรูปภาพแต่ละครั้งจะมีการสุ่มตัวอักษรภาษาอังกฤษช่องละ 2 ตัวอักษร ซึ่งตัวอักษรนี้จะถูกสุ่มขึ้นมาใหม่ทุกครั้งที่มีการปรากฏของรูปภาพใบหน้าบุคคล โดยให้ตั้งรหัสผ่าน 1 รอบ เลือก 8 รูปภาพ เมื่อเลือกภาพใดให้พิมพ์ตัวอักษรที่อยู่ข้างใต้ของภาพนั้นให้ถูกต้องเพื่อนำไปใช้เป็นรหัสผ่าน

ภาพที่ 3.2 ตัวอย่างรูปแบบการทดลองของกลุ่มที่ 2 รอบที่ 1



ภาพที่ 3.3 ตัวอย่างรูปแบบการทดลองของกลุ่มที่ 2 รอบที่ 2

กลุ่มการทดลองที่ 2 จะใช้การนำเสนอรูปแบบของรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าบุคคลขนาดใหญ่ จาก 4 ประเภท ได้แก่ ใบหน้าผู้ชาย ใบหน้าผู้หญิง ใบหน้าเด็ก และใบหน้าการ์ตูน โดยใช้รูปภาพใบหน้าบุคคลประเภทละ 1 รูปภาพ แล้วเป็นส่วนในแต่ละรูปภาพเป็น 9 ส่วน โดยจะแสดงรอบละ 2 ประเภท รวม 18 ส่วนต่อรอบ ผู้ใช้จะต้องเลือกรูปภาพใบหน้าบุคคลรอบละ 4 รูปภาพ จำนวน 2 รอบ รวมจำนวนที่ผู้เข้าร่วมการทดลองเลือก 8 รูปภาพจากทั้งหมด 36 รูปภาพ การปรากฏของรูปภาพแต่ละครั้งจะมีการสุ่มตัวอักษรภาษาอังกฤษช่องละ 2 ตัวอักษร ซึ่งตัวอักษรนี้

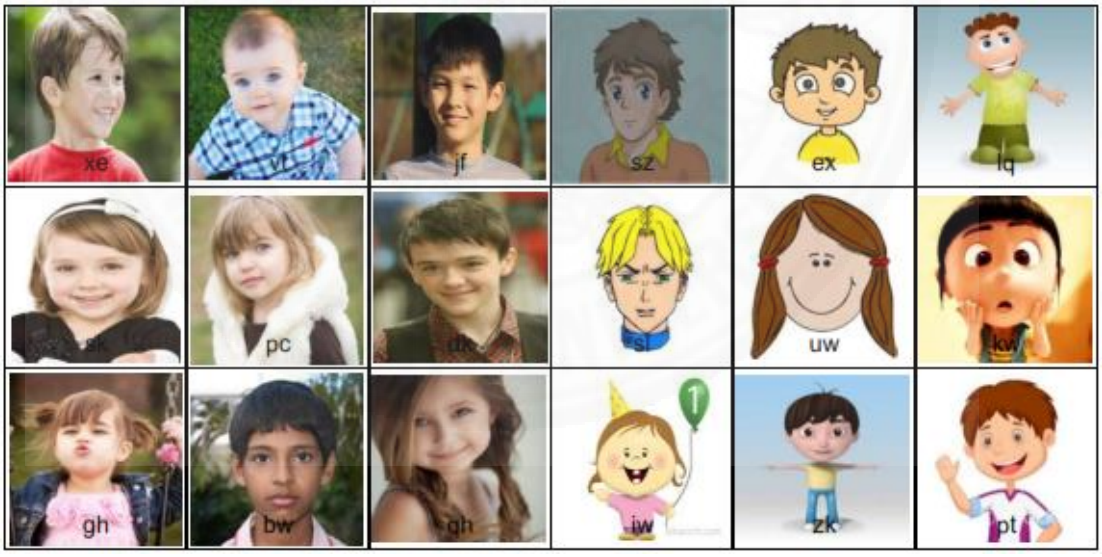
จะถูกสุ่มขึ้นมาใหม่ทุกครั้งที่มีการปรากฏของรูปภาพใบหน้าบุคคล เมื่อเลือกภาพใดให้พิมพ์ตัวอักษรที่อยู่ข้างใต้ของภาพนั้นให้ถูกต้องเพื่อนำไปใช้เป็นรหัสผ่าน

ภาพที่ 3.4 ตัวอย่างรูปแบบการทดลองของกลุ่มที่ 3

กลุ่มการทดลองที่ 3 จะใช้การนำเสนอรูปแบบของรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าบุคคลขนาดเล็ก จาก 4 ประเภท ได้แก่ ใบหน้าผู้ชาย ใบหน้าผู้หญิง ใบหน้าเด็ก และใบหน้าการ์ตูน โดยใช้รูปภาพใบหน้าบุคคลประเภทละ 9 รูปภาพ รวม 36 รูปภาพ ผู้เข้าร่วมการทดลองจะต้องเลือกรูปภาพใบหน้าบุคคลจำนวน 8 รูปภาพจากทั้งหมด 36 รูปภาพ การปรากฏของรูปภาพแต่ละครั้งจะมีการสุ่มตัวอักษรภาษาอังกฤษช่องละ 2 ตัวอักษร ซึ่งตัวอักษรนี้จะถูกสุ่มขึ้นมาใหม่ทุก

ครั้งที่มีการปรากฏของรูปภาพใบหน้าบุคคล เมื่อเลือกภาพใดให้พิมพ์ตัวอักษรที่อยู่ข้างใต้ของภาพนั้นให้ถูกต้องเพื่อนำไปใช้เป็นรหัสผ่าน

ภาพที่ 3.5 ตัวอย่างรูปแบบการทดลองของกลุ่มที่ 4 รอบที่ 1



ภาพที่ 3.6 ตัวอย่างรูปแบบการทดลองของกลุ่มที่ 4 รอบที่ 2

กลุ่มการทดลองที่ 4 จะใช้การนำเสนอรูปแบบของรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าบุคคลขนาดเล็ก จาก 4 ประเภท ได้แก่ ใบหน้าผู้ชาย ใบหน้าผู้หญิง ใบหน้าเด็ก และใบหน้าการ์ตูน โดยใช้รูปภาพใบหน้าบุคคลประเภทละ 9 รูปภาพ โดยจะแสดงรอบละ 2 ประเภท รวม 18 รูปภาพต่อรอบ ผู้ใช้จะต้องเลือกรูปภาพใบหน้าบุคคลรอบละ 4 รูปภาพ จำนวน 2 รอบ รวมจำนวนที่

ผู้เข้าร่วมการทดลองเลือก 8 รูปภาพจากทั้งหมด 36 รูปภาพ การปรากฏของรูปภาพแต่ละครั้งจะมีการสุ่มตัวอักษรภาษาอังกฤษช่องละ 2 ตัวอักษร ซึ่งตัวอักษรนี้จะถูกสุ่มขึ้นมาใหม่ทุกครั้งที่มีการปรากฏของรูปภาพใบหน้าบุคคล เมื่อเลือกภาพใดให้พิมพ์ตัวอักษรที่อยู่ข้างใต้ของภาพนั้นให้ถูกต้องเพื่อนำไปใช้เป็นรหัสผ่าน

ผู้เข้าร่วมการทดลองแต่ละคน จะได้รับมอบหมายให้ทำการทดลองคนละ 1 การทดลอง โดยใช้รูปแบบการศึกษาแบบสุ่มตัวอย่าง จากกลุ่มพนักงานการประปาส่วนภูมิภาค ที่มีช่วงอายุระหว่าง 25 – 50 โดยทำการเก็บรวบรวมจากกลุ่มตัวอย่างเพียงครั้งเดียว ใช้โปรแกรม และแบบสอบถามเป็นเครื่องมือหลักในการเก็บรวบรวมข้อมูล

3.1.3 กลุ่มตัวอย่างที่ใช้ในการวิจัย

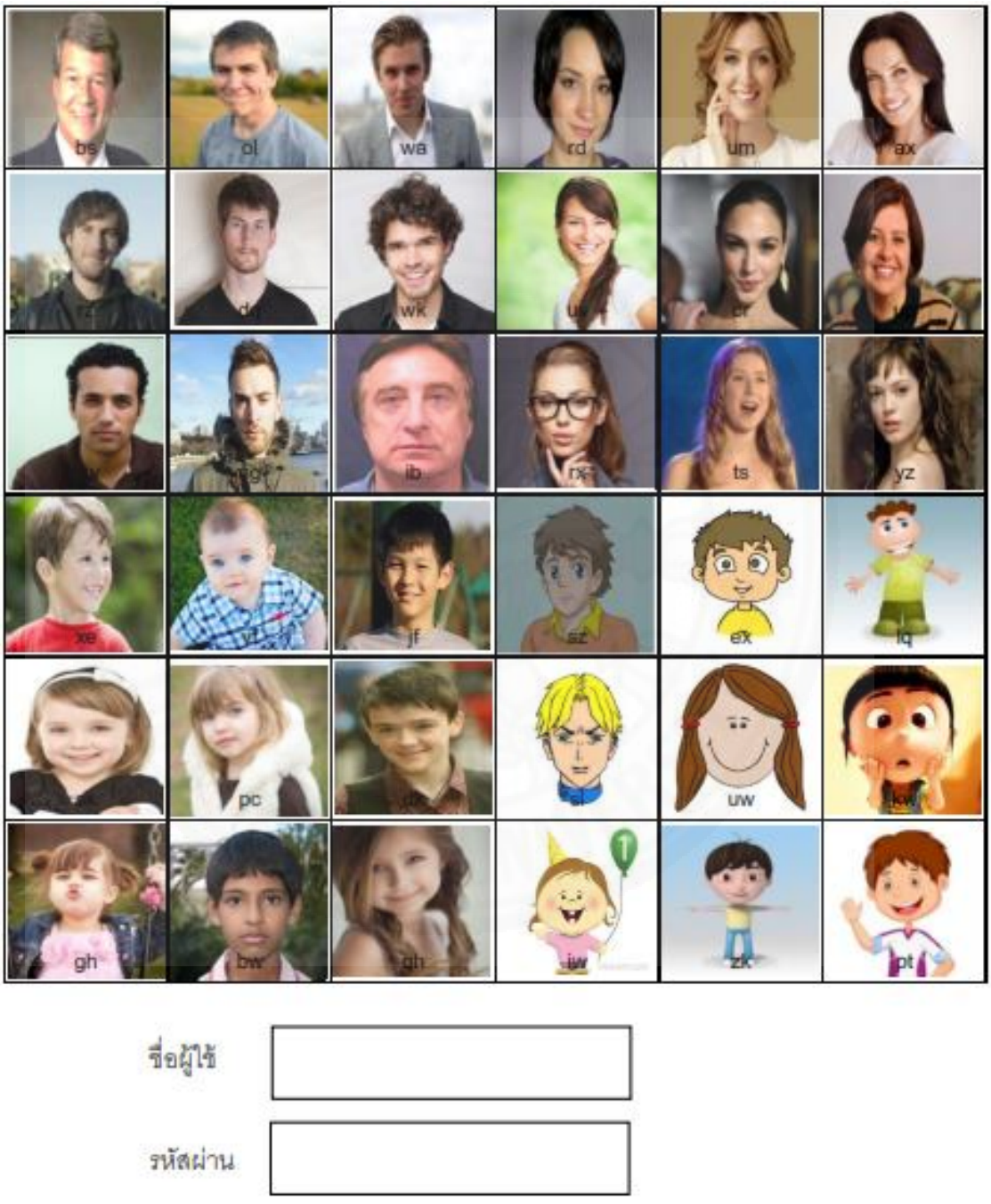
Lazar, Feng, and Hochheiser (2010) ได้อธิบายไว้ในหนังสือ Research Methods in Human Computer Interaction ว่า เพื่อที่จะให้ผลการทดลองมีความแม่นยำควรมีจำนวนกลุ่มตัวอย่าง 20 คนต่อกลุ่มการทดลอง เนื่องจากการทดลองต้องมีการเก็บข้อมูลถึง 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนทันที ครั้งที่ 2 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนไปล้ว 7 วัน และครั้งที่ 3 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนไปล้ว 15 วัน ผู้วิจัยได้ทำการสุ่มกลุ่มตัวอย่างจากพนักงานการประปาส่วนภูมิภาคเขต 2 ทั้งเพศชายและเพศหญิง จำนวนทั้งหมด 80 คน ซึ่งมีพื้นฐานการใช้งานคอมพิวเตอร์ในระดับใกล้เคียงกัน และเคยผ่านการใช้งานระบบการพิสูจน์ตัวตนมาแล้ว ผู้เข้าร่วมการทดลองแต่ละคนจะได้รับมอบหมายให้เข้ารับการทดสอบด้านการใช้งาน คนละ 1 รูปแบบการพิสูจน์ตัวตน และผู้เข้าร่วมการทดลองก็จะได้รับมอบหมายให้เข้ารับการทดสอบด้านความปลอดภัยคนละ 1 รูปแบบการพิสูจน์ตัวตน

3.1.4 เครื่องมือที่ใช้ในการทดลอง

การศึกษาเบื้องต้นจากบทที่ผ่านมา แสดงให้เห็นว่าการจำลองสถานการณ์การใช้งานระบบจริง ทำให้ผู้ใช้มีความตระหนักและระมัดระวังในการสร้างรหัสผ่านมากขึ้น การพัฒนาระบบสารสนเทศขึ้นมาเพื่อใช้ประกอบการทดลองจึงถูกสร้างขึ้น ผู้วิจัยได้พัฒนาระบบประวัติการรับชำระค่าน้ำประปา โดยกำหนดให้ผู้เข้าร่วมทดลองที่อยู่ตามการประปาส่วนภูมิภาคสาขาต่างๆ ได้ส่งข้อมูลการรับชำระค่าน้ำประปาผ่านระบบที่ได้สร้างขึ้น

สำหรับรหัสผ่านที่ใช้ในการเข้าสู่ระบบ เพื่อให้สอดคล้องกับงานวิจัยจึงได้ออกแบบให้เป็นตารางกริด โดยมีรูปภาพของใบหน้าบุคคลอยู่ในแต่ละช่อง พร้อมทั้งมีตัวอักษรภาษาอังกฤษที่ถูก

สุ่มขึ้นมารูปภาพละ 2 ตัวอักษร ผู้เข้าร่วมการทดลองจะเลือกภาพใบหน้าบุคคลที่ต้องการที่ต้องการแล้วพิมพ์ตัวอักษรภาษาอังกฤษที่ถูกสุ่มขึ้นมาให้ในแต่ละช่อง ในส่วนของชื่อผู้ใช้ กำหนดให้เป็นรหัสพนักงานของการประปาส่วนภูมิภาคสาขาต่างๆ ตัวอย่างของหน้าจอรหัสผ่าน แสดงดังภาพที่ 3.7



ภาพที่ 3.7 ตัวอย่างหน้าจอรหัสผ่าน

3.1.5 การเก็บรวบรวมข้อมูล

งานวิจัยนี้ ได้ทำการเก็บรวบรวมข้อมูลจากผู้เข้าร่วมการทดลอง โดยมีขั้นตอนดังนี้

ส่วนที่ 1 การลงทะเบียน เริ่มจากการให้ผู้เข้าร่วมการทดลองเข้าไปยังระบบสารสนเทศที่ได้จัดเตรียมไว้ หลังจากนั้นเป็นการลงทะเบียนเข้าใช้งานเพื่อเก็บข้อมูลเบื้องต้นของกลุ่มตัวอย่างก่อนเริ่มทำการทดลอง และกำหนดกลุ่มทดลองให้แก่ผู้เข้าร่วมการทดลองแต่ละคน

ส่วนที่ 2 การสร้างรหัสผ่าน จะทำการเก็บข้อมูล รหัสผ่าน วันที่และเวลาที่ใช้ในการสร้างรหัสผ่านรูปภาพ และผลสำเร็จของการสร้างรหัสผ่านรูปภาพ

ส่วนที่ 3 การพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ จะเก็บข้อมูลวันที่และจำนวนครั้งที่ใช้ในการพยายามระลึกรหัสผ่านรูปภาพของตนเอง เพื่อนำไปคำนวณเป็นคะแนนความสำเร็จในการพิสูจน์ตัวตนด้วยรหัสผ่าน

โดยทดลองทีละกลุ่มการทดลอง และให้กลุ่มที่ยังไม่ได้ทดลอง 1 คน มายืนสังเกตการณ์เพื่อเตรียมตัวทำการทดลองความปลอดภัยของรหัสผ่าน สำหรับการทดลองด้านประสิทธิภาพการใช้งานง่ายจะทำการทดลองทั้งหมด 3 ครั้ง คือ หลังจากการสร้างรหัสผ่านรูปภาพทันที หลังจากการสร้างรหัสผ่านรูปภาพ 7 วัน และหลังจากการสร้างรหัสผ่านรูปภาพ 15 วัน เพื่อจะวัดความสามารถในการจำได้ของผู้เข้าร่วมการทดลอง ส่วนการวัดประสิทธิภาพความปลอดภัย จะทำการทดลองเพียงครั้งเดียว คือ หลังจากผู้เข้าร่วมการทดลองเข้าสู่ระบบสำเร็จครั้งแรกทันที และการเก็บข้อมูลด้านความพึงพอใจที่ผู้ใช้มีต่อการใช้งานระบบรหัสผ่านรูปภาพจะถูกประเมินโดยใช้แบบสอบถามหลังจากที่ผู้เข้าร่วมการทดลองได้ทำการทดลองเรียบร้อยแล้ว

3.2 โครงสร้างและขั้นตอนการทำงานของระบบ

รูปแบบระบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ใช้ในงานวิจัยนี้ ได้นำรูปภาพใบหน้าบุคคลมาใช้ร่วมกับขั้นตอนการสร้างรหัสผ่านรูปภาพ โดยได้ออกแบบตารางกริดให้มีรูปภาพของใบหน้าบุคคลอยู่ในแต่ละช่อง พร้อมทั้งเปลี่ยนจากการใช้เมาส์คลิกที่รูปภาพของใบหน้าบุคคลมาเป็นการพิมพ์ตัวอักษรภาษาอังกฤษที่กำกับอยู่ในแต่ละช่อง เพื่อเป็นการป้องกันการขโมยรหัสผ่านโดยตัวอักษรที่กำกับแต่ละช่องนั้น เป็นการสุ่มตัวอักษรขึ้นมา เพื่อไม่ให้มีความหมาย

3.2.1 ขั้นตอนการทำงานของระบบ

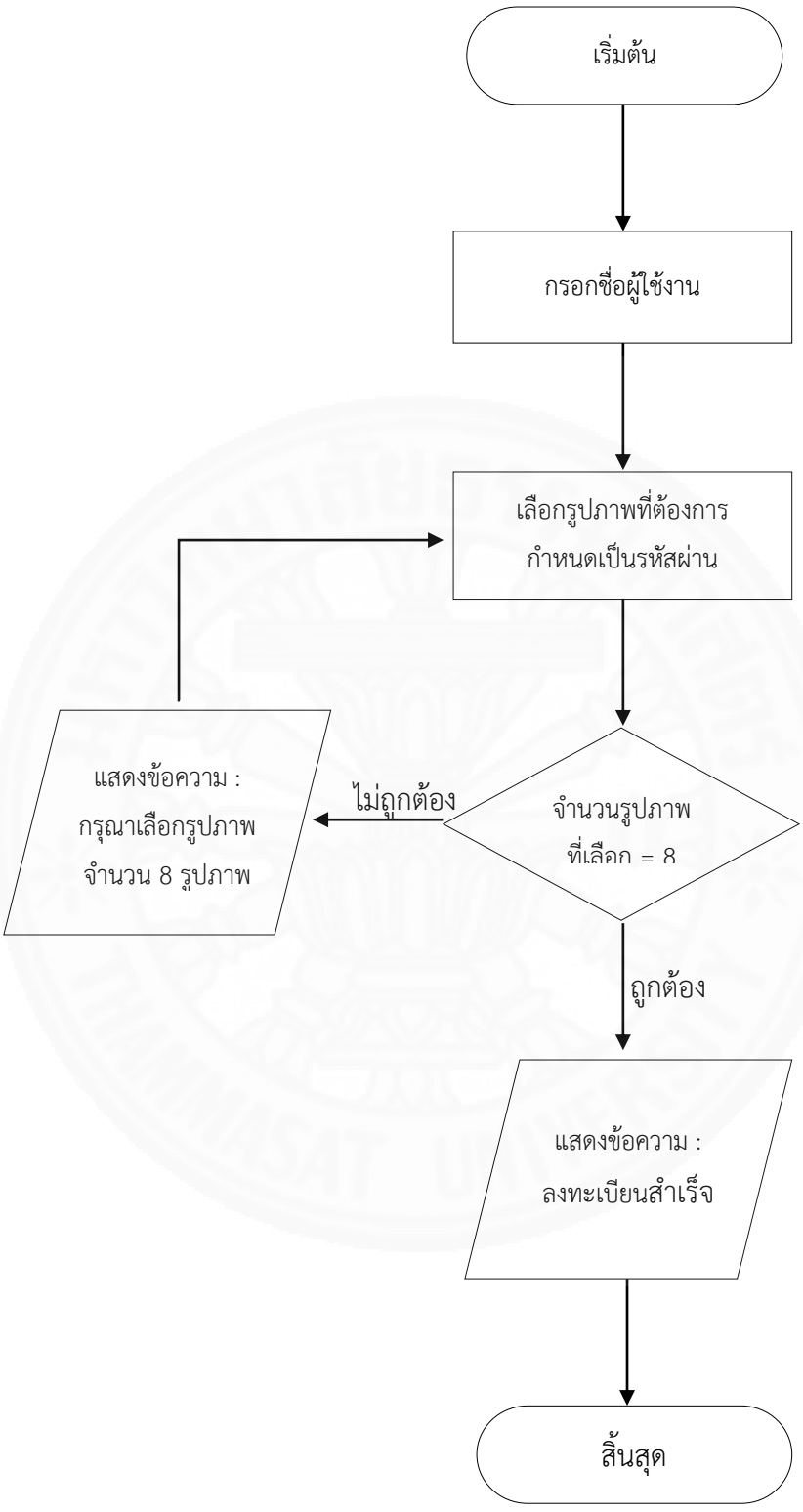
ในส่วนนี้จะอธิบายถึงวิธีการใช้งานระบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ใช้ในงานวิจัยนี้ มี 2 ขั้นตอนหลัก คือ การลงทะเบียน และการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพเพื่อเข้าสู่ระบบ

3.2.1.1 ขั้นตอนการลงทะเบียน (Register)

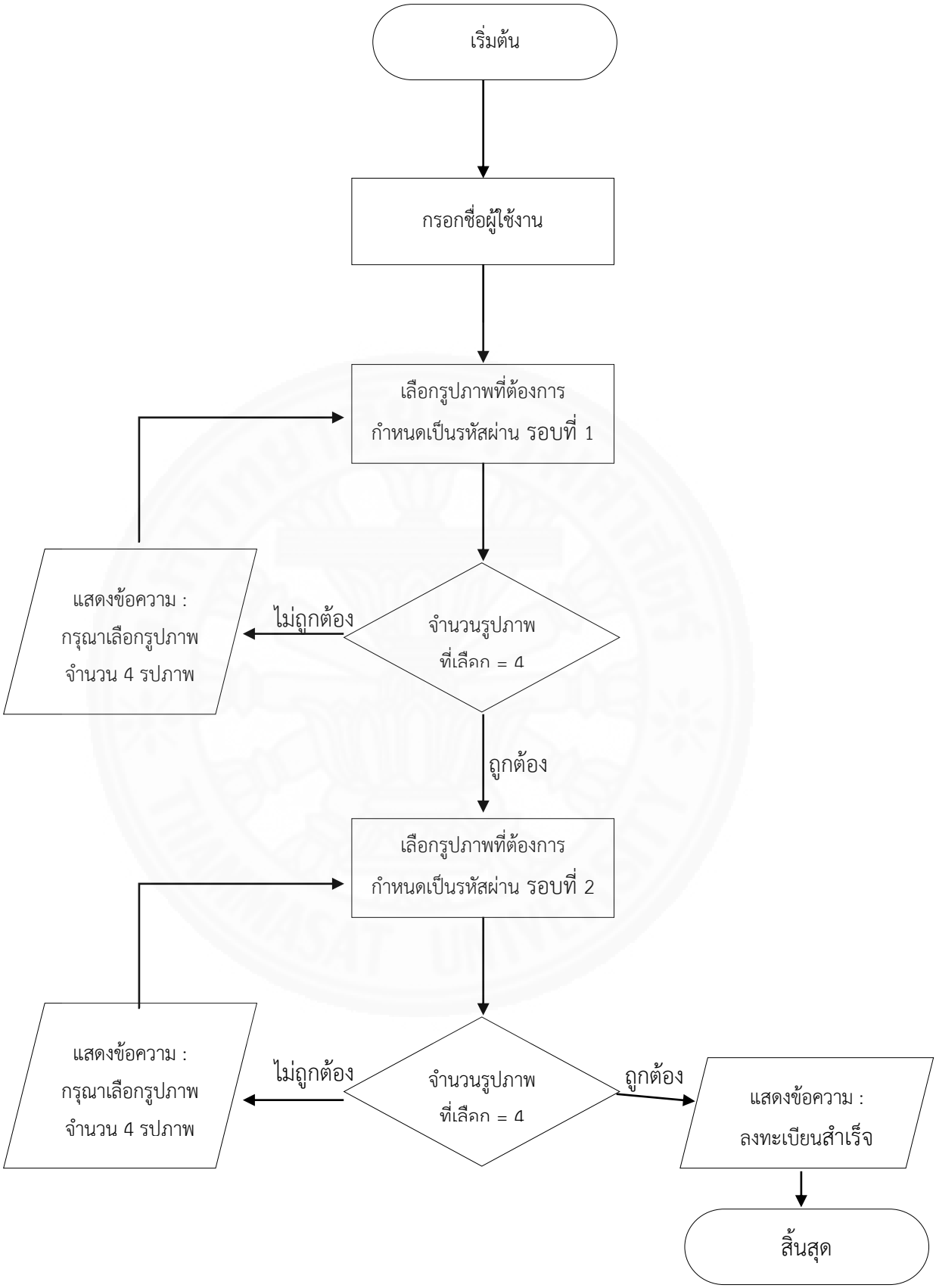
เมื่อผู้เข้าร่วมการทดลองอยู่ในหน้าหลักของระบบ ให้ผู้เข้าร่วมการทดลองทำการคลิกที่ปุ่มลงทะเบียน ระบบจะให้ผู้เข้าร่วมการทดลองตั้งชื่อผู้ใช้งานเป็นรหัสพนักงานของการประปาส่วนภูมิภาค หลังจากนั้นจะเข้าสู่ขั้นตอนการสร้างรหัสผ่านรูปภาพด้วยการพิมพ์ตัวอักขระที่กำกับไว้ในแต่ละช่อง จำนวน 8 ช่อง เมื่อสร้างรหัสผ่านได้ตามต้องการแล้วให้คลิกที่ปุ่มยืนยันการลงทะเบียน ระบบจะบันทึก ชื่อผู้ใช้งาน และรหัสผ่านนั้นไว้

ขั้นตอนการลงทะเบียนจะมีวิธีการแตกต่างกันตามโปรแกรที่ได้ออกแบบไว้ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยแบ้งเป็น 2 โปรแกรม คือ โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ โดยมีขั้นตอนการทำงาน ดังนี้

1. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ เริ่มจากให้ผู้เข้าร่วมการทดลองกรอกรหัสพนักงานเพื่อใช้เป็นชื่อผู้ใช้งาน หลังจากนั้นให้ผู้เข้าร่วมการทดลองพิมพ์ตัวอักษรภาษาอังกฤษที่อยู่ใต้รูปภาพที่ต้องการเลือกเป็นรหัสผ่าน ทั้งหมด 8 รูปภาพ โดยสามารถเลือกรูปภาพใดจากประเภทใดก็ได้ ทั้งกลุ่มการทดลองที่มีการนำเสนอรูปภาพด้วยใบหน้าบุคคลขนาดใหญ่แบ่งส่วนและกลุ่มการทดลองที่มีการนำเสนดรูปภาพด้วยใบหน้าบุคคลขนาดเล็ก เมื่อเลือกรูปภาพเสร็จเรียบร้อยแล้วให้ทำการคลิกปุ่มยืนยันการลงทะเบียน เป็นอันเสร็จขั้นตอนการลงทะเบียน



ภาพที่ 3.8 ผังขั้นตอนการลงทะเบียนของกลุ่มการทดลองที่ใช้รอบจำนวนรอบในการสร้างรหัสผ่าน 1 รอบ ร่วมกับการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่แบ่งส่วนหรือรูปภาพเล็ก



ภาพที่ 3.9 ผังขั้นตอนการลงทะเบียนของกลุ่มการทดลองที่ใช้รอบจำนวนรอบในการสร้างรหัสผ่าน 2 รอบ ร่วมกับการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่แบ่งส่วนหรือรูปภาพเล็ก

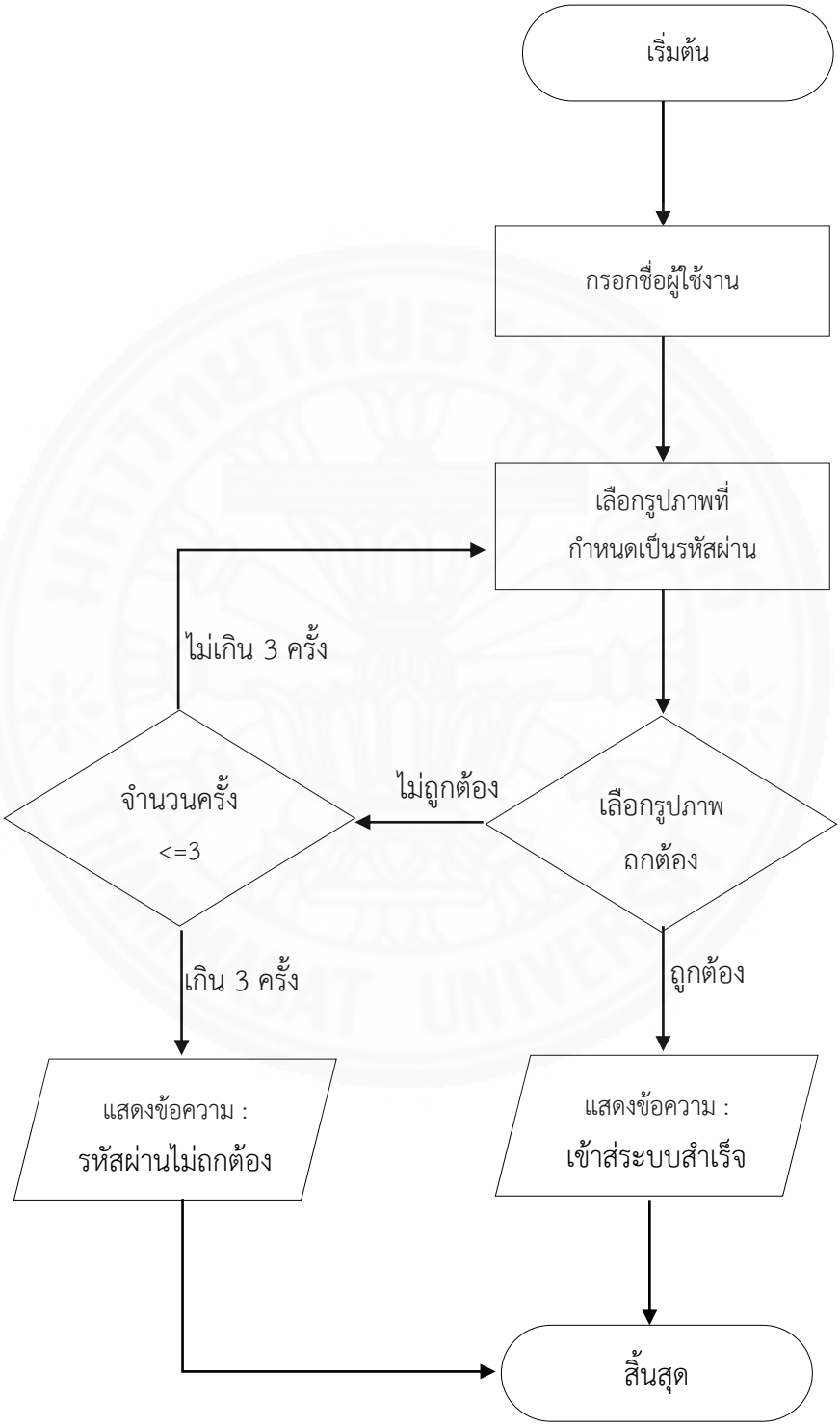
2. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ เริ่มจากให้ผู้เข้าร่วมการทดลองกรอกรหัสพนักงานเพื่อใช้เป็นชื่อผู้ใช้งาน หลังจากนั้นให้ผู้เข้าร่วมการทดลองพิมพ์ตัวอักษรภาษาอังกฤษที่อยู่ใต้รูปภาพที่ต้องการเลือกเป็นรหัสผ่าน ซึ่งแบ่งการตั้งรหัสผ่านออกเป็น 2 รอบ รอบละ 4 รูปภาพ โดยในแต่ละรอบจะมีประเภทของรูปภาพให้เลือกรอบละ 2 ประเภท เมื่อสร้างรหัสผ่านรอบแรกเรียบร้อยแล้วให้คลิกที่ปุ่มสร้างรหัสผ่านส่วนถัดไป แล้วให้เลือกรหัสผ่านอีก 4 รูปภาพ จนครบทั้งหมด 8 รูปภาพ โดยสามารถเลือกรูปภาพใดจากประเภทใดก็ได้ ทั้งกลุ่มการทดลองที่มีการนำเสนอรูปภาพด้วยใบหน้าบุคคลขนาดใหญ่แบ่งส่วนและกลุ่มการทดลองที่มีการนำเสนดรูปภาพด้วยใบหน้าบุคคลขนาดเล็ก เมื่อเลือกรูปภาพในรอบที่ 2 เสร็จเรียบร้อยแล้วให้ทำการคลิกปุ่มยืนยันการลงทะเบียน เป็นอันเสร็จขั้นตอนการลงทะเบียน

3.2.1.2 ขั้นตอนการเข้าสู่ระบบ (Login)

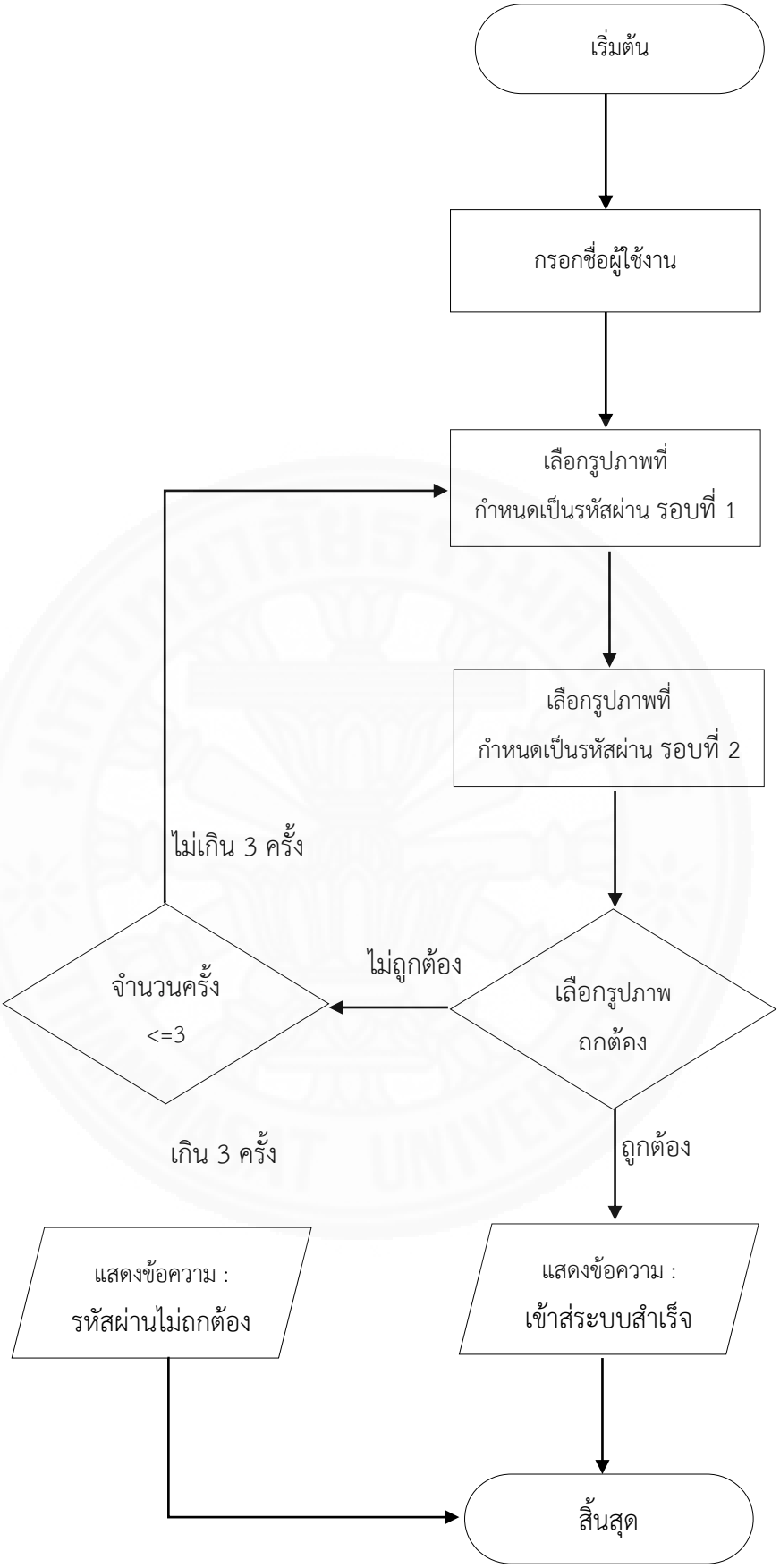
เมื่อผู้เข้าร่วมการทดลองอยู่ในหน้าหลัก ให้ผู้เข้าร่วมการทดลองคลิกที่ปุ่มเข้าสู่ระบบ เมื่อเข้าสู้หน้าเข้าสู่ระบบให้ผู้เข้าร่วมการทดลองใส่ชื่อผู้ใช้งาน ระบบจะแสดงรูปภาพประกอบตามกลุ่มการทดลอง จากนั้นให้ผู้เข้าร่วมการทดลองเลือกรูปภาพที่ใช้เป็นรหัสผ่านในขั้นตอนการลงทะเบียนที่ผ่านมา แล้วพิมพ์ตัวอักขระที่ปรากฏไว้ในแต่ละช่อง ให้ตรงกับรูปภาพที่เป็นรหัสผ่าน เมื่อเรียบร้อยแล้วให้คลิกที่ปุ่มเข้าสู่ระบบ หากใส่ชื่อผู้ใช้งานและรหัสผ่านได้ถูกต้องก็จะผ่านการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ แต่ถ้าใส่ชื่อผู้ใช้งานและรหัสผ่านไม่ถูกต้อง ระบบจะอนุญาตให้ใส่ชื่อผู้ใช้และรหัสผ่านได้ไม่เกิน 3 ครั้ง โดยที่ตัวอักษรจะถูกสุ่มขึ้นใหม่ทุกครั้ง โดยจะแบ่งโปรแกรมที่ได้ออกแบบตามปัจจัยจำนวนรอบในการสร้างรหัสผ่านรูปภาพ แบ่งเป็น 2 โปรแกรม คือ โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ โดยมีขั้นตอนการทำงาน ดังนี้

1. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ เริ่มจากการใช้ผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งานซึ่งเป็นรหัสพนักงานของผู้เข้าร่วมการทดลอง แล้วให้ทำการพิสูจน์ตัวตนโดยการพิมพ์ตัวอักษรภาษาอังกฤษที่อยู่ใต้รูปภาพที่ได้เลือกไว้เป็นรหัสผ่านในขั้นตอนการลงทะเบียน ทั้งหมด 8 รูปภาพ เมื่อใส่รหัสผ่านเสร็จเรียบร้อยแล้วให้คลิกที่ปุ่มเข้าสู่ระบบ ถ้าผู้เข้าร่วมการทดลองเลือกรูปภาพได้อย่างถูกต้องตามที่ได้สร้างไว้ในขั้นตอนการลงทะเบียน ก็จะสามารถเข้าสู่ระบบได้สำเร็จ หากไม่สามารถพิสูจน์ตัวตนได้สำเร็จในครั้งแรก ระบบจะอนุญาตให้ผู้เข้าร่วมการทดลองสามารถพิสูจน์ตัวตนได้อีก 2 ครั้ง รวมจำนวนครั้งที่ผู้เข้าร่วมการทดลองสามารถพิสูจน์ตัวตนได้ไม่เกิน 3 ครั้ง ถ้าผู้เข้าร่วมการทดลองสามารถพิสูจน์ตัวตนได้สำเร็จไม่เกิน 3 ครั้ง ก็จะสามารถเข้าสู่

ระบบได้ หากผู้เข้าร่วมการทดลองไม่สามารถพิสูจน์ตัวตนได้สำเร็จภายใน 3 ครั้ง จะไม่สามารถเข้าสู่ระบบได้ และถือว่าสิ้นสุดการทดลอง



ภาพที่ 3.10 ผังงานขั้นตอนการพิสูจน์ตัวตนเพื่อเข้าสู่ระบบของกลุ่มการทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ



ภาพที่ 3.11 ผังงานขั้นตอนการพิสูจน์ตัวตนเพื่อเข้าสู่ระบบของกลุ่มการทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

2. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ เริ่มจากการใช้ผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งานซึ่งเป็นรหัสพนักงานของผู้เข้าร่วมการทดลอง แล้วให้ทำการพิสูจน์ตัวตนโดยการพิมพ์ตัวอักษรภาษาอังกฤษที่อยู่ใต้รูปภาพที่ได้เลือกไว้เป็นรหัสผ่านในขั้นตอนการลงทะเบียน โดยให้เลือกรหัสผ่านรูปภาพ 2 รอบ รอบละ 4 รูปภาพ เมื่อเลือกรหัสผ่านรูปภาพในรอบแรกแล้วให้คลิกที่ปุ่มถัดไป เพื่อเลือกรหัสภาพรูปภาพอีก 4 รูปภาพ ในรอบที่ 2 รวมทั้งหมด 8 รูปภาพ เมื่อใส่รหัสผ่านเสร็จเรียบร้อยแล้วให้คลิกที่ปุ่มเข้าสู่ระบบ ถ้าผู้เข้าร่วมการทดลองเลือกรูปภาพได้อย่างถูกต้องตามที่ได้สร้างไว้ในขั้นตอนการลงทะเบียน ก็จะสามารถเข้าสู่ระบบได้สำเร็จ หากไม่สามารถพิสูจน์ตัวตนได้สำเร็จในครั้งแรก ระบบจะอนุญาตให้ผู้เข้าร่วมการทดลองสามารถพิสูจน์ตัวตนได้อีก 2 ครั้ง รวมจำนวนครั้งที่ผู้เข้าร่วมการทดลองสามารถพิสูจน์ตัวตนได้ไม่เกิน 3 ครั้ง ถ้าผู้เข้าร่วมการทดลองสามารถพิสูจน์ตัวตนได้สำเร็จไม่เกิน 3 ครั้ง ก็จะสามารถเข้าสู่ระบบได้ หากผู้เข้าร่วมการทดลองไม่สามารถพิสูจน์ตัวตนได้สำเร็จภายใน 3 ครั้ง จะไม่สามารถเข้าสู่ระบบได้ และถือว่าสิ้นสุดการทดลอง

3.3 การออกแบบการทดลองและการวัดผล

การออกแบบการทดลองและการวัดผล จะอธิบายถึง รายละเอียดของการออกแบบการทดลองด้านการใช้งาน (Usability) ด้านความปลอดภัย (security) และการออกแบบแบบสอบถามความพึงพอใจที่มีต่อระบบ โดยมีรายละเอียด ดังนี้

3.3.1 การออกแบบการทดลอง

กำหนดให้ผู้เข้าร่วมการทดลองทั้งหมดแบ่งออกเป็น 4 กลุ่มการทดลองแบบสุ่ม เพื่อทำการทดลองด้านการใช้งาน กลุ่มละ 1 รูปแบบ และจับคู่กันแบบสุ่มเพื่อทำการทดลองทางด้านความปลอดภัยอีกคนละ 1 รูปแบบ โดยที่รูปแบบที่กำหนดมีดังนี้

3.3.1.1 การทดลองด้านการใช้งาน (Usability)

การทดลองด้านการใช้งานเริ่มจากผู้วิจัยอธิบายวัตถุประสงค์และรายละเอียดการทดลองให้ผู้เข้าร่วมการทดลองทราบ แล้วจึงเริ่มทำการทดลอง โดยจะทำการทดลองทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 ทำการทดลองการพิสูจน์ตัวตนหลังจากลงทะเบียนทันที ครั้งที่ 2 ทำการทดลองการพิสูจน์ตัวตนหลังจากลงทะเบียน 7 วัน และครั้งที่ 3 ทำการทดลองการพิสูจน์ตัวตนหลังจากลงทะเบียน 15 วัน รายละเอียดดังนี้

การทดลองครั้งที่ 1 ทำการทดลองการพิสูจน์ตัวตนหลังจากลงทะเบียนทันที โดยเริ่มจากการให้ผู้เข้าร่วมการทดลองตอบแบบสอบถามข้อมูลทั่วไป และผู้วิจัยจะสาธิตการใช้งานโปรแกรมที่ได้ออกแบบ เมื่อผู้เข้าร่วมการทดลองเข้าใจวิธีการใช้งานโปรแกรมแล้ว ก็จะให้ทำการทดลองโดยเริ่มจากการลงทะเบียนเพื่อสร้างรหัสผ่านรูปภาพ เมื่อลงทะเบียนเสร็จเรียบร้อยแล้ว ให้ทำการพิสูจน์ตัวตนทันที เพื่อเข้าไปใช้ระบบระบบส่งข้อมูลการรับชำระค่าน้ำประปา ของการประปาส่วนภูมิภาคสาขาในสังกัดการประปาส่วนภูมิภาคเขต 2

การทดลองครั้งที่ 2 ทำการทดลองการพิสูจน์ตัวตนหลังจากลงทะเบียนไปแล้ว 7 วัน โดยให้ผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตน เพื่อเข้าไปใช้ระบบระบบส่งข้อมูลการรับชำระค่าน้ำประปา ของการประปาส่วนภูมิภาคสาขาในสังกัดการประปาส่วนภูมิภาคเขต 2

การทดลองครั้งที่ 3 ทำการทดลองการพิสูจน์ตัวตนหลังจากลงทะเบียนไปแล้ว 15 วัน โดยให้ผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตน เพื่อเข้าไปใช้ระบบระบบส่งข้อมูลการรับชำระค่าน้ำประปา ของการประปาส่วนภูมิภาคสาขาในสังกัดการประปาส่วนภูมิภาคเขต 2

ในการทดลองแต่ละครั้งจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนทั้งหมด 3 ครั้ง หากไม่สามารถพิสูจน์ตัวตนได้สำเร็จภายใน 3 ครั้ง ถือว่าสิ้นสุดการทดลอง

3.3.1.2 การทดลองด้านความปลอดภัย (Security)

การทดลองด้านความปลอดภัย ให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนด้วยการใช้วิธีการแอบมอง (Shoulder Surfing) โดยพยายามแอบมองในขณะที่ผู้เข้าร่วมการทดลองด้านการใช้งานกำลังทำการพิสูจน์ตัวตน เมื่อผู้เข้าร่วมการทดลองด้านการใช้งานพิสูจน์ตัวตนเสร็จสิ้น จะให้ผู้ที่รับหน้าที่โจรกรรมทำการพิสูจน์ตัวตน โดยนำรหัสผ่านที่โจรกรรมได้มาทำการพิสูจน์ตัวตน โดยให้โอกาสในการพิสูจน์ตัวตน 3 ครั้ง หากไม่สามารถพิสูจน์ตัวตนได้สำเร็จภายใน 3 ครั้ง ถือว่าสิ้นสุดการทดลอง

3.3.2 การออกแบบสอบถาม

แบบสอบถามความพึงพอใจ ซึ่งเป็นทั้งคำถามในรูปแบบปลายปิดและปลายเปิดเป็นเครื่องมือในการเก็บรวบรวมข้อมูลด้านความพึงพอใจที่ผู้ใช้มีต่อระบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ใช้ในงานวิจัยนี้ แบ่งออกเป็น 4 ส่วน ได้แก่

ส่วนที่ 1 คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง ได้แก่ เพศ อายุ ระดับการศึกษา และอาชีพ

ส่วนที่ 2 คำถามเกี่ยวกับพฤติกรรมการใช้การพิสูจน์ตัวตน เช่น เคยใช้ระบบการพิสูจน์ตัวตนหรือไม่

ส่วนที่ 3 ความพึงพอใจเกี่ยวกับระบบพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ใช้ในงานวิจัยนี้

ส่วนที่ 4 ข้อคิดเห็นเพิ่มเติมเกี่ยวกับระบบพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ใช้ในงานวิจัยนี้

เนื่องจากการตอบแบบสอบถามในส่วนที่ 3 เป็นการวัดแล้วให้คำตอบตามความรู้สึก จะไม่สามารถวัดหามาตรฐานของพฤติกรรมที่ต้องการวัดได้ งานวิจัยนี้ได้ใช้ตัวเลขมากำหนดให้ค่าของพฤติกรรมแปลงเป็น เรตติ้งสเกล (Rating scale) 5 สเกล โดยกำหนดเป็นค่าคะแนนจากน้อยไปหามากตามการเกิดพฤติกรรม 1-5 ซึ่งเป็นคะแนนมาตรฐานที่ใช้วัดในงานวิจัยและง่ายต่อการตีความ โดยแบ่งคะแนนระดับความพึงพอใจเป็น 5 ระดับ คือ

- พอใจอย่างยิ่ง ให้ค่าคะแนนเท่ากับ 5 คะแนน
- พอใจ ให้ค่าคะแนนเท่ากับ 4 คะแนน
- ไม่แน่ใจ ให้ค่าคะแนนเท่ากับ 3 คะแนน
- ไม่พอใจ ให้ค่าคะแนนเท่ากับ 2 คะแนน
- ไม่พอใจอย่างยิ่ง ให้ค่าคะแนนเท่ากับ 1 คะแนน

ทั้งนี้เพื่อนำไปปรับปรุงประสิทธิภาพของการทำงานระบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ

3.3.3 หลักสถิติที่ใช้ในการวิเคราะห์ข้อมูล

งานวิจัยนี้จะนำผลที่ได้จากการทดลองและแบบสอบถามไปประมวลผล เพื่อวิเคราะห์และสรุปผลการทดลอง อาศัยการใช้โปรแกรมสำเร็จรูปทางสถิติ SPSS และหลักสถิติในการวิเคราะห์ข้อมูล เพื่อให้การประเมินผลที่ได้มีความถูกต้องและน่าเชื่อถือ สามารถนำผลการวิเคราะห์ข้อมูลที่ได้ไปสรุปผลการทดลอง

ในการวิเคราะห์ข้อมูลของงานวิจัยนี้ ใช้การคำนวณวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ที่ระดับความเชื่อมั่น 95% เพื่อวิเคราะห์และตอบสมมติฐานของงานวิจัย

บทที่ 4

ผลการทดลอง

งานวิจัยนี้ได้ศึกษาเกี่ยวกับรหัสผ่านรูปภาพแบบกริดที่มีการนำรูปภาพใบหน้าบุคคลมาใช้เป็นรหัสผ่านโดยจะมีตัวอักษรภาษาอังกฤษกำกับไว้แต่ละรูปภาพเพื่อเพิ่มความยากในการโจรกรรมรหัสผ่าน หลังจากทดลองแล้วจึงได้ทำการวิเคราะห์ผลการทดลองของการมีรูปภาพใบหน้าบุคคลในการสร้างรหัสผ่านที่มีผลต่อการจำรหัสผ่านของผู้เข้าร่วมการทดลอง และความสำเร็จในการเข้าสู่ระบบ ในการวิเคราะห์ข้อมูลของงานวิจัยนี้ ใช้การคำนวณวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ที่ระดับความเชื่อมั่น 95% เพื่อวิเคราะห์และตอบสมมติฐานของงานวิจัย เนื่องมีตัวแปรต้นที่ถูกนำมาใช้ในงานวิจัย 2 ตัวแปร ประกอบด้วย จำนวนรอบที่ใช้ในการสร้างรหัสผ่านและการพิสูจน์ตัวตน มี 2 ระดับ คือ 1 รอบ และ 2 รอบ และอีกตัวแปร คือ ลักษณะการนำเสนอรูปภาพใบหน้าบุคคลสำหรับรหัสผ่าน มี 2 ระดับ คือ รูปภาพใหญ่ตัดเป็นส่วนๆ และ รูปภาพย่อยในแต่ละกริด

4.1 ผลการวิเคราะห์ข้อมูลส่วนตัวของผู้เข้าร่วมการทดลอง

หลังจากการดำเนินการทดลองที่ได้นำเสนอไว้ในระเบียบวิธีวิจัยข้างต้นแล้ว มีผู้เข้าร่วมการทดลองทั้งหมดเป็นพนักงานการประปาส่วนภูมิภาคจำนวน 80 คน จำแนกเป็นเพศชาย 36 คน และเพศหญิง 44 คน โดยที่ผู้เข้าร่วมการทดลองทั้งหมดมีประสบการณ์การใช้คอมพิวเตอร์อย่างน้อย 1 ปี

ตารางที่ 4.1

จำนวนร้อยละของผู้เข้าร่วมการทดลอง จำแนกตามเพศ

เพศ	จำนวนคน	ร้อยละ
ชาย	36	45.00
หญิง	44	55.00
รวม	80	100.00

4.2 ผลการวิเคราะห์ผลการทดลองทางด้านประสิทธิภาพการใช้งาน (Usability)

ปัจจัยที่นำมาใช้ในการศึกษามี 2 ปัจจัย คือ จำนวนรอบที่ใช้ในการสร้างรหัสผ่านและการพิสูจน์ตัวตน มี 2 ระดับ คือ 1 รอบ และ 2 รอบ และอีกปัจจัย คือ ลักษณะการใช้รูปภาพสำหรับรหัสผ่าน มี 2 ระดับ คือ รูปภาพใหญ่ตัดเป็นส่วนๆ และ รูปภาพย่อยในแต่ละกริด

4.2.1 ผลการทดลองการเข้าสู่ระบบด้วยรหัสผ่านรูปภาพหลังจากลงทะเบียนทันที

ผลการทดลองที่ถูกเก็บในการศึกษาครั้งนี้ประกอบไปด้วย จำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ และความสำเร็จในการเข้าสู่ระบบ โดยใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ที่ระดับความเชื่อมั่น 95% ในการวิเคราะห์ความแตกต่างของผลการทดลอง

4.2.1.1 จำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ

การวิเคราะห์ผลการทดลองเกี่ยวกับจำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ ผู้เข้าร่วมการทดลองสามารถล็อคอินเข้าสู่ระบบได้ไม่เกิน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองในรูปแบบของคะแนนการล็อคอินเข้าสู่ระบบ โดยที่มีเกณฑ์ในการบันทึกคะแนนจากการทดลอง ดังนี้

ตารางที่ 4.2

การบันทึกคะแนนการล็อคอินเข้าสู่ระบบ

คะแนน	คำอธิบาย
3	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งแรก
2	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งที่ 2
1	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งที่ 3
0	ไม่สามารถล็อคอินเข้าสู่ระบบ

ผู้เข้าร่วมการทดลองจะถูกบันทึกคะแนนการล็อคอินเข้าสู่ระบบตามตารางที่ 4.2 เมื่อนำมาวิเคราะห์ผลการทดลองจะได้ ดังนี้

ตารางที่ 4.3

คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

กลุ่มการทดลอง	จำนวนคน				
	ล็อคอินเข้าสู่ระบบได้ในครั้งแรก	ล็อคอินเข้าสู่ระบบได้ในครั้งที่ 2	ล็อคอินเข้าสู่ระบบได้ในครั้งที่ 3	ไม่สามารถล็อคอินเข้าสู่ระบบ	รวม
1	17	2	1	0	20
2	17	1	2	0	20
3	16	2	2	0	20
4	16	4	0	0	20
รวม	66	9	5	0	80

ผลการทดลองการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันทีปรากฏว่า ผู้เข้าร่วมการทดลองในแต่ละกลุ่มการทดลองสามารถล็อคอินเข้าสู่ระบบได้ทุกคน ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งแรกมีจำนวน 66 คน ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งที่ 2 มีจำนวน 9 คน และผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งที่ 3 มีจำนวนเพียง 5 คน จากผู้เข้าร่วมการทดลองทั้งหมด 80 คน โดยที่ผู้เข้าร่วมการทดลองในกลุ่มที่ 1 และ 2 สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งแรกมากที่สุด มีจำนวนกลุ่มละ 17 คน

ตารางที่ 4.4

ค่าสถิติวิเคราะห์คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	2.80	0.523	20
	2 รอบ	2.75	0.639	20
	รวม	2.78	0.577	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	2.70	0.657	20
	2 รอบ	2.80	0.410	20
	รวม	2.75	0.543	40
รวม	1 รอบ	2.75	0.588	40
	2 รอบ	2.77	0.530	40
	รวม	2.76	0.557	80

จากผลการทดลอง ตารางที่ 4.4 แสดงให้เห็นว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบสูงที่สุดถึง 2.78 คะแนน แสดงว่าสามารถล็อคอินเข้าสู่ระบบด้วยจำนวนครั้งที่น้อยกว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลย่อยในแต่ละกริด ส่งผลให้ผู้เข้าร่วมการทดลองสามารถจำรหัสผ่านของตนเองได้

ตารางที่ 4.5

ค่า Levene Statistice สถิติวิเคราะห์คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

F	df1	df2	Sig.
0.720	3	76	0.543

* ที่ระดับนัยสำคัญ 0.05

การวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน (Levene's test) ชี้ให้เห็นว่าค่าความแปรปรวนของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที ผู้เข้าร่วมการทดลองแต่ละกลุ่มนั้นไม่แตกต่างกัน (P=0.543;P>0.05) ที่ระดับนัยสำคัญ P<0.05 จึงสามารถนำผลการทดลองนี้ไปใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ได้

ตารางที่ 4.6

ค่าสถิติเปรียบเทียบกลุ่มการทดลองที่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

ปัจจัยทดสอบ	Type III Sum of Squares	df	Mean Square	F	Sig.
ลักษณะรูปภาพใบหน้าบุคคล	0.013	1	0.013	0.039	0.844
จำนวนรอบ	0.013	1	0.013	0.039	0.844
ลักษณะรูปภาพใบหน้าบุคคล * จำนวนรอบ	0.113	1	0.113	0.351	0.555

* ที่ระดับนัยสำคัญ 0.05

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริดไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที (P=0.844;P>0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะไม่ทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

การทดสอบอิทธิพลของจำนวนรอบของรหัสผ่านที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที พบว่า ผู้เข้าร่วมการทดลองที่มีจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที (P=0.844;P>0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบจะไม่ทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่านที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริด และจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที ($P=0.555;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ ไม่มีอิทธิพลร่วมกันต่อคะแนนการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

ตารางที่ 4.7

ค่าประมาณการแบบช่วงของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันทีแยกตามลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่าน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	2.800	0.523
	2 รอบ	2.750	0.639
รูปภาพย่อยในแต่ละกริด	1 รอบ	2.700	0.657
	2 รอบ	2.800	0.410

เมื่อศึกษาค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันทีแยกตามตามลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่าน พบว่า กลุ่มการทดลองที่ใช้รูปภาพใหญ่แบ่งเป็นส่วนย่อยประกอบกับจำนวนรอบของรหัสผ่าน 1 รอบ และกลุ่มการทดลองที่ใช้รูปภาพย่อยในแต่ละกริดประกอบกับจำนวนรอบของรหัสผ่าน 2 รอบ จะมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบสูงสุด ในขณะที่กลุ่มการทดลองที่ใช้รูปภาพย่อยในแต่ละกริดประกอบกับจำนวนรอบของรหัสผ่าน 1 รอบ จะมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบต่ำกว่ากลุ่มการทดลองอื่นๆ

4.2.1.2 ความสำเร็จในการล็อคอินเข้าสู่ระบบ

การวิเคราะห์ผลการทดลองเกี่ยวกับความสำเร็จในการล็อคอินเข้าสู่ระบบ หากผู้เข้าร่วมการทดลองสามารถล็อคอินเข้าสู่ระบบได้ไม่เกิน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองว่าสามารถล็อคอินเข้าสู่ระบบสำเร็จ แต่ถ้าผู้เข้าร่วมการทดลองไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองครั้งนั้นว่าไม่สามารถล็อคอินเข้าสู่ระบบสำเร็จ

ตารางที่ 4.8

จำนวนผู้เข้าร่วมการทดลองในแต่ละปัจจัยการทดลอง

ปัจจัยหลัก	ปัจจัยย่อย	จำนวนคน
ลักษณะของรูปภาพใบหน้าบุคคล	รูปภาพใหญ่แบ่งเป็นส่วนย่อย	20
	รูปภาพย่อยในแต่ละกริด	20
จำนวนรอบในการสร้างและเข้าสู่ระบบ	1 รอบ	20
	2 รอบ	20

ตารางที่ 4.9

จำนวนผู้เข้าร่วมการทดลองในแต่ละกลุ่มการทดลอง

กลุ่มการทดลองที่	จำนวนคน
1	20
2	20
3	20
4	20

ตารางที่ 4.10

ค่าสถิติวิเคราะห์ความสำเร็จการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	1.00	0.000	20
	2 รอบ	1.00	0.000	20
	รวม	1.00	0.000	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	1.00	0.000	20
	2 รอบ	1.00	0.000	20
	รวม	1.00	0.000	40
รวม	1 รอบ	1.00	0.000	40
	2 รอบ	1.00	0.000	40
	รวม	1.00	0.000	80

ตารางที่ 4.11

ร้อยละของความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	จำนวน	ล้มเหลว (คน)	สำเร็จ (คน)	ล้มเหลว (%)	สำเร็จ (%)
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	20	0	20	0	100
	2 รอบ	20	0	20	0	100
รูปภาพย่อยในแต่ละกริด	1 รอบ	20	0	20	0	100
	2 รอบ	20	0	20	0	100
รวม		80	0	80	0	100

ผลการวิเคราะห์สถิติความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที พบว่า ผู้เข้าร่วมการทดลองทุกคนสามารถล็อคอินเข้าสู่ระบบได้

4.2.2 ผลการทดลองการเข้าสู่ระบบด้วยรหัสผ่านรูปภาพหลังจากลงทะเบียน 7 วัน

ผลการทดลองที่ถูกเก็บในการศึกษาครั้งนี้ประกอบไปด้วย จำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ และความสำเร็จในการเข้าสู่ระบบ โดยใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ที่ระดับความเชื่อมั่น 95% ในการวิเคราะห์ความแตกต่างของผลการทดลอง

4.2.2.1 จำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ

การวิเคราะห์ผลการทดลองเกี่ยวกับจำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ ผู้เข้าร่วมการทดลองสามารถล็อคอินเข้าสู่ระบบได้ไม่เกิน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองในรูปแบบของคะแนนการล็อคอินเข้าสู่ระบบ ระบบ โดยที่มีเกณฑ์ในการบันทึกคะแนนจากการทดลอง ดังนี้

ตารางที่ 4.12

การบันทึกคะแนนการล็อคอินเข้าสู่ระบบ

คะแนน	คำอธิบาย
3	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งแรก
2	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งที่ 2
1	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งที่ 3
0	ไม่สามารถล็อคอินเข้าสู่ระบบ

ผู้เข้าร่วมการทดลองจะถูกบันทึกคะแนนการล็อคอินเข้าสู่ระบบตามตารางที่ 4.11 เมื่อนำมาวิเคราะห์ผลการทดลองจะได้ ดังนี้

ตารางที่ 4.13

คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

กลุ่มการทดลอง	จำนวนคน				
	ล็อคอินเข้าสู่ระบบได้ในครั้งแรก	ล็อคอินเข้าสู่ระบบได้ในครั้งที่ 2	ล็อคอินเข้าสู่ระบบได้ในครั้งที่ 3	ไม่สามารถล็อคอินเข้าสู่ระบบ	รวม
1	12	5	1	2	20
2	9	7	3	1	20
3	5	8	4	3	20
4	6	8	3	3	20
รวม	32	28	11	9	80

ผลการทดลองการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ปรากฏว่า ผู้เข้าร่วมการทดลองในแต่ละกลุ่มการทดลองไม่สามารถล็อคอินเข้าสู่ระบบได้ทุกคน มีบางคนไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งแรกมีจำนวน 32 คน ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งที่ 2 มีจำนวน 28 คน ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งที่ 3 มีจำนวน 11 คน และผู้เข้าร่วมการทดลองที่ไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง มีจำนวน 9 คน จากผู้เข้าร่วมการทดลองทั้งหมด 80 คน โดยที่ผู้เข้าร่วมการทดลองในกลุ่มที่ 1 คือ หน่วยทดลองที่มีลักษณะรูปภาพใบหน้าบุคคลเป็นรูปภาพใหญ่แบ่งเป็นส่วนย่อยประกอบกับจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งแรกมากที่สุด มีจำนวน 12 คน

ตารางที่ 4.14

คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	2.35	0.988	20
	2 รอบ	2.20	0.894	20
	รวม	2.28	0.933	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	1.75	1.020	20
	2 รอบ	1.85	1.040	20
	รวม	1.80	1.018	40
รวม	1 รอบ	2.05	1.037	40
	2 รอบ	2.03	0.974	40
	รวม	2.04	0.999	80

ผลการทดลองของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ตามตารางที่ 4.13 แสดงให้เห็นว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยทั้งผู้เข้าร่วมการทดลองที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบก็ตาม จะมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบ 2.28 คะแนน ซึ่งสูงกว่าค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบของกลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลเป็นรูปภาพย่อยในแต่ละกริด แสดงว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยสามารถล็อคอินเข้าสู่ระบบด้วยจำนวนครั้งที่น้อยกว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลย่อยในแต่ละกริด ส่งผลให้ผู้เข้าร่วมการทดลองสามารถจำรหัสผ่านของตนเองได้ ต่อไปเป็นการวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน(Levene’s test) เพื่อวิเคราะห์ความแปรปรวนของแต่ละกลุ่มการทดลองว่ามีความแตกต่างกันอย่างไร

ตารางที่ 4.15

ค่า Levene Statistice สถิติวิเคราะห์คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

F	df1	df2	Sig.
0.132	3	76	0.941

* ที่ระดับนัยสำคัญ 0.05

การวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน (Levene's test) ชี้ให้เห็นว่าค่าความแปรปรวนของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ผู้เข้าร่วมการทดลองแต่ละกลุ่มนั้นไม่แตกต่างกัน (P=0.941;P>0.05) ที่ระดับนัยสำคัญ P<0.05 จึงสามารถนำผลการทดลองนี้ไปใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ได้

ตารางที่ 4.16

ค่าสถิติเปรียบเทียบกลุ่มการทดลองที่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

ปัจจัยทดสอบ	Type III Sum of Squares	df	Mean Square	F	Sig.
ลักษณะรูปภาพใบหน้าบุคคล	4.513	1	4.513	4.631	0.035 *
จำนวนรอบ	0.013	1	0.013	0.013	0.910
ลักษณะรูปภาพใบหน้าบุคคล * จำนวนรอบ	0.313	1	0.313	0.321	0.573

* ที่ระดับนัยสำคัญ 0.05

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริดส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน (P=0.035;P<0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า ลักษณะรูปภาพใบหน้า

บุคคลที่แตกต่างกัน จะทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

การทดสอบอิทธิพลของจำนวนรอบของรหัสผ่านที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ผู้เข้าร่วมการทดลองที่มีจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ($P=0.910;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบจะไม่ทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่านที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริด และจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ($P=0.573;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ ไม่มีอิทธิพลร่วมกันต่อคะแนนการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

ตารางที่ 4.17

ค่าประมาณการแบบช่วงของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน แยกตามลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่าน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	2.350	0.988
	2 รอบ	2.200	0.894
รูปภาพย่อยในแต่ละกริด	1 รอบ	1.750	1.020
	2 รอบ	1.850	1.040

เมื่อศึกษาค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน แยกตามตามลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่าน พบว่า กลุ่มการทดลองที่

ใช้รูปภาพใหญ่แบ่งเป็นส่วนย่อยทั้งที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบ จะมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบสูงกว่ากลุ่มการทดลองที่ใช้รูปภาพย่อยในแต่ละกริดทั้งที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบ

4.2.2.2 ความสำเร็จในการล็อคอินเข้าสู่ระบบ

การวิเคราะห์ผลการทดลองเกี่ยวกับความสำเร็จในการล็อคอินเข้าสู่ระบบ หากผู้เข้าร่วมการทดลองสามารถล็อคอินเข้าสู่ระบบได้ไม่เกิน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองว่าสามารถล็อคอินเข้าสู่ระบบสำเร็จ แต่ถ้าผู้เข้าร่วมการทดลองไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองครั้งนั้นว่าไม่สามารถล็อคอินเข้าสู่ระบบสำเร็จ

ตารางที่ 4.18

จำนวนผู้เข้าร่วมการทดลองในแต่ละปัจจัยการทดลอง

ปัจจัยหลัก	ปัจจัยย่อย	จำนวนคน
ลักษณะของรูปภาพใบหน้าบุคคล	รูปภาพใหญ่แบ่งเป็นส่วนย่อย	20
	รูปภาพย่อยในแต่ละกริด	20
จำนวนรอบในการสร้างและเข้าสู่ระบบ	1 รอบ	20
	2 รอบ	20

ผู้เข้าร่วมการทดลองจะถูกแบ่งออกเป็น 4 กลุ่มการทดลอง มีจำนวนกลุ่มละเท่าๆกัน คือ กลุ่มละ 20 คน รวมผู้เข้าร่วมการทดลองทั้งหมด 80 คน ดังตารางที่ 4.18

ตารางที่ 4.19

จำนวนผู้เข้าร่วมการทดลองในแต่ละกลุ่มการทดลอง

กลุ่มการทดลองที่	จำนวนคน
1	20
2	20
3	20
4	20
รวม	80

ผู้เข้าร่วมการทดลองจะถูกบันทึกความสำเร็จการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน เมื่อนำมาวิเคราะห์ผลการทดลองจะได้ ดังนี้

ตารางที่ 4.20

ค่าสถิติวิเคราะห์ความสำเร็จการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	0.90	0.308	20
	2 รอบ	0.95	0.224	20
	รวม	0.93	0.267	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	0.85	0.366	20
	2 รอบ	0.85	0.366	20
	รวม	0.85	0.362	40
รวม	1 รอบ	0.88	0.335	40
	2 รอบ	0.90	0.304	40
	รวม	0.89	0.318	80

ตารางที่ 4.21

ร้อยละของความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	จำนวน	ล้มเหลว (คน)	สำเร็จ (คน)	ล้มเหลว (%)	สำเร็จ (%)
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	20	2	18	10.00	90.00
	2 รอบ	20	1	19	5.00	95.00
รูปภาพย่อยในแต่ละกริด	1 รอบ	20	3	17	15.00	85.00
	2 รอบ	20	3	17	15.00	85.00
รวม		80	9	71	11.25	88.75

ผลการวิเคราะห์สถิติความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ผู้เข้าร่วมการทดลองส่วนใหญ่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง คิดเป็นร้อยละ 88.75 ของผู้เข้าร่วมการทดลองทั้งหมด ส่วนหน่วยทดลองที่ไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง มีเพียงร้อยละ 11.25 ของผู้เข้าร่วมการทดลองทั้งหมดเท่านั้น

ตารางที่ 4.22

ค่า Levene Statistice สถิติวิเคราะห์ความสำเร็จในการล็อคอินเข้าสู่ระบบ หลังจากลงทะเบียน 7 วัน

F	df1	df2	Sig.
1.996	3	76	0.122

* ที่ระดับนัยสำคัญ 0.05

การวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน (Levene's test) ชี้ให้เห็นว่าค่าความแปรปรวนของความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ผู้เข้าร่วมการทดลองแต่ละกลุ่มนั้นไม่แตกต่างกัน (P=0.122;P>0.05) ที่ระดับนัยสำคัญ P<0.05 จึงสามารถนำผลการทดลองนี้ไปใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ได้

ตารางที่ 4.23

ค่าสถิติเปรียบเทียบกลุ่มการทดลองที่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบ หลังจากลงทะเบียน 7 วัน

ปัจจัยทดสอบ	Type III Sum of Squares	df	Mean Square	F	Sig.
ลักษณะรูปภาพใบหน้าบุคคล	0.113	1	0.113	1.089	0.300
จำนวนรอบ	0.013	1	0.013	0.121	0.729
ลักษณะรูปภาพใบหน้าบุคคล * จำนวนรอบ	0.013	1	0.013	0.121	0.729

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลที่มีต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริดไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ($P=0.300;P<0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะไม่ทำให้ความสำเร็จในการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

การทดสอบอิทธิพลของจำนวนรอบของรหัสผ่านที่มีต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ผู้เข้าร่วมการทดลองที่มีจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ($P=0.729;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบจะไม่ทำให้ความสำเร็จในการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่านที่มีต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริด และจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ($P=0.729;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ ไม่มีอิทธิพลร่วมกันต่อความสำเร็จในการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน

4.2.3 ผลการทดลองการเข้าสู่ระบบด้วยรหัสผ่านรูปภาพหลังจากลงทะเบียน 15 วัน

การวิเคราะห์ผลการทดลองของการเข้าสู่ระบบด้วยรหัสผ่านรูปภาพหลังจากลงทะเบียน 15 วันที่ถูกเก็บในการศึกษาครั้งนี้ประกอบไปด้วย จำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ และความสำเร็จในการเข้าสู่ระบบ โดยใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ที่ระดับความเชื่อมั่น 95% ในการวิเคราะห์ความแตกต่างของผลการทดลอง

4.2.3.1 จำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ

การวิเคราะห์ผลการทดลองเกี่ยวกับจำนวนครั้งที่ใช้ในการล็อคอินเข้าสู่ระบบ ด้วยรหัสผ่านรูปภาพหลังจากลงทะเบียน 15 วัน ผู้เข้าร่วมการทดลองทุกคนในแต่ละกลุ่มการทดลองสามารถล็อคอินเข้าสู่ระบบได้ไม่เกิน 3 ครั้ง หากผู้เข้าร่วมการทดลองไม่สามารถล็อคอินเข้า

ระบบได้ภายใน 3 ครั้ง จะไม่สามารถเข้าสู่ระบบได้ ระบบจะมีการบันทึกผลการทดลองในรูปแบบของคะแนนการล็อคอินเข้าสู่ระบบ โดยที่มีเกณฑ์ในการบันทึกคะแนนจากการทดลอง ดังนี้

ตารางที่ 4.24

การบันทึกคะแนนการล็อคอินเข้าสู่ระบบ

คะแนน	คำอธิบาย
3	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งแรก
2	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งที่ 2
1	สามารถล็อคอินเข้าสู่ระบบได้ในครั้งที่ 3
0	ไม่สามารถล็อคอินเข้าสู่ระบบ

ผู้เข้าร่วมการทดลองจะถูกบันทึกคะแนนการล็อคอินเข้าสู่ระบบตามตารางที่ 4.25 เมื่อนำมาวิเคราะห์ผลการทดลองจะได้ ดังนี้

ตารางที่ 4.25

คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

กลุ่มการทดลอง	จำนวนคน				
	ล็อคอินเข้าสู่ระบบได้ในครั้งแรก	ล็อคอินเข้าสู่ระบบได้ในครั้งที่ 2	ล็อคอินเข้าสู่ระบบได้ในครั้งที่ 3	ไม่สามารถล็อคอินเข้าสู่ระบบ	รวม
1	9	5	2	4	20
2	8	6	2	4	20
3	3	6	5	6	20
4	3	8	3	6	20
รวม	23	25	12	20	80

ผลการทดลองการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ปรากฏว่าผู้เข้าร่วมการทดลองในแต่ละกลุ่มการทดลองไม่สามารถล็อคอินเข้าสู่ระบบได้ทุกคน มีบางคนไม่

สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งแรกมีจำนวน 23 คน ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งที่ 2 มีจำนวน 25 คน ผู้เข้าร่วมการทดลองที่สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งที่ 3 มีจำนวน 12 คน และผู้เข้าร่วมการทดลองที่ไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง มีจำนวน 20 คน จากผู้เข้าร่วมการทดลองทั้งหมด 80 คน โดยที่ผู้เข้าร่วมการทดลองในกลุ่มที่ 1 คือ หน่วยทดลองที่มีลักษณะรูปภาพใบหน้าบุคคลเป็นรูปภาพใหญ่แบ่งเป็นส่วนย่อยประกอบกับจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ สามารถล็อคอินเข้าสู่ระบบสำเร็จในครั้งแรกมากที่สุด มีจำนวน 9 คน

ตารางที่ 4.26

คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	1.95	1.191	20
	2 รอบ	1.90	1.165	20
	รวม	1.93	1.163	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	1.30	1.081	20
	2 รอบ	1.40	1.095	20
	รวม	1.35	1.075	40
รวม	1 รอบ	1.63	1.170	40
	2 รอบ	1.65	1.145	40
	รวม	1.64	1.150	80

ผลการทดลองของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ตามตารางที่ 4.26 แสดงให้เห็นว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยทั้งผู้เข้าร่วมการทดลองที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบก็ตาม จะมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบ 1.93 คะแนน ซึ่งสูงกว่าค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบของกลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลเป็นรูปภาพย่อยในแต่ละกริด แสดงว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยสามารถล็อคอินเข้าสู่ระบบด้วยจำนวนครั้งที่น้อยกว่ากลุ่มการทดลองที่มีลักษณะ

ของรูปภาพใบหน้าบุคคลย่อยในแต่ละกริด ส่งผลให้ผู้เข้าร่วมการทดลองสามารถจำรหัสผ่านของตนเองได้ ต่อไปเป็นการวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน(Levene's test) เพื่อวิเคราะห์ความแปรปรวนของแต่ละกลุ่มการทดลองว่ามีความแตกต่างกันอย่างไร

ตารางที่ 4.27

ค่า Levene Statistice สถิติวิเคราะห์คะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

F	df1	df2	Sig.
0.020	3	76	0.996

* ที่ระดับนัยสำคัญ 0.05

การวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน (Levene's test) ชี้ให้เห็นว่าค่าความแปรปรวนของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ผู้เข้าร่วมการทดลองแต่ละกลุ่มนั้นไม่แตกต่างกัน (P=0.996;P>0.05) ที่ระดับนัยสำคัญ P<0.05 จึงสามารถนำผลการทดลองนี้ไปใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ได้

ตารางที่ 4.28

ค่าสถิติเปรียบเทียบกลุ่มการทดลองที่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบ หลังจากลงทะเบียน 15 วัน

ปัจจัยทดสอบ	Type III Sum of Squares	df	Mean Square	F	Sig.
ลักษณะรูปภาพใบหน้าบุคคล	6.613	1	6.613	5.141	0.026
จำนวนรอบ	0.013	1	0.013	0.010	0.922
ลักษณะรูปภาพใบหน้าบุคคล * จำนวนรอบ	0.113	1	0.113	0.087	0.768

* ที่ระดับนัยสำคัญ 0.05

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริดส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ($P=0.026;P<0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

การทดสอบอิทธิพลของจำนวนรอบของรหัสผ่านที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ผู้เข้าร่วมการทดลองที่มีจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ($P=0.922;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบจะไม่ทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่านที่มีต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริด และจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ($P=0.768;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ ไม่มีอิทธิพลร่วมกันต่อคะแนนการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

เมื่อศึกษาค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน แยกตามตามลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่าน พบว่า กลุ่มการทดลองที่ใช้รูปภาพใหญ่แบ่งเป็นส่วนย่อยทั้งที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบ จะมีค่าเฉลี่ยของคะแนนการล็อคอินเข้าสู่ระบบสูงกว่ากลุ่มการทดลองที่ใช้รูปภาพย่อยในแต่ละกริดทั้งที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบ ดังจะแสดงตามตารางด้านล่าง

ตารางที่ 4.29

ค่าประมาณการแบบช่วงของคะแนนการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน แยกตามลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่าน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	1.950	1.191
	2 รอบ	1.900	1.165
รูปภาพย่อยในแต่ละกริด	1 รอบ	1.300	1.081
	2 รอบ	1.400	1.095

4.2.3.2 ความสำเร็จในการล็อคอินเข้าสู่ระบบ

การวิเคราะห์ผลการทดลองเกี่ยวกับความสำเร็จในการล็อคอินเข้าสู่ระบบ หากผู้เข้าร่วมการทดลองสามารถล็อคอินเข้าสู่ระบบได้ไม่เกิน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองว่าสามารถล็อคอินเข้าสู่ระบบสำเร็จ แต่ถ้าผู้เข้าร่วมการทดลองไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง ระบบจะมีการบันทึกผลการทดลองครั้งนั้นว่าไม่สามารถล็อคอินเข้าสู่ระบบสำเร็จ

ตารางที่ 4.30

จำนวนผู้เข้าร่วมการทดลองในแต่ละปัจจัยการทดลอง

ปัจจัยหลัก	ปัจจัยย่อย	จำนวนคน
ลักษณะของรูปภาพใบหน้าบุคคล	รูปภาพใหญ่แบ่งเป็นส่วนย่อย	20
	รูปภาพย่อยในแต่ละกริด	20
จำนวนรอบในการสร้างและเข้าสู่ระบบ	1 รอบ	20
	2 รอบ	20

ตารางที่ 4.31

จำนวนผู้เข้าร่วมการทดลองในแต่ละกลุ่มการทดลอง

กลุ่มการทดลองที่	จำนวนคน
1	20
2	20
3	20
4	20
รวม	80

ผู้เข้าร่วมการทดลองจะถูกบันทึกความสำเร็จการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน เมื่อนำมาวิเคราะห์ผลการทดลองจะได้ ดังนี้

ตารางที่ 4.32

ค่าสถิติวิเคราะห์ความสำเร็จการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	0.80	0.410	20
	2 รอบ	0.80	0.410	20
	รวม	0.80	0.405	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	0.70	0.470	20
	2 รอบ	0.70	0.470	20
	รวม	0.70	0.464	40
รวม	1 รอบ	0.75	0.439	40
	2 รอบ	0.75	0.439	40
	รวม	0.75	0.436	80

ตารางที่ 4.33

ร้อยละของความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	จำนวน	ล้มเหลว (คน)	สำเร็จ (คน)	ล้มเหลว (%)	สำเร็จ (%)
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	20	4	16	20.00	80.00
	2 รอบ	20	4	16	20.00	80.00
รูปภาพย่อยในแต่ละกริด	1 รอบ	20	6	14	30.00	70.00
	2 รอบ	20	6	14	30.00	70.00
รวม		80	20	60	25.00	75.00

ผลการวิเคราะห์สถิติความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ผู้เข้าร่วมการทดลองส่วนใหญ่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง คิดเป็นร้อยละ 75 ของผู้เข้าร่วมการทดลองทั้งหมด ส่วนหน่วยทดลองที่ไม่สามารถล็อคอินเข้าสู่ระบบได้ภายใน 3 ครั้ง มีเพียงร้อยละ 25 ของผู้เข้าร่วมการทดลองทั้งหมด

ตารางที่ 4.34

ค่า Levene Statistice สถิติวิเคราะห์ความสำเร็จในการล็อคอินเข้าสู่ระบบ หลังจากลงทะเบียน 15 วัน

F	df1	df2	Sig.
1.389	3	76	0.253

* ที่ระดับนัยสำคัญ 0.05

การวิเคราะห์ผลการทดลองด้วยสถิติทดสอบความแปรปรวนเลวีน (Levene’s test) ชี้ให้เห็นว่าค่าความแปรปรวนของความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ผู้เข้าร่วมการทดลองแต่ละกลุ่มนั้นไม่แตกต่างกัน ($P=0.253;P>0.05$) ที่ระดับนัยสำคัญ $P<0.05$ จึงสามารถนำผลการทดลองนี้ไปใช้วิธีการวิเคราะห์ความแปรปรวนแบบสองทาง (Two-way ANOVA) ได้

ตารางที่ 4.35

ค่าสถิติเปรียบเทียบกลุ่มการทดลองที่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบ หลังจากลงทะเบียน 15 วัน

ปัจจัยทดสอบ	Type III Sum of Squares	df	Mean Square	F	Sig.
ลักษณะรูปภาพใบหน้าบุคคล	0.200	1	0.200	1.027	0.314
จำนวนรอบ	0.000	1	0.000	0.000	1.000
ลักษณะรูปภาพใบหน้าบุคคล * จำนวนรอบ	0.000	1	0.000	0.000	1.000

* ที่ระดับนัยสำคัญ 0.05

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลที่มีต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริดไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน (P=0.314;P<0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะทำให้ความสำเร็จในการล็อคอินเข้าสู่ระบบไม่แตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

การทดสอบอิทธิพลของจำนวนรอบของรหัสผ่านที่มีต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ผู้เข้าร่วมการทดลองที่มีจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน (P=1.000;P>0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ จะทำให้ความสำเร็จในการล็อคอินเข้าสู่ระบบไม่แตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

การทดสอบอิทธิพลของลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของรหัสผ่านที่มีต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริด และจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน (P=1.000;P>0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า

ลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ ไม่มีอิทธิพลร่วมกันต่อความสำเร็จในการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน

4.3 ผลการวิเคราะห์ผลการทดลองทางด้านประสิทธิภาพความปลอดภัย

การวิเคราะห์ผลการทดลองทางด้านประสิทธิภาพความปลอดภัยจะทำการทดลองกับทุกกลุ่มการทดลองร่วมกับผู้ทดลองปกติ ในวันเดียวกับการล็อคอินเข้าสู่ระบบครั้งแรกหลังจากลงทะเบียนเรียบร้อยแล้ว มีการเก็บผลการทดลองเกี่ยวกับความสำเร็จในการโจรกรรมรหัสผ่าน โดยสามารถทำการโจรกรรมรหัสผ่านได้ไม่เกิน 3 ครั้ง หลังจากทำการทดลองเรียบร้อยแล้ว ได้ผลการทดลอง ดังนี้

ตารางที่ 4.36

ค่าสถิติวิเคราะห์ความสำเร็จในการโจรกรรมรหัสผ่าน

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	จำนวน	ล้มเหลว (คน)	สำเร็จ (คน)	ล้มเหลว (%)	สำเร็จ (%)
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	20	20	0	100	0
	2 รอบ	20	20	0	100	0
รูปภาพย่อยในแต่ละกริด	1 รอบ	20	20	0	100	0
	2 รอบ	20	20	0	100	0
รวม		80	80	0	100	0

ผลการวิเคราะห์ค่าสถิติความสำเร็จในการโจรกรรมรหัสผ่าน พบว่า ไม่มีผู้เข้าร่วมการทดลองคนใดสามารถโจรกรรมรหัสผ่านได้สำเร็จ แสดงว่ารูปแบบของรหัสผ่านรูปภาพที่ให้ผู้ใช้พิมพ์ตัวอักษรภาษาอังกฤษที่ปรากฏใต้รูปภาพใบหน้าบุคคลนั้น สามารถป้องกันการโจรกรรมรหัสผ่านด้วยเทคนิค Shoulder Surfing ได้

4.4 ผลการวิเคราะห์ผลการทดลองทางด้านความพึงพอใจ

การวิเคราะห์ผลการทดลองทางด้านความพึงพอใจ ผู้เข้าร่วมการทดลองในทุกกลุ่มการทดลองจะได้รับแบบสอบถามความพึงพอใจ เพื่อประเมินผลหลังจากทำการทดลองเรียบร้อยแล้ว หลังจากที่ผู้เข้าร่วมการทดลองได้ทำแบบสอบถามเรียบร้อยแล้วจึงได้นำมาวิเคราะห์ผลการประเมินดังนี้

ตารางที่ 4.37

ค่าสถิติวิเคราะห์ความพึงพอใจ

รายการประเมิน	N	Minimum	Maximum	Mean	Std. Deviation
เป็นเครื่องมือช่วยจำรหัสผ่านได้ง่ายขึ้นมากกว่ารหัสผ่านแบบตัวอักษร	80	2	5	3.51	0.871
เป็นเครื่องมือช่วยให้ท่านจำรหัสผ่านได้ยาวนานยิ่งขึ้น	80	2	5	3.50	0.675
เป็นเครื่องมือช่วยให้ระลึกถึงรหัสผ่านได้ดีเมื่อเวลาผ่านไป และกลับมาใช้งานอีกครั้ง	80	2	5	3.55	0.654
พึงพอใจระบบทำงานรหัสผ่านรูปภาพโดยรวม	80	2	5	3.76	0.484
ช่วยเพิ่มระดับความปลอดภัยจากผู้คุกคามได้มากกว่ารหัสผ่านตัวอักษร	80	3	5	4.21	0.544
พึงพอใจกับเวลาที่ใช้ในการใส่รหัสผ่านรูปภาพ	80	2	4	2.94	0.643
การวางตำแหน่งปุ่มทำงาน และการสื่อความหมาย มีความเข้าใจได้ง่ายและเหมาะสมในการใช้งาน	80	2	5	3.68	0.522
จำนวนตัวอักษรที่ต้องพิมพ์มีความเหมาะสม	80	2	4	3.15	0.553
การปรากฏของข้อความใต้รูปภาพมีความ	80	2	4	3.15	0.576

ชัดเจน					
ชนิดของใบหน้าบุคคลที่แสดงให้เลือกใช้งานเป็นรหัสผ่านรูปภาพ มีความเหมาะสม	80	3	4	3.74	0.443
ค่าเฉลี่ย	80	3.00	4.00	3.5188	0.20629

ตารางที่ 4.38

ค่าสถิติวิเคราะห์ความพึงพอใจตามกลุ่มการทดลอง

ลักษณะของรูปภาพใบหน้าบุคคล	จำนวนรอบในการสร้างและเข้าสู่ระบบ	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	จำนวน
รูปภาพใหญ่แบ่งเป็นส่วนย่อย	1 รอบ	3.6150	0.22542	20
	2 รอบ	3.4850	0.18144	20
	รวม	3.5500	0.21243	40
รูปภาพย่อยในแต่ละกริด	1 รอบ	3.4900	0.19708	20
	2 รอบ	3.4850	0.20333	20
	รวม	3.4875	0.19766	40
รวม	1 รอบ	3.5525	0.21837	40
	2 รอบ	3.4850	0.19021	40
	รวม	3.5188	0.20629	80

จากสถิติวิเคราะห์ความพึงพอใจตามกลุ่มการทดลอง ตามตารางที่ 4.37 แสดงให้เห็นว่ากลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยทั้งผู้เข้าร่วมการทดลองที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบก็ตาม จะมีค่าเฉลี่ยของความพึงพอใจ 3.55 ซึ่งสูงกว่าค่าเฉลี่ยความพึงพอใจของกลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลเป็น รูปภาพย่อยในแต่ละกริด

ตารางที่ 4.39

ค่าสถิติเปรียบเทียบกลุ่มการทดลองที่ส่งผลต่อความพึงพอใจของผู้เข้าร่วมการทดลอง

ปัจจัยทดสอบ	Type III Sum of Squares	df	Mean Square	F	Sig.
ลักษณะรูปภาพใบหน้าบุคคล	0.078	1	0.078	1.906	0.171
จำนวนรอบ	0.091	1	0.091	2.224	0.140
ลักษณะรูปภาพใบหน้าบุคคล * จำนวนรอบ	0.078	1	0.078	1.906	0.171

ค่าสถิติวิเคราะห์ความพึงพอใจตามกลุ่มการทดลอง พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริดไม่ส่งผลต่อความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อรหัสผ่านรูปภาพ (P=0.314;P<0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะทำให้ความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อรหัสผ่านรูปภาพไม่แตกต่างกัน

ค่าสถิติวิเคราะห์ความพึงพอใจตามกลุ่มการทดลอง พบว่า ผู้เข้าร่วมการทดลองที่มีจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อรหัสผ่านรูปภาพ (P=1.000;P>0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ จะทำให้ความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อรหัสผ่านรูปภาพไม่แตกต่างกัน

ค่าสถิติวิเคราะห์ความพึงพอใจตามกลุ่มการทดลอง พบว่า ลักษณะรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และรูปภาพย่อยในแต่ละกริด และจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบทั้ง 1 รอบ และ 2 รอบ ไม่ส่งผลต่อความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อรหัสผ่านรูปภาพ (P=1.000;P>0.05) ที่ระดับนัยสำคัญ P<0.05 แสดงว่า ลักษณะรูปภาพใบหน้าบุคคลและจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบ ไม่มีอิทธิพลร่วมกันต่อความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อรหัสผ่านรูปภาพ

4.5 ผลการวิเคราะห์เพิ่มเติม

การวิเคราะห์ผลการทดลองเพิ่มเติม ประกอบไปด้วย ผลการวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน และผลการวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ มีรายละเอียดดังนี้

4.5.1 ผลการวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน

การวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน (Password space) สำหรับการตั้งรหัสผ่านรูปภาพ โดยเลือก 8 รูปภาพเป็นรหัสผ่าน จากตัวเลือกทั้งหมด 36 รูปภาพ โดยแยกตามปัจจัยจำนวนรอบของการตั้งรหัสผ่านและรูปแบบการนำเสนอรูปภาพใบหน้าบุคคล ดังนี้

กรณีที่ 1 จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และรูปแบบในการนำเสนอรูปภาพใบหน้าบุคคลทั้งที่เป็นรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วนหรือรูปภาพใบหน้าบุคคลขนาดเล็ก

$$P_{n,r} = \frac{n!}{(n-r)!} = \frac{36!}{(36-8)!}$$

$$= \frac{36!}{28!}$$

$$= 1{,}220{,}096{,}908{,}800$$

จากการคำนวณด้วยวิธีเรียงสับเปลี่ยน (permutation) จะได้ความเป็นไปได้ของรหัสผ่านเท่ากับ 1,220,096,908,800 วิธี

กรณีที่ 2 จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และรูปแบบในการนำเสนอรูปภาพใบหน้าบุคคลทั้งที่เป็นรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วนหรือรูปภาพใบหน้าบุคคลขนาดเล็ก

รอบที่ 1 $P_{n,r} = \frac{18!}{(18-4)!} = \frac{18!}{14!} = 73{,}440$

รอบที่ 2 $P_{n,r} = \frac{18!}{(18-4)!} = \frac{18!}{14!} = 73{,}440$

รวม 2 รอบ = 73,440 + 73,440

= 146,880

จากการคำนวณด้วยวิธีเรียงสับเปลี่ยน (permutation) จะได้ความเป็นไปได้ของรหัสผ่านเท่ากับ 146,880 วิธี

4.5.2 ผลการวิเคราะห์ความถี่ของตำแหน่งรูปภาพ

การวิเคราะห์ความความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ โดยการวิเคราะห์ตำแหน่งของรูปภาพที่ถูกเลือกเพื่อตั้งเป็นรหัสผ่าน จากตำแหน่งของรูปภาพทั้งหมด 36 ช่อง โดยแยกตามปัจจัยวิธีการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าขนาดใหญ่แบ่งส่วน และปัจจัยวิธีการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าขนาดเล็ก ได้ดังนี้

ตารางที่ 4.40

ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มการทดลองที่ใช้รูปแบบการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นใหญ่หน้าขนาดใหญ่แบ่งส่วน

2.19	4.69	0.94	0.94	4.69	2.81
1.88	6.88	0.31	3.75	6.25	4.06
0.63	5.94	0.94	0.63	5.31	1.25
2.50	2.50	1.88	2.81	2.81	0.63
4.06	7.19	1.25	0.94	6.56	0.63
2.19	0.63	2.19	2.50	2.19	2.50

ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มการทดลองที่ใช้รูปแบบการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นใหญ่หน้าขนาดใหญ่แบ่งส่วน ตามตารางที่ 4.40 ปรากฏว่า บริเวณที่ถูกเลือกมากที่สุด จะเป็นบริเวณที่เป็นอวัยะสำคัญของใบหน้าบุคคล สังเกตว่า บริเวณตำแหน่งตรงกลางของรูปภาพ ซึ่งจะเป็นบริเวณจมูกหรือหน้าผากมักจะเป็นตำแน่งที่ถูกเลือกมากที่สุด นอกจากนี้ในส่วนของรูปภาพใบหน้าผู้หญิงที่อยู่ตำแหน่ง 9 ช่องซ้ายบน สังเกตว่าบริเวณที่เป็นตุ้มหูทั้ง 2 ข้าง ก็เป็นตำแหน่งที่ถูกเลือกมากเช่นเดียวกัน

ตารางที่ 4.41

ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มการทดลองที่ใช้รูปแบบการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นใหญ่หน้าขนาดเล็ก

4.06	1.88	2.19	2.50	4.69	4.69
1.88	2.50	1.88	3.75	4.06	2.81
3.13	2.19	2.19	1.56	4.06	3.75
3.75	2.19	1.88	2.81	2.81	3.44
2.81	2.81	2.19	1.56	2.19	1.88
3.44	1.88	2.19	2.50	2.19	3.75

ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มการทดลองที่ใช้รูปแบบการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นใหญ่หน้าขนาดใหญ่แบ่งส่วน ตามตารางที่ 4.41 พบว่า ตำแหน่งของรูปภาพใบหน้าบุคคลที่ถูกผู้เข้าร่วมการทดลองเลือกมีลักษณะกระจาย บริเวณที่ถูกเลือกมากที่สุดจะเป็นบริเวณขอบตารางในแต่ละประเภทของรูปภาพใบหน้าบุคคล โดยเฉพาะมุมของตารางทั้ง 4 มุม

จะถูกผู้เข้าร่วมการทดลองเลือกมากที่สุด เกิดจากการจำใบหน้าบุคคลทั้งใบหน้าจะต้องจำรายละเอียดความแตกต่างของใบหน้าทั้งหมด ทำให้ผู้เข้าร่วมการทดลองเลือกที่จะใช้วิธีการเลือกรหัสผ่านจากตำแหน่งของตารางโดยเฉพาะขอบตารางโดยไม่สนใจรูปภาพใบหน้าบุคคล

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้ได้ศึกษาปัจจัยที่ส่งผลกระทบต่อประสิทธิภาพใช้งาน ความปลอดภัย และความพึงพอใจเกี่ยวกับรหัสผ่านรูปภาพแบบกริดที่มีการนำรูปภาพใบหน้าบุคคลมาใช้เป็นรหัสผ่านโดยจะมีตัวอักษรภาษาอังกฤษกำกับไว้แต่ละรูปภาพเพื่อเพิ่มความยากในการโจรกรรมรหัสผ่าน โดยมีปัจจัยที่ถูกนำมาใช้ในงานวิจัย 2 ปัจจัย ประกอบด้วย จำนวนรอบที่ใช้ในการสร้างรหัสผ่านและการพิสูจน์ตัวตน มี 2 ระดับ คือ 1 รอบ และ 2 รอบ และอีกปัจจัย คือ ลักษณะการใช้รูปภาพสำหรับรหัสผ่าน มี 2 ระดับ คือ รูปภาพใหญ่ตัดเป็นส่วนๆ และ รูปภาพย่อยในแต่ละกริด การทดลองถูกออกแบบเป็น 2x2 Between Subject Factorial Design มี 4 กลุ่มการทดลอง ผู้เข้าร่วมการทดลองกลุ่มละ 20 คน ใช้ผู้ร่วมการทดลองทั้งหมด 80 คน โดยจะมีการเก็บผลการล็อคอินเข้าสู่ระบบ 3 ครั้ง คือ ผลการล็อคอินเข้าสู่ระบบทันทีหลังจากการลงทะเบียน ผลการล็อคอินเข้าสู่ระบบหลังจากการลงทะเบียน 7 วัน และผลการล็อคอินเข้าสู่ระบบหลังจากการลงทะเบียน 15 วัน หลังจากทดลองแล้วจึงได้ทำการวิเคราะห์ผลการทดลองของการมีรูปภาพใบหน้าบุคคลในการสร้างรหัสผ่านที่มีผลต่อการจำรหัสผ่านของผู้เข้าร่วมการทดลอง และความสำเร็จในการเข้าสู่ระบบ นอกจากนี้ยังมีการทดลองประสิทธภาพด้านความปลอดภัย ด้วยการจำลองการโจรกรรมข้อมูลรหัสผ่านด้วยวิธี Shoulder Surfing โดยทำการทดลองกับการล็อคอินเข้าสู่ระบบครั้งแรกหลังจากลงทะเบียนทันที ซึ่งจะให้ผู้ที่ไม่ได้ทดลองมายืนมองอยู่ด้านหลัง จากนั้นให้ทดลองเข้าสู่ระบบ แล้วนำผลการทดลองนี้มาวิเคราะห์ประสิทธิภาพด้านความปลอดภัยของรหัสผ่าน ซึ่งในบทนี้จะกล่าวถึงการสรุปผลที่ได้จากการทดลอง ประโยชน์ที่ได้รับของงานวิจัยและข้อเสนอแนะในการวิจัยในอนาคต

5.1 สรุปผลการวิจัย

จากผลการทดลองในบทที่ผ่านมา สามารถนำมาสรุปผลการวิจัย โดยจะทำการสรุปผลการวิจัยในด้านต่างๆ ประกอบด้วย การสรุปผลการวิจัยด้านประสิทธิภาพการใช้งาน ประสิทธิภาพความปลอดภัย และความพึงพอใจ

5.1.1 ประสิทธิภาพการใช้งาน

ผลจากการวิเคราะห์ปัจจัยลักษณะการใช้รูปภาพใบหน้าบุคคลสำหรับรหัสผ่าน ทั้งแบบที่เป็นรูปภาพใหญ่ตัดเป็นส่วนๆ และ รูปภาพย่อยในแต่ละกริด รวมทั้งปัจจัยจำนวนรอบที่ใช้ในการสร้างรหัสผ่านและการพิสูจน์ตัวตน ทั้ง 1 รอบ และ 2 รอบ จะส่งผลต่อประสิทธิภาพการใช้งาน โดยหากมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที ปรากฏว่า ผู้เข้าร่วมการทดลองทุกคนสามารถเข้าสู่ระบบได้ภายใน 3 ครั้ง อิทธิพลของกลุ่มการทดลองที่มีลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบแตกต่างกัน และไม่มีอิทธิพลร่วมกันต่อคะแนนการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียนทันที

ประสิทธิภาพการใช้งาน โดยหากมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ปรากฏว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ส่วนจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบแตกต่างกัน ไม่ส่งผลให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน และไม่มีอิทธิพลร่วมกันต่อคะแนนการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 7 วัน ขณะที่ความสำเร็จในการเข้าสู่ระบบคิดเป็นร้อยละ 88.75 ของผู้เข้าร่วมการทดลองทั้งหมด

สำหรับประสิทธิภาพการใช้งาน หากมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ปรากฏว่า ลักษณะรูปภาพใบหน้าบุคคลที่แตกต่างกัน จะทำให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ส่วนจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบแตกต่างกัน ไม่ส่งผลให้คะแนนการล็อคอินเข้าสู่ระบบแตกต่างกัน และไม่มีอิทธิพลร่วมกันต่อคะแนนการล็อคอินเข้าสู่ระบบ เมื่อมีการล็อคอินเข้าสู่ระบบหลังจากลงทะเบียน 15 วัน ขณะที่ความสำเร็จในการเข้าสู่ระบบคิดเป็นร้อยละ 75 ของผู้เข้าร่วมการทดลองทั้งหมด

จากการวิเคราะห์ผลการทดลอง พบว่า ลักษณะของรูปภาพใบหน้าบุคคลที่มีใหญ่แบ่งเป็นส่วนๆ ส่งผลให้ผู้ใช้สามารถจำรหัสผ่านได้ดีกว่ารูปภาพย่อย อย่างมีนัยสำคัญ เนื่องจากการจดจำเพียงบางส่วนของใบหน้านั้นจะจำเพียงแค่ความหมายของสิ่งที่จะจำ เช่น จำเพียงว่าจมูก ปาก หู เป็นต้น ซึ่งต่างกับการจดจำทั้งใบหน้าที่ต้องมีการจดจำรายละเอียดต่างๆของใบหน้าทั้งหมด เช่น สีผิว ลักษณะของปาก ลักษณะของตา เป็นต้น แล้วนำรายละเอียดทุกส่วนของใบหน้ามาประกอบกันเพื่อแยกความแตกต่างของแต่ละใบหน้า สอดคล้องกับทฤษฎีทางจิตวิทยาเกี่ยวกับการจดจำใบหน้าของมนุษย์

จากสมมติฐาน การมีจำนวนรอบของการตั้งรหัสผ่านเพียงรอบเดียว ทำให้ผู้ใช้มีตัวเลือกที่จะนำมาสร้างรหัสผ่านถึง 36 รูปภาพ น่าจะทำให้ผู้ใช้มีตัวเลือกหลากหลายกว่าการตั้งรหัสผ่านรูปภาพ 2 รอบ ที่มีตัวเลือกในการตั้งรหัสผ่านเพียงรอบละ 18 รูปภาพ แต่จากการทดลองพบว่า จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และ 2 รอบ ส่งผลต่อการใช้งาน ไม่แตกต่างกัน

เนื่องจากว่า การตั้งรหัสผ่านรูปภาพ 1 รอบ มีจำนวนตัวเลือกเยอะ จะทำให้มีทั้งข้อดีและข้อเสีย ข้อดีคือ ทำให้ผู้ใช้มีตัวเลือกเยอะสามารถตัดสินใจเลือกรหัสภาพรูปภาพได้หลากหลาย ส่วนข้อเสียคือตัวเลือกเยอะอาจทำให้ผู้ใช้ตัดสินใจเลือกรูปภาพไม่ถูก ไม่รู้ว่าจะเลือกรูปภาพใดมาเป็นรหัวผ่านดี สำหรับการตั้งรหัสผ่านรูปภาพ 2 รอบ มีตัวเลือกน้อยกว่าการตั้งรหัสผ่านรูปภาพ 1 รอบนั้น ก็มีทั้งข้อดีและข้อเสียเช่นกัน ข้อดีคือ การมีจำนวนตัวเลือกน้อยทำให้ผู้ใช้สามารถตัดสินใจเลือกรหัสผ่านรูปภาพได้ง่าย ไม่ต้องตัดสินใจมาก ส่วนข้อเสียคือ การที่มีจำนวนตัวเลือกน้อยทำให้ผู้ใช้ไม่สามารถเลือกรูปภาพมาเป็นรหัสผ่านจากจำนวนตัวเลือกที่จำกัดได้

เมื่อสรุปวิเคราะห์ผลการทดลอง พบว่า การใช้รหัสผ่านรูปภาพที่เป็นใบหน้าบุคคลส่งผลให้ผู้ใช้งานสามารถจดจำรหัสผ่านได้ดีขึ้น เมื่อเวลาผ่านไปสามารถช่วยให้ระลึกถึงรหัสผ่านได้

5.1.2 ประสิทธิภาพความปลอดภัย

การโจรกรรมรหัสผ่านรูปภาพด้วยเทคนิค Shoulder Surfing ได้ถูกนำมาใช้ในการทดสอบสอบประสิทธิภาพด้านความปลอดภัยของรหัสผ่านรูปภาพที่ได้ออกแบบไว้ โดยสมมติฐานที่ตั้งไว้ได้คาดการณ์ว่าจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ซึ่งจะมีจำนวนรูปภาพทั้งหมด 36 รูปภาพน่าจะทำให้โจรกรรมรหัสผ่านได้ยากกว่าการตั้งรหัสผ่านด้วยจำนวนรอบ 2 รอบ เนื่องจากการตั้งรหัสผ่านด้วยจำนวนรอบ 1 รอบนั้น มีจำนวนรูปภาพตัวเลือกที่มากกว่า การตั้งรหัสผ่าน 2 รอบ น่าจะทำให้ผู้โจรกรรมเดารหัสผ่านได้ยากกว่า

ผลการวิเคราะห์ค่าสถิติความสำเร็จในการโจรกรรมรหัสผ่าน พบว่า ไม่มีผู้เข้าร่วมการทดลองคนใดสามารถโจรกรรมรหัสผ่านได้สำเร็จ ทั้งผู้เข้าร่วมการทดลองที่อยู่ในกลุ่มของการตั้งรหัส 1 รอบ หรือ 2 รอบก็ตาม แสดงว่ารูปแบบของรหัสผ่านรูปภาพที่ให้ผู้ใช้พิมพ์ตัวอักษรภาษาอังกฤษที่ปรากฏใต้รูปภาพใบหน้าบุคคลนั้น สามารถป้องกันการโจรกรรมรหัสผ่านด้วยเทคนิค Shoulder Surfing ได้ นอกจากนี้ จากการทดลอง พบว่า ปัจจัยด้านจำนวนรอบของการสร้างรหัสผ่านและการเข้าสู่ระบบไม่ส่งผลต่อความสำเร็จในการล็อคอินเข้าสู่ระบบ เนื่องจากการที่จะโจรกรรมรหัสผ่านได้นั้น ผู้โจรกรรมจะต้องคาดเดาให้ได้ว่าผู้ใช้เลือกรูปภาพใด โดยไม่สารถที่จะเดาตัวอักษรที่พิมพ์ได้ เพราะว่าตัวอักษรจะถูกสุ่มขึ้นมาใหม่ทุกครั้ง และเนื่องจากผู้ใช้ไม่ได้คลิกที่รูปภาพใบหน้าบุคคลบนหน้าจอคอมพิวเตอร์ทำให้เพิ่มความยากในการโจรกรรม

5.1.3 ความพึงพอใจของผู้เข้าร่วมการทดลอง

จากแบบสอบถามที่ให้ผู้เข้าร่วมการทดลองผู้เข้าร่วมการทดลองในทุกกลุ่มการทดลองจะได้รับ เพื่อประเมินผลหลังจากทำการทดลอง พบว่า ผู้เข้าร่วมการทดลองในทุกกลุ่มการทดลองมีความพึงพอใจในระบบรหัสผ่านรูปภาพใบหน้าบุคคลที่ได้ออกแบบในงานวิจัยนี้ไม่แตกต่าง

กัน โดยกลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อยทั้งผู้เข้าร่วมการทดลองที่มีเงื่อนไขจำนวนรอบในการสร้างและเข้าสู่ระบบ 1 รอบ หรือ 2 รอบก็ตาม จะมีค่าเฉลี่ยของความพึงพอใจ สูงกว่าค่าเฉลี่ยความพึงพอใจของกลุ่มการทดลองที่มีลักษณะของรูปภาพใบหน้าบุคคลเป็น รูปภาพย่อยในแต่ละกริด

5.2 อภิปรายผลการวิจัย

การพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ได้ถูกออกแบบในงานวิจัยนี้ มีพื้นฐานมาจากรหัสผ่านรูปภาพแบบ S-Passface พบว่า การใช้รูปภาพใบหน้าบุคคลขนาดใหญ่แล้วแบ่งส่วน จะทำให้ผู้ใช้สามารถจดจำรหัสได้ได้ดีกว่าการใช้รูปภาพใบหน้าบุคคลขนาดเล็กมาเป็นรหัสผ่านรูปภาพ เนื่องจากการจำเพียงบางส่วนของใบหน้านั้นมีกระบวนการจำที่ไม่ซับซ้อนเท่ากับการจดจำทั้งใบหน้าที่ผู้ใช้ต้องให้รายละเอียดส่วนต่างๆของใบหน้า

จากการสังเกตการณ์พฤติกรรมของผู้เข้าร่วมการทดลองในการลงทะเบียนสร้างรหัสผ่านและการล็อคอินเข้าสู่ระบบ จะเห็นว่า ผู้เข้าร่วมการทดลองบางคนจะสร้างรหัสผ่านโดยเลือกจากรูปภาพที่อยู่ขอบของตาราง ซึ่งหากมีรูปแบบในการเลือกรหัสผ่านเช่นนี้อาจทำให้ผู้โจรกรรมสามารถคาดเดาได้ง่ายทำให้อาจเกิดปัญหาด้านความปลอดภัยได้ ผู้เข้าร่วมการทดลองบางคนจะเลือกภาพที่เป็นส่วนใกล้เคียงกันในกรณีที่เป็นรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งเป็นส่วนย่อย หรืออาจมีการเลือกส่วนที่เป็นอวัยวะที่แห็นเด่นชัด เพื่อให้สามารถจดจำองค์ประกอบได้ง่าย

การเลือกใช้รูปภาพใบหน้าบุคคลในการสร้างรหัสผ่านรูปภาพในงานวิจัยนี้ เนื่องจากมีงานวิจัยทางด้านจิตวิทยาที่ระบุว่ามนุษย์สามารถจดจำและแยกแยะลักษณะของใบหน้าบุคคลได้ดีกว่ารูปภาพวัตถุอื่นๆ อย่างไรก็ตาม รูปภาพใบหน้าบุคคลที่นำมาใช้ในงานวิจัยบางภาพอาจมีลักษณะที่โดดเด่นกว่ารูปภาพอื่น เช่น ใส่แว่นตา หรือใบหน้าใหญ่เต็มช่องตาราง เป็นต้น ทำให้ผู้ใช้อาจเกิดความสนใจและมีแนวโน้มที่จะเลือกรูปภาพเหล่านี้มาใช้เป็นรหัสผ่านรูปภาพได้ ซึ่งอาจทำให้ผู้ที่ต้องการจะโจรกรรมรหัสผ่านสามารถคาดเดาได้

5.3 ประโยชน์ของงานวิจัย

จากการวิเคราะห์ผลการทดลองแสดงให้เห็นว่า การออกแบบรหัสรหัสผ่านรูปภาพใบหน้าบุคคลทำให้ได้รับประโยชน์ในเชิงทฤษฎี คือ งานวิจัยนี้มีส่วนสนับสนุนงานวิจัยรหัสผ่านรูปภาพแบบ S-Passface ถือเป็นรูปแบบของรหัสผ่านรูปภาพที่ดีทั้งในแง่ของการใช้งานที่ผู้ใช้สามารถจดจำรหัสผ่านได้ และในแง่ของความปลอดภัยที่ให้ผู้ใช้พิมพ์ตัวอักษรใต้รูปภาพใบหน้าบุคคลแทนการ

คลิกที่รูปภาพ ทำให้ผู้ไม่หวังดีสามารถโจรกรรมรหัสผ่านได้ยาก นอกจากนี้ การใช้รูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วนมาเป็นตัวเลือกในการสร้างรหัสผ่านจะทำให้ผู้ใช้สามารถจดจำรหัสผ่านรูปภาพได้ดีขึ้น สอดคล้องกับทฤษฎีด้านจิตวิทยาเกี่ยวกับการจดจำใบหน้าของมนุษย์ ซึ่งการจำเพียงบางส่วนของใบหน้ามีความซับซ้อนและรายละเอียดน้อยกว่าการจำทั้งใบหน้า เนื่องจากการจำบางส่วนของใบหน้า ผู้ใช้เพียงแค่จำว่าสิ่งนั้นคืออะไร เช่น จมูก ปาก เป็นต้น ต่างจากจำทั้งใบหน้าที่จำเป็นต้องจดจำรายละเอียดของทุกส่วนของใบหน้า

ประโยชน์ในเชิงการนำไปใช้ของงานวิจัยนี้ คือ การนำรูปแบบการนำเสนอรูปภาพใบหน้าบุคคลที่เป็นรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วนไปใช้งานเป็นรหัสผ่านรูปภาพ เนื่องจากการนำเสนอรูปรูปภาพใบหน้าบุคคลด้วยรูปภาพใบหน้าบุคคลขนาดใหญ่แบ่งส่วนจะส่งผลให้ผู้ใช้จำรหัสผ่านได้ดีขึ้น สำหรับจำนวนรอบที่ใช้ในการสร้างรหัสผ่านรูปภาพนั้น จากผลการทดลองแสดงให้เห็น จำนวนรอบในการสร้างรหัสผ่าน 1 รอบ หรือ 2 รอบ ไม่ส่งผลต่อประสิทธิภาพด้านการใช้งานและความปลอดภัย ดังนั้น หากมีการนำจำนวนรอบในการสร้างรหัสผ่าน 1 รอบไปใช้งาน จะช่วยให้ผู้พัฒนาเขียนโปรแกรมได้ง่ายขึ้น เนื่องจากไม่ต้องตรวจสอบรหัสผ่านซ้ำ 2 รอบ

5.4 แนวทางการวิจัยในอนาคต

เพื่อประโยชน์ในการนำไปใช้งานในอนาคต สามารถพัฒนางานวิจัยเพื่อเพิ่มประสิทธิภาพในด้านการใช้งานและประสิทธิภาพด้านความปลอดภัย ได้ดังนี้

1. ควรศึกษากลุ่มประชากรเพิ่มเติมจากเดิมให้มีความหลากหลายทั้งกลุ่มทำงาน และกลุ่มช่วงอายุต่างๆ รวมทั้งเพิ่มเติมกลุ่มตัวอย่างประชากรให้มีจำนวนมากขึ้น เพื่อนำมาปรับปรุงประสิทธิภาพของรหัสผ่านรูปภาพให้ดียิ่งขึ้น

2. ควรศึกษาเกี่ยวกับรูปแบบการเลือกรหัสผ่าน เนื่องจากจากการสังเกต พบว่า มีผู้เข้าร่วมการทดลองบางส่วนมีรูปแบบการเลือกรูปภาพในลักษณะบริเวณขอบหรือตรงกลางของตาราง อาจเกิดจากรูปภาพที่ต้องการอยู่ในตำแหน่งนั้นพอดีหรือผู้เข้าร่วมการทดลองสนใจตำแหน่งของตารางก็ได้ หากผู้ใช้มีรูปแบบการเลือกรหัสผ่านจากตำแหน่งของตารางอาจส่งผลให้ผู้ไม่หวังดีสามารถเดารูปแบบของรหัสผ่านได้

3. ในงานวิจัยนี้ได้ให้ผู้ใช้พิมพ์ตัวอักษรภาษาอังกฤษใต้รูปภาพแทนการคลิกที่รูปภาพเพื่อป้องกันการโจรกรรมรหัสผ่านด้วยเทคนิค Shoulder surfing ควรที่จะทดสอบการโจรกรรมรหัสผ่านด้วยวิธีอื่นด้วย เช่น การโจรกรรมรหัสผ่านด้วยเทคนิค Brute force ที่เป็นการสุ่มรหัสผ่านในทุกความเป็นไปได้ของตัวอักษร เป็นต้น เพื่อนำไปปรับปรุงประสิทธิภาพของรหัสผ่านรูปภาพให้มีความปลอดภัยเพิ่มขึ้น

รายการอ้างอิง

หนังสือ

กัลยา วานิชย์บัญชา. (2552). การใช้ SPSS for Windows ในการวิเคราะห์ข้อมูล. กรุงเทพฯ: โรงพิมพ์ ธรรมสาร.

อุบลวรรณ ภวกานันท์. (2555). จิตวิทยาการรู้ คิด และปัญญา(Cognitive Psychology). กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัย ธรรมศาสตร์.

วิทยานิพนธ์

สาโรจน์ เชตนุช, อิทธิพลของภาพประกอบที่มีผลต่อการระลึกได้ของรหัสผ่านรูปภาพที่ประกอบด้วยรูปทรงในตาราง. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2555.

Articles

Akpulat, M., Bicakci, K. & Cil, U. (2013). Revisiting Graphical Passwords for Augmenting, not Replacing, Text Pass words. ACSAC 2013 : 29th Annual Computer Security Applications Conference, 119-128

A. M. Eljetlawi and N. Ithnin. (2008). Graphical password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods. Proceeding of 2008 IEEE Third International Conference on Convergence and Hybrid Information Technology, 1137-1143.

Farnaz, T., Maslin, M., & Azizah, A. M. (2013). An Enhancement on Passface Graphical Password Authentication Journal of Basic and Applied Scientific Research. Vol.3, 135-141

Forget, A., Chiasson, S., Oorschot, V., & Biddle, R (2008). Improving Text Passwords Though Persuasion. Symposium on Usable Privacy and Security (SOUPS).

H. Tao and C. Adams. (2008). Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security, Vol.7, No.2, 273-292.

Lashkari, A. H., Zakaria, O. B., Farmand, S., & Saleh, R. (2009). Shoulder Surfing attack in graphical password authentication. (IJCSIS) International Journal of Computer Science and Information Security Vol. 6, NO. 2, 145-154

L. Sobrado and J. Birget. (2002). Graphical Passwords. The Rutgers Scholar. An Electronic Bullentin of Undergraduate Research, Rutgers University, Camden New Jersey, Vol. 4.

Mohamed, A. H. Norafida. (2007). Graphical password: Security and Usability Issues. UTM seminar.

Morris, R., & Thompson, K. (1979). Password security: A case history. Communications of the ACM (11), 594-597

Paivio, A., Rogers, T. B., &Smythe, P. C. (1968). Why are pictures easier to recall than word?. Psychonomic Science, 137-138.

T. Zangooei, M. Mansoori and I. Welch. (2012). A Hybrid Recognition and Recall Based Approach in Graphical Passwords. Proceeding of 2012 ACM, 665-673.

W. Hu, X. Wu and G. Wei. (2010). The Security Analysis of Graphical Passwords. Proceeding of IEEE 2010 International Conference on Communications and Intelligence Information Security, 200-203.

Electronic Media

Real User Corporation. *The science behide Passface.* www.realuser.com : June, 2005

ภาคผนวก

ภาคผนวก ก
แบบสอบถาม

เนื่องงานวิจัยนี้ได้ทำหน้าโปรแกรมขึ้นมาใหม่เพื่อทำการทดลองกับผู้ร่วมการทดลอง เพื่อได้ทราบถึงความคิดเห็นของผู้ร่วมการทดลองที่มีต่อหน้าโปรแกรมที่ใช้งาน โดยรูปแบบแบบสอบถามดังนี้

คำชี้แจงสำหรับผู้ตอบแบบสอบถาม

1. การศึกษาวิจับครั้งนี้มีวัตถุประสงค์เพื่อการศึกษาความคิดเห็นของบุคคลต่อการใช้งานระบบรหัสผ่านรูปภาพ (Graphical Password) เอกสารส่งเสริมการปรับปรุงระบบนี้เพื่อความคุ้มค่าในประเด็นด้าน *ประสิทธิผล* หรือ การนำความรู้ที่ได้รับไปใช้งานต่อไป

2. แบบสอบถามมีทั้งหมด 4 หน้า แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลพื้นฐาน เกี่ยวกับผู้ตอบแบบสอบถาม ได้แก่ เพศ อายุ ระดับการศึกษา (Checklists) และ/ หรือเติมคำลงในช่วงว่างที่กำหนด

ส่วนที่ 2 ความคิดเห็นของผู้ตอบแบบสอบถามต่อการระบบ Graphical Password และความสวยงามของหน้าต่างโปรแกรม

ส่วนที่ 3 ข้อเสนอแนะ เพื่อพิจารณาประเด็นปัญหาที่พบและสิ่งที่ความปรับปรุง

ส่วนที่ 1 ข้อมูลพื้นฐาน เกี่ยวกับผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่อง ❍ หน้าข้อความที่ตรงกับสภาพความเป็นจริงของท่านหรือเติมข้อความลงในช่องว่างที่กำหนด

1. สถานภาพ ❍ อาจารย์
❍ นักศึกษา ป.ตรี / นักศึกษา ป.โท
❍ พนักงานเอกชน / รัฐวิสาหกิจ
❍ อื่นๆ โปรดระบุ.....

2. เพศ ❍ ชาย ❍ หญิง

3. อายุ ❍ ต่ำกว่า 30 ปี ❍ มากกว่า30-40 ปี ❍ มากกว่า 40-50 ปี
❍ มากกว่า 50 ปีขึ้นไป

4. ระดับการศึกษาขั้นสูงสุดที่สำเร็จการศึกษาแล้ว
❍ ต่ำกว่าปริญญาตรี ❍ ปริญญาตรี ❍ปริญญาโท
❍ ปริญญาเอก

5. ท่านคิดว่า ทักษะการใช้งานคอมพิวเตอร์ของท่านจัดอยู่ในระดับ
❍ อ่อนที่สุด ❍ อ่อน ❍ พอใช้ ❍ ดี ❍ ดีมาก

ส่วนที่ 2 ความคิดเห็นของผู้ตอบแบบสอบถามต่อการระบบ Graphical Password และความสวยงามของหน้าต่างโปรแกรม

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่องว่างที่ตรงกับความคิดเห็นของท่านมากที่สุด

5 = เห็นด้วยอย่างยิ่ง 4 = เห็นด้วย 3 = ไม่แน่ใจ 2 = ไม่เห็นด้วย
1 = ไม่เห็นด้วยอย่างยิ่ง

รายการประเมิน	5	4	3	2	1
1. เป็นเครื่องมือช่วยให้ท่านจำรหัสผ่านของท่านได้ง่ายขึ้นมากกว่ารหัสผ่านแบบตัวอักษร					
2. เป็นเครื่องมือช่วยให้ท่านจำรหัสผ่านของท่านได้ยาวนานยิ่งขึ้น					
3. เป็นเครื่องมือช่วยให้ระลึกถึงรหัสผ่านของท่านได้ดี เมื่อเวลาผ่านไป และกลับมาใช้งานอีกครั้ง					
4. ท่านพึงพอใจระบบทำงานรหัสผ่านรูปภาพโดยรวม					
5. วิธีนี้จะช่วยให้ท่านเพิ่มระดับความปลอดภัยจากผู้คุกคามได้มากกว่ารหัสผ่านตัวอักษร					
6. ท่านพึงพอใจกับเวลาที่ใช้ในการใส่รหัสผ่านรูปภาพ					
7. การวางตำแหน่งปุ่มทำงาน และการสื่อความหมาย มีความเข้าใจได้ง่ายและเหมาะสมในการใช้งาน					
8. จำนวนตัวอักษรที่ต้องพิมพ์มีความเหมาะสม					
9. การปรากฏของข้อความใต้รูปภาพมีความชัดเจน					
10. ชนิดของใบหน้าบุคคลที่แสดงให้เลือกใช้งานเป็นรหัสผ่านรูปภาพ มีความเหมาะสม					

ส่วนที่ 3

ข้อติชมและข้อเสนอแนะเพื่อปรับปรุงระบบรหัสผ่านรูปภาพ

.....

.....

.....

ประวัติผู้เขียน

ชื่อ	นายนิพัทธิ์ ภัทรโสภณกุล
วันเดือนปีเกิด	11 กรกฎาคม 2529
วุฒิการศึกษา	ปีการศึกษา 2551: วิทยาศาสตรบัณฑิต (เทคโนโยลีคอมพิวเตอร์) มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ตำแหน่ง	นักวิชาการคอมพิวเตอร์ การประปาส่วนภูมิภาค

ผลงานทางวิชาการ

นิพัทธิ์ ภัทรโสภณกุล, และ ณัฐธนนท์ หงส์วริทธิ์ธร. (2556). *อิทธิพลของรูปภาพประกอบที่มีต่อการระลึกได้ของรหัสผ่าน.* International Computer Science and Engineering Conference (ICSEC 2013), 536-541

ประสบการณ์ทำงาน	2554-ปัจจุบัน นักวิชาการคอมพิวเตอร์ การประปาส่วนภูมิภาค 2553-2554 นักวิชาการคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ