

ผลของการมีจุดอ้างอิงและวิธีการสร้างรหัสผ่าน ที่มีต่อความปลอดภัยและการใช้งานรหัสผ่านรูปภาพแบบกริด Effects of Reference Points and Password Creation Approach on Security and Usability of Grid-based Graphical

ณัฐรณนธ์ หงส์วรสิทธิ์* และเกรียงไกร มะโนใจ

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี

มหาวิทยาลัยธรรมศาสตร์ ศูนย์รังสิต ตำบลคลองหนึ่ง อำเภอคลองหลวง จังหวัดปทุมธานี 12120

Nuttanont Hongwarittorn* and Kriangkrai Manochai

Department of Computer Science, Faculty of Science and Technology,

Thammasat University, Rangsit Centre, Khlong Nueng, Khlong Luang, Pathum Thani 12120

บทคัดย่อ

งานวิจัยนี้ได้ออกแบบรหัสผ่านรูปภาพโดยมุ่งเน้นใช้ตารางกริดมาใช้ในการออกแบบและศึกษาเปรียบเทียบปัจจัยที่นำมาใช้ในการออกแบบ เพื่อศึกษาผลจากการใช้ตารางกริด (ตารางกริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิง) และวิธีการสร้างรหัสผ่าน (รหัสผ่านแบบผู้ใช้สร้างเองกับรหัสผ่านที่ระบบสร้างให้) ด้านประสิทธิภาพการใช้งานและประสิทธิภาพความปลอดภัย ใช้รูปแบบการทดลองแบบ between-subject design แบ่งเป็น 4 กลุ่มการทดลองแบบสุ่ม ผู้เข้าร่วมการทดลองจำนวน 60 คน แบ่งเป็นกลุ่มการทดลอง กลุ่มละ 15 คน ประกอบด้วย กลุ่มที่ใช้ตารางกริดแบบมีจุดอ้างอิงผู้ใช้สร้างรหัสผ่านเอง กลุ่มที่ใช้ตารางกริดแบบมีจุดอ้างอิงระบบสร้างรหัสผ่านให้ กลุ่มที่ใช้ตารางกริดแบบไม่มีจุดอ้างอิงผู้ใช้สร้างรหัสผ่านเอง และกลุ่มที่ใช้ตารางกริดแบบไม่มีจุดอ้างอิงระบบสร้างรหัสผ่านให้ แล้วประเมินประสิทธิภาพด้านการใช้งานและความปลอดภัยด้วยจำนวนครั้งที่ใช้เข้าระบบ เวลาเฉลี่ยที่ใช้เข้าระบบ และความสำเร็จในการเข้าระบบ ผลการศึกษาชี้ให้เห็นว่าปัจจัยที่ส่งผลต่อประสิทธิภาพการใช้งานและความปลอดภัยคือปัจจัยการได้มาของรหัสผ่าน โดยรหัสผ่านที่ผู้ใช้สร้างเองจะส่งผลต่อประสิทธิภาพการใช้งานดีกว่ารหัสผ่านที่ระบบสร้างให้ ขณะเดียวกันรหัสผ่านที่ผู้ใช้สร้างเองก็ส่งผลต่ออัตราความสำเร็จในการโจรกรรมสูงกว่าเช่นกัน ส่วนของปัจจัยรูปแบบตารางกริดกลับไม่ส่งผลต่อประสิทธิภาพการใช้งานและประสิทธิภาพความปลอดภัย ด้านความพึงพอใจพบว่าผู้ใช้มีความพึงพอใจมากต่อโปรแกรมการพิสูจน์ตัวตนที่ออกแบบ ขณะที่ผลการวิเคราะห์ความพึงพอใจแยกตามกลุ่มการทดลองพบว่ามีความพึงพอใจไม่แตกต่างกัน

คำสำคัญ : รหัสผ่านรูปภาพ; ตารางกริด; จุดอ้างอิง; การสร้างรหัสผ่าน

*ผู้รับผิดชอบบทความ : nth@cs.tu.ac.th

Abstract

This research was aimed at creating a graphical password by using grid tables and comparing the factors used for creating them. This study was to investigate the effects of types of grid tables (grid tables with a reference point and without a reference point) and the method of password creation (password set by users and passwords set by a computer system) on usability and security. There were four experimental groups. A between-subject design was employed to conduct the experiment. Purposive sampling was used due to the research constraints. The current study was conducted with 60 users. Each group had 15 samples. The 4 groups comprised of a group of users creating passwords by themselves by using a grid table with a reference point, a group of users creating passwords automatically by using a grid table with a reference point, a group of users creating passwords by themselves by using a grid table without a reference point, and a group of users creating a password automatically by using a grid table without a reference point. The usability and security evaluations were determined by numbers of logging in the system, average time spent for logging in, and the success of logging in. The current study showed that the password-creation method factor affected the usability and security significantly. The passwords set by users themselves resulted in better recalls than the system-created passwords. However, the passwords created by users increased the probability of them being stolen. The factor of types of grid table contrarily did not affect the usability and security. In terms of satisfaction, the users were satisfied with the created authentication program and their satisfaction was not different among the experimental groups.

Keywords: picture password; grid; reference point; password creation

1. บทนำ

ทุกวันนี้ระบบเครือข่ายคอมพิวเตอร์เต็มไปด้วยอันตรายจากการคุกคามข้อมูลจากผู้ไม่ประสงค์ดี เช่น attacker, hacker, cracker และ spammer ในการโจรกรรมข้อมูลสำคัญขององค์กรไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลทางธุรกิจ ซึ่งเป็นข้อมูลที่มีความสำคัญสูงและเป็นความลับภายในองค์กร ถ้าข้อมูลเหล่านี้ถูกโจรกรรมหรือรั่วไหลออกไป ข้อมูลเหล่านี้อาจถูกนำไปใช้ในทางที่ผิดและสร้างความเสียหายร้ายแรงได้ทั้งในระดับตัวบุคคลและองค์กร ด้วยเหตุนี้กระบวนการพิสูจน์ตัวตนจึงมีความสำคัญอย่างมาก

กระบวนการพิสูจน์ตัวตนในปัจจุบันมีหลากหลายเทคนิค ซึ่งเทคนิคที่เป็นที่นิยมใช้กันอย่างแพร่หลายคือการใช้รหัสผ่านตัวอักษร วิธีการนี้ยังมีข้อเสียหลายอย่าง ปัญหาที่สำคัญอย่างหนึ่งของรหัสผ่านตัวอักษรคือรหัสผ่านจำได้ยาก จากการศึกษที่ผ่านมาแสดงให้เห็นว่าผู้ใช้จะเลือกตั้งรหัสผ่านที่สั้นและมีความหมายเพื่อที่จะจำได้ง่าย [1] ซึ่งส่งผลให้รหัสผ่านเหล่านี้สามารถถูกคาดเดาและถูกโจมตีได้ง่ายด้วยวิธี small dictionary attack [2] แต่ถ้าตั้งรหัสผ่านที่ซับซ้อนคาดเดาได้ยาก ผู้ใช้ก็จะเกิดปัญหาในเรื่องของการลืมและระลึกถึงรหัสผ่าน การสำรวจของ Xiaoyuan ในปี

ค.ศ. 2005 เปิดเผยว่าสามารถโจรกรรมรหัสผ่าน (password cracker) ประมาณ 80 % บนเครือข่าย ตัวอย่างได้ภายในเวลา 30 วินาทีเท่านั้น [3] รหัสผ่านรูปภาพ [4] จึงเป็นทางเลือกหนึ่งที่สามารถนำมาใช้ในกระบวนการเข้าสู่ระบบของผู้ใช้แทนการใช้รหัสผ่านตัวอักษร รหัสผ่านรูปภาพจะช่วยเพิ่มความใช้งานง่ายและจดจำได้ง่าย จากผลการยืนยันทางจิตวิทยาพบว่ามนุษย์สามารถรับรู้และจดจำ รูปทรงเรขาคณิต ลวดลาย ข้อความ และสีได้ดีกว่าตัวอักษรที่ไม่มี ความหมาย ซึ่งช่วยสนับสนุนถึงความเป็นไปได้อย่างมากที่จะใช้วิธีการพิสูจน์ตัวตนด้วยภาพแทนการพิสูจน์ ตัวด้วยรหัสผ่านตัวอักษร [5] ทำให้กระบวนการพิสูจน์ ตัวตนมีการศึกษาวิจัยและพัฒนาอย่างต่อเนื่องและ ในปัจจุบันยังมีงานวิจัยเกี่ยวกับรหัสผ่านรูปภาพที่อยู่ ระหว่างการวิจัยอีกจำนวนมาก

Jermyn และคณะ ได้เสนอวิธี draw-a-secret (DAS) [1] ซึ่งจะให้ผู้ใช้งานวาดรหัสผ่านได้ไม่ซ้ำกัน ความเป็นไปได้ในการสร้างรหัสผ่านของวิธีนี้มีมากกว่าวิธี รหัสผ่านตัวอักษร แต่วิธีการนี้ยังมีปัญหาเมื่อผู้ใช้งาน เส้นทับบนเส้นตาราง หรือลงบนจุดตัด วิธีการนี้ยังไม่ สามารถแยกได้ว่าผู้ใช้งานทดลองบนช่องไหน

Dhamija และ Perrig ได้เสนอวิธีพิสูจน์ตัวตน ที่เรียกว่า Déjà vu [6] ใช้รูปภาพที่เป็นนามธรรมทดลอง เปรียบเทียบกับรหัสผ่านแบบตัวตัวอักษรและแบบ PIN ผลการทดลองชี้ให้เห็นว่าผู้ใช้ 90 % สามารถพิสูจน์ ตัวตนสำเร็จ ขณะที่การใช้รหัสผ่านตัวอักษรและ PIN ผู้ใช้สามารถพิสูจน์ตัวตนสำเร็จเพียง 70 % เท่านั้น

Real User Corporation ได้พัฒนารหัสผ่าน ภาพด้วยรูปใบหน้าคนที่เรียกว่า Passface TM [7] จากข้อสันนิษฐานว่ามนุษย์สามารถจำใบหน้ามนุษย์ได้ ง่ายกว่ารูปภาพอื่น

Towhidi และคณะ ได้เสนอวิธีการปรับปรุง ความปลอดภัยของ Passface ที่เรียกว่า S-Passface

[8] เพื่อป้องกันการโจมตีจากการแอบมองจากด้านหลัง (shoulder surfing attack) สามารถป้องกันการโจมตี แบบการแอบมองได้ถึง 100 เปอร์เซ็นต์ แต่วิธีนี้จะทำให้ ความง่ายในการใช้งานลดลงเช่นกัน

วัชรินทร์ และณัฐชนน ได้ศึกษาเปรียบเทียบ เพื่อหาปัจจัยที่มีอิทธิพลต่อประสิทธิภาพการใช้งาน และความปลอดภัยของวิธีการพิสูจน์ตัวตนด้วย รหัสผ่านรูปภาพแบบรูปการ์ตูน [9] ซึ่งมีปัจจัยการใช้ ตารางกริดและปัจจัยรูปแบบการได้มาของรหัสผ่าน พบว่าผู้ใช้สร้างรหัสผ่านเองจะมีประสิทธิภาพด้าน การใช้งานที่ดีกว่า แต่ถ้าระบบสุ่มรหัสผ่านให้จะมี ประสิทธิภาพด้านความปลอดภัยที่ดีกว่า

อนุพงศ์ และณัฐชนน ได้วิจัยเชิงสำรวจถึง ปัจจัยในการออกแบบรหัสผ่านรูปภาพแบบกริด [10] ผลการวิจัยพบว่าควรใช้ตารางกริดขนาด 4x4 ที่เป็น รูปแบบจตุรัส และรูปภาพที่ควรนำมาสร้างเป็น รหัสผ่านควรเป็นรูปภาพแบบรูปธรรม ซึ่งควรเป็น รูปภาพสิ่งมีชีวิตและรูปภาพวัตถุ

เจริญ และณัฐชนน ได้ทดลองเรื่องจำนวน รูปภาพที่เหมาะสมที่จะนำมาใช้ในการสร้างรหัสผ่าน แบบรูปภาพ [11] ผลการทดลองชี้ให้เห็นว่าจำนวน ภาพที่ผู้เข้าร่วมการทดลองสามารถระลึกได้ส่วนใหญ่ อยู่ที่ 4 ถึง 6 รูป

เกรียงไกร และณัฐชนน ได้ทดลองเรื่อง รูปแบบตารางกริดและรูปแบบภาพที่ส่งผลต่อการ จดจำรูปภาพ [12] ผลการทดลองชี้ให้เห็นว่ารูปแบบ ตารางกริดที่เหมาะสมควรเป็นแบบจตุรัส ส่วนรูปแบบ ภาพบุคคลกับไม่ใช่บุคคลไม่ได้ส่งผลต่อจำนวนภาพที่ จำได้ของผู้เข้าร่วมการทดลอง

Tao และ Adams ได้พัฒนาวิธีที่เรียกว่า Pass-Go [13] เป็นวิธีการหนึ่งที่ใช้ตารางกริดที่คล้ายกับ วิธีการของ DAS ซึ่งชี้ให้เห็นว่าวิธีการนี้ช่วยยกระดับ ความปลอดภัยและความเป็นไปได้ของรหัสผ่านมากขึ้น

Lin และคณะ ได้พัฒนาวิธีการที่เรียกว่า BDAS (Background DAS) [14] ต่อยอดจากวิธีการ Draw-a-secret (DAS) โดยการใช้ภาพพื้นหลังเข้ามาเป็นส่วนหนึ่งของรหัสผ่านรูปภาพ ซึ่งนอกจากจะทำให้รหัสผ่านรูปภาพมีความปลอดภัยสูงแล้วยังทำให้การระลึกรหัสผ่านรูปภาพของผู้ใช้ง่ายขึ้นอีกด้วย

Ray's scheme ซึ่งเสนอโดย Ray เป็นวิธีการพิสูจน์ตัวตนแบบระบบไฮบริด (hybrid system) [15] โดยผสมระหว่างการเรียนรู้จำ (recognition based scheme) และการระลึกได้ (recall based scheme) สำหรับอุปกรณ์มือถือ ผลการศึกษาชี้ให้เห็นว่าวิธีการนี้มีประโยชน์และสะดวกในการใช้งานมากกว่าวิธีการแบบดั้งเดิมบนหน้าจอเดสก์ท็อป

Arianeshad และคณะ ได้เสนอวิธีที่เรียกว่า Grid Points [16] โดยใช้ eye-tracking เป็นอุปกรณ์ช่วยสร้างรหัสผ่าน โดยการออกแบบรหัสผ่านรูปภาพแบบกริดจำนวน 4 รูปแบบ โดยพบว่าตารางกริดขนาด 5×4 (รูปแบบที่ 1) เป็นรูปแบบที่นิยมใช้โดยทั่วไปบนระบบล็อกหน้าจอ (pattern lock) ของอุปกรณ์แอนดรอยด์เป็นรูปแบบที่ดีที่สุดในการใช้งาน (อัตราการความสำเร็จในการเข้าสู่ระบบสูงและใช้เวลาน้อย)

งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบกริดมาศึกษาถึงปัจจัยที่มีอิทธิพลต่อประสิทธิภาพการใช้งานและความปลอดภัย โดยปัจจัยที่จะนำมาศึกษาเปรียบเทียบได้แก่ ปัจจัยการใช้ตารางกริด ประกอบด้วยตารางกริดแบบมีจุดอ้างอิง (reference point) และตารางกริดแบบไม่มีจุดอ้างอิง ปัจจัยรูปแบบการได้มาของรหัสผ่าน ประกอบไปด้วยการที่ผู้ใช้งานสร้างรหัสผ่านเองทั้งหมดและการที่ระบบสร้างรหัสผ่านให้ทั้งหมด แล้วผู้ใช้งานสามารถปรับแก้ตำแหน่งภาพได้ และปัจจัยประเภทของภาพสำหรับเป็นตัวเลือกในการสร้างรหัสผ่าน ประกอบไปด้วยการผสมกันระหว่างผลไม้กับ

สัตว์เลี้ยง ซึ่งเป็นรูปภาพที่บุคคลทั่วไปรู้จักเป็นอย่างดี โดยมีสมมติฐานว่าปัจจัยรูปแบบการได้มาของรหัสผ่านและปัจจัยประเภทของภาพสำหรับเป็นตัวเลือกในการสร้างรหัสผ่านจะส่งผลกระทบต่อประสิทธิภาพการใช้งาน ประสิทธิภาพความปลอดภัย และความพึงพอใจที่ผู้ใช้มีต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบกริดแตกต่างกัน

2. ระเบียบวิธีการศึกษา

2.1 ระเบียบวิธีวิจัยที่ใช้ในการศึกษาวิจัย

งานวิจัยนี้ศึกษาเปรียบเทียบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบผลไม้และสัตว์เลี้ยงแบบมีปัจจัยการใช้ตารางกริดแบบมีจุดอ้างอิง (reference point) และไม่มีจุดอ้างอิง (จุดอ้างอิงหมายถึงการกำหนดจุดลงบนตารางกริดที่ไม่ใช่พื้นที่การสร้างรหัสผ่านและจุดที่กำหนดมือถือเป็นรหัสผ่านกำหนดเพื่อให้เกิดมุมมองมากกว่าหนึ่งมุมมอง) และแบบมีปัจจัยรูปแบบการได้มาของรหัสผ่าน เพื่อนำมาวัดประสิทธิภาพเปรียบเทียบกันทั้งในเรื่องของประสิทธิภาพในด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจ โดยกำหนดตัวแปรและสมมติฐานที่ใช้ในการทดลองดังนี้

2.1.1 รหัสผ่านรูปภาพแบบกริดที่มีจุดอ้างอิงบนตารางกริดจะส่งผลกระทบต่อประสิทธิภาพด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจมากกว่าแบบไม่มีจุดอ้างอิงบนตารางกริด

2.2.2 รหัสผ่านรูปภาพแบบกริดที่มีรูปแบบการได้มาของรหัสผ่านแบบผู้สร้างรหัสผ่านเองทั้งหมดจะส่งผลกระทบต่อประสิทธิภาพด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจมากกว่ารหัสผ่านแบบระบบสุ่มสร้างให้ทั้งหมด

2.2.3 ปฏิสัมพันธ์ระหว่างรหัสผ่านรูปภาพ

แบบกริดที่มีจุดอ้างอิงกับรูปแบบการได้มาของรหัสผ่านจะส่งผลต่อประสิทธิภาพด้านการใช้งาน ด้านความปลอดภัยและความพึงพอใจของผู้ใช้

2.2 การออกแบบการทดลอง

งานวิจัยใช้การทดลองแบบ 2x2 between subjects design หน่วยทดลองจะถูกสุ่มลงในกลุ่มการทดลอง 1 กลุ่ม จาก 4 กลุ่มทดลอง จากกลุ่มผู้เข้าร่วม

การทดลองโดยเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างจำนวน 3 ครั้ง โดยใช้โปรแกรมและแบบสอบถามเป็นเครื่องมือหลักในการเก็บรวบรวมข้อมูล เพื่อศึกษาเปรียบเทียบประสิทธิภาพการทำงานของผู้ใช้โปรแกรมการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพบนตารางกริดทั้ง 4 รูปแบบ (ตารางที่ 1)

ตารางที่ 1 รูปแบบการทดลองที่ออกแบบ

ปัจจัยที่ศึกษา		รูปแบบตารางกริด	
		มีจุดอ้างอิง	ไม่มีจุดอ้างอิง
รูปแบบการได้มาของรหัสผ่าน	รหัสผ่านที่ผู้ใช้สร้างเอง	กลุ่มทดลองที่ 1	กลุ่มทดลองที่ 3
	รหัสผ่านที่ระบบสร้างขึ้น	กลุ่มทดลองที่ 2	กลุ่มทดลองที่ 4

งานวิจัยนี้เลือกใช้กลุ่มตัวอย่าง จำนวน 60 คน ทั้งเพศชายและเพศหญิง โดยผู้เข้าร่วมการทดลองทุกคนเคยผ่านการใช้งานระบบการพิสูจน์ตัวตนมาแล้ว และผ่านการใช้งานคอมพิวเตอร์มาอย่างน้อย 1 ปี แบ่งกลุ่มตัวอย่างออกเป็น 4 กลุ่ม กลุ่มละ 15 คน แต่ละกลุ่มจะเข้ารับการทดสอบด้านการใช้งานกลุ่มละ 1 รูปแบบ การพิสูจน์ตัวตนและผู้เข้ารับการทดสอบทางด้านความปลอดภัยจำนวน 7 คน แยกต่างหากจากกลุ่มผู้เข้าร่วมการทดลองด้านประสิทธิภาพการใช้งาน

2.3 เครื่องมือที่ใช้ในการเก็บข้อมูล

รูปแบบโปรแกรมการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบภาพวัตถุทั่วไปที่ใช้ในการทดลองในครั้งนี้ ถูกพัฒนาขึ้นด้วยภาษา C#.NET ทำงานบนระบบปฏิบัติการ Microsoft Windows 7 ประมวลผลด้วยโปรแกรม Internet Explorer ในคอมพิวเตอร์แบบพกพา มีหน่วยประมวลผลยี่ห้ออินเทล (Intel® Core™ i5) ความเร็วในการประมวลผล 2.3 กิกะเฮิร์ตซ์ มีหน่วยความจำหลัก 4 กิกะไบต์ และมีจอภาพแบบ LCD ขนาด 14 นิ้ว ที่มีความละเอียดของจอภาพ

1366x768 พิกเซล ในส่วนของการศึกษาความพึงพอใจของผู้ใช้ จะใช้แบบสอบถามออนไลน์เก็บข้อมูลเบื้องต้นก่อนผู้ทดลองจะเริ่มทดลอง เมื่อทดลองเสร็จจะใช้แบบประเมินออนไลน์เพื่อเก็บข้อมูลด้านความพึงพอใจในการใช้งานโปรแกรม

2.4 การเก็บรวบรวมข้อมูล

งานวิจัยนี้เก็บรวบรวมข้อมูลโดยใช้ระยะเวลาเก็บข้อมูล 3 สัปดาห์ โดยใช้แบบสอบถามเก็บข้อมูลเบื้องต้นของผู้เข้าร่วมการทดลอง หลังจากนั้นจะใช้โปรแกรมการพิสูจน์ตัวตนที่ออกแบบทดลองเพื่อเก็บข้อมูลการทดลองทางด้านประสิทธิภาพการใช้งานและความปลอดภัย โดยการทดลองทางด้านประสิทธิภาพการใช้งานนั้นจะทดลองทั้งหมด 3 ครั้ง ได้แก่ หลังจากสร้างรหัสผ่านวันแรกทันที หลังจากสร้างรหัสผ่าน 3 วัน และหลังจากสร้างรหัสผ่าน 15 วัน เพื่อจะวัดความสามารถในการจำได้ (retention over time) แต่ในส่วนของการทดลองทางด้านประสิทธิภาพความปลอดภัยจะทดลอง 2 ครั้ง คือ หลังจากผู้เข้าร่วมการทดลองเข้าสู่ระบบสำเร็จครั้งแรกทันทีและหลังจาก

สร้างรหัสผ่าน 15 วัน เมื่อผู้เข้าร่วมการทดลองทดลองเสร็จจะใช้แบบสอบถามหลังการทดลองเก็บข้อมูลด้านความพึงพอใจในการใช้งานระบบที่ออกแบบ

2.5 ขั้นตอนการพัฒนาโปรแกรม

งานวิจัยนี้เลือกใช้ขนาดตารางกริด 5x5 และเลือกรูปวัตถุทั่วไปมาใช้ในการทดลองประกอบไปด้วยภาพผลไม้และสัตว์เลี้ยง ซึ่งเป็นภาพที่พบเห็นทั่วไปและเป็นที่รู้จัก รวมทั้งสิ้น 49 ภาพ จัดเรียงเป็นแถวทั้งหมด 7 แถว แถวละ 7 รูป วิธีการเลือกรูปไปใส่เป็นรหัสผ่าน ให้คลิกเมาส์ซ้ายที่รูปที่ต้องการแล้วลากไปวางบนตารางกริดตามตำแหน่งที่ต้องการสร้างเป็นรหัสผ่าน ถ้าตำแหน่งที่ต้องการวางรูปมีรูปอยู่แล้วจะเป็นการวางรูปใหม่ทับรูปเก่า ส่วนวิธีการเอารูปออกให้คลิกเมาส์ซ้ายที่รูปที่ต้องการจะเอาออก 1 ครั้ง ถ้าต้องการล้างรหัสผ่านทั้งตารางให้กดที่ปุ่มยกเลิก หากยืนยันสร้างรหัสผ่านให้กดที่ปุ่มลงทะเบียน

2.6 การนำผลการทดลองที่ได้มาวัดผล

งานวิจัยนี้จะนำผลการทดลองที่ได้จากการทดลองและแบบสอบถาม ไปวิเคราะห์ข้อมูลด้วยวิธีการ two-way ANOVA ผลการทดลองที่ได้จากการทดลองแบ่งออกเป็น ผลการทดลองทางด้านประสิทธิภาพการใช้งาน จะประกอบไปด้วย จำนวนครั้งที่ใช้พิสูจน์ตัวตนเวลาเฉลี่ยที่ใช้พิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน ผลการทดลองด้านประสิทธิภาพความปลอดภัย ประกอบด้วยจำนวนครั้งที่ใช้เพื่อโจรกรรมรหัสผ่าน เวลาเฉลี่ยที่ใช้ในการโจรกรรมรหัสผ่าน และความสำเร็จในการโจรกรรมรหัสผ่าน รวมทั้งความพึงพอใจที่มีต่อระบบวัดจากการเก็บข้อมูลจากแบบสอบถามหลังการทดลอง

2.7 วิธีการทดลอง

เมื่อผู้เข้าร่วมการทดลองพร้อมทดลอง การทดลองจะเริ่มจากการอธิบายวัตถุประสงค์ของการวิจัย แก่กลุ่มตัวอย่างต่อการทดลองหนึ่งครั้ง กลุ่มตัวอย่าง

ประกอบด้วยผู้เข้าร่วมการทดลองที่พิสูจน์ตัวตนและ ผู้เข้าร่วมการทดลองที่โจรกรรม การทดลองแบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 จะเริ่มทดลองโดยใช้แบบสอบถามเก็บข้อมูลเบื้องต้นของผู้เข้าร่วมการทดลอง

ส่วนที่ 2 จะใช้โปรแกรมการพิสูจน์ตัวตนที่ออกแบบทดลองเพื่อเก็บข้อมูลการทดลองด้านประสิทธิภาพการใช้งานและความปลอดภัย เมื่อผู้เข้าร่วมการทดลองเปิดโปรแกรมขึ้นมาก็จะเข้าสู่หน้าลงทะเบียน ระบบจะให้ผู้เข้าร่วมการทดลองตั้งชื่อผู้ใช้งานที่เป็นตัวอักษร หลังจากนั้นจะเข้าสู่ขั้นตอนการสร้างรหัสผ่าน โดยผู้เข้าร่วมการทดลองกลุ่มที่สร้างรหัสผ่านเองทั้งหมดจะต้องสร้างรหัสผ่านด้วยการเลือกรูปวัตถุทั่วไปจำนวน 6 รูป จากทั้งหมด 49 รูป ไปจัดวางลงในตารางกริดขนาด 5x5 ขณะที่ผู้เข้าร่วมการทดลองกลุ่มที่ระบบสร้างรหัสผ่านให้ระบบจะสุ่มรหัสผ่านจำนวน 6 ภาพ ให้อัตโนมัติ โดยผู้เข้าร่วมการทดลองสามารถเลื่อนตำแหน่งภาพได้ แต่ไม่สามารถเปลี่ยนภาพได้ ซึ่งทั้ง 2 แบบ ไม่สามารถใช้รูปซ้ำกันเกิน 2 ภาพ และไม่สามารถวางภาพติดกันในแนวตั้งและแนวนอนในการตั้งเป็นรหัสผ่านได้ เมื่อสร้างรหัสผ่านได้ตามที่ต้องการก็ให้กดปุ่มยืนยันการลงทะเบียน เพื่อบันทึก ชื่อผู้ใช้งาน และรหัสผ่านลงฐานข้อมูล (รูปที่ 1)



รูปที่ 1 ตัวอย่างหน้าจอเข้าสู่ระบบของโปรแกรมแบบมีจุดอ้างอิงบนตารางกริด

เมื่อผู้เข้าร่วมการทดลองลงทะเบียนเสร็จเรียบร้อยแล้วก็จะทดลองพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่านที่ลงทะเบียน โดยเริ่มจากผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งานที่เป็นตัวอักษรและใส่รหัสผ่าน โดยการเลือกรูปภาพจำนวน 6 รูป ที่เป็นรหัสผ่านมาจัดวางลงในตารางกริดขนาด 5x5 โดยต้องวางตามตำแหน่งเหมือนกันกับขั้นตอนลงทะเบียน เมื่อใส่รหัสผ่านเสร็จก็ให้กดปุ่มเข้าสู่ระบบ ถ้าชื่อผู้ใช้งานและรหัสผ่านถูกต้องก็จะผ่านการพิสูจน์ตัวตนสามารถเข้าสู่ระบบได้สำเร็จ

และส่วนที่ 3 เมื่อผู้เข้าร่วมการทดลองทำการทดลองเสร็จจะใช้แบบสอบถามหลังการทดลองเก็บข้อมูลด้านความพึงพอใจในการใช้งานระบบที่ออกแบบจึงจะถือว่าทดลองเสร็จสิ้น

3. ผลการศึกษา

งานวิจัยนี้มีผู้เข้าร่วมการทดลองทั้งสิ้น 60 คน แบ่งเป็น 4 กลุ่มการทดลอง กลุ่มการทดลองละ 15 คน แบ่งเป็นเพศชาย 32 คน เพศหญิง 28 คน ผู้เข้าร่วมการทดลองส่วนใหญ่มีช่วงอายุระหว่าง 21-30 ปี (73.3 %) โดยส่วนใหญ่มีการศึกษาระดับปริญญาตรีจำนวน 54 คน (90 %) ระดับความถี่ในการใช้งานคอมพิวเตอร์จำนวน 54 คน ที่ใช้งานคอมพิวเตอร์ทุกวัน (75 %) ผู้เข้าร่วมการทดลองทุกคนเคยผ่านการใช้งานการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษร ในจำนวนนี้ 11 คน เคยใช้งานระบบการพิสูจน์ตัวตนด้วยการใช้รูปภาพเป็นรหัสผ่าน ส่วนพฤติกรรมการตั้งรหัสผ่าน จำนวน 47 คน ที่ตั้งรหัสผ่านเหมือนกันบางบัญชีและแตกต่างกันบางบัญชี (78.3 %) วิธีการเก็บรักษาการรหัสผ่านผู้เข้าร่วมการทดลองจำนวน 56 คน ใช้วิธีการจำ (93.3 %) และจำนวน 19 คน ใช้วิธีการจดบันทึกไว้ (31.7 %)

การวิเคราะห์ผลการทดลองด้านประสิทธิภาพการใช้งานและด้านความปลอดภัยจะใช้การวิเคราะห์

สถิติแบบมีพารามิเตอร์ (parametric) ประกอบด้วย การวิเคราะห์ความแปรปรวนแบบสองทาง (two-way ANOVA) การวิเคราะห์ความแปรปรวนแบบทางเดียว (one-way ANOVA) และการวิเคราะห์สถิติแบบไม่มีพารามิเตอร์ (non-parametric) เพื่อวิเคราะห์หาความแตกต่างของผลการทดลองดังนี้

3.1 การทดลองด้านประสิทธิภาพการใช้งาน

ผลการทดลองทั้ง 3 ครั้ง (หลังจากสร้างรหัสผ่านทันที หลังจากสร้างรหัสผ่าน 3 วัน และหลังจากสร้างรหัสผ่าน 15 วัน) สามารถนำมาวิเคราะห์สถิติเพื่อหาความแตกต่างของกลุ่มการทดลองในด้านประสิทธิภาพการใช้งานสามารถสรุปได้ดังตารางที่ 2

ตารางที่ 2 แสดงค่าเฉลี่ยของผลการทดลองด้านประสิทธิภาพการใช้งาน สามารถสรุปได้ว่าปัจจัยรูปแบบตาราง กริดไม่ได้ส่งผลต่อจำนวนครั้งที่ใช้พิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้พิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน ขณะที่รูปแบบการได้มาของรหัสผ่านกลับส่งผลต่อจำนวนครั้งที่ใช้พิสูจน์ตัวตนอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$) โดยรหัสผ่านที่ผู้ใช้สร้างเอง (mean = 2.14, S.D. = 2.025) จะมีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนน้อยกว่ารหัสผ่านที่ระบบสร้างให้ (mean = 3.93, S.D. = 2.312) ในด้านเวลาเฉลี่ยที่ใช้พิสูจน์ตัวตนก็ส่งผลอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$) โดยรหัสผ่านที่ผู้ใช้สร้างเอง (mean = 74.23, S.D. = 72.565) จะใช้จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนน้อยกว่ารหัสผ่านที่ระบบสร้างให้ (mean = 135.02, S.D. = 86.960) และความสำเร็จในการพิสูจน์ตัวตนก็ส่งผลอย่างมีนัยสำคัญทางสถิติเช่นเดียวกัน ($p < 0.05$) โดยรหัสผ่านที่ผู้ใช้สร้างเอง (80.00 %) มีความสำเร็จในการพิสูจน์ตัวตนมากกว่ารหัสผ่านที่ระบบสร้างให้ (46.67 %)

3.2 การทดลองด้านประสิทธิภาพความปลอดภัย

ตารางที่ 2 ค่าเฉลี่ยของผลการทดลองด้านประสิทธิภาพการใช้งาน

ปัจจัยที่ศึกษา	ค่าเฉลี่ยของผลการทดลองด้านประสิทธิภาพการใช้งาน											
	จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน (ครั้ง)				เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน (วินาที)				ความสำเร็จในการพิสูจน์ตัวตน (%)			
	วันแรก	3 วัน	15 วัน	เฉลี่ย	วันแรก	3 วัน	15 วัน	เฉลี่ย	วันแรก	3 วัน	15 วัน	เฉลี่ย
ตารางกริดแบบมีจุดอ้างอิง	1.87	3.43	3.53	2.94	66.77	131.83	120.80	106.47	83.33	53.33	56.67	65.56
ตารางกริดแบบไม่มีจุดอ้างอิง	2.00	3.47	3.93	3.13	74.47	133.70	100.20	102.79	83.33	53.33	46.67	61.11
P-value	0.786	0.958	0.461	0.590	0.645	0.941	0.225	0.759	0.786	0.955	0.599	3.778
ผู้ใช้สร้างรหัสผ่านเอง	1.33	2.43	2.67	2.14	40.90	106.97	74.83	74.23	93.33	73.33	70.00	80.00
ระบบสุ่มรหัสผ่านให้	2.53	4.47	4.80	3.93	100.33	158.57	146.17	135.02	73.33	33.33	33.33	46.67
P-value	0.013	0.001	0.000	0.000	0.000	0.045	0.000	0.000	0.013	0.001	0.000	0.000

ตารางที่ 3 ค่าเฉลี่ยของผลการทดลองด้านประสิทธิภาพความปลอดภัย

ปัจจัยที่ศึกษา	ค่าเฉลี่ยของผลการทดลองด้านประสิทธิภาพด้านการใช้งาน								
	จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน (ครั้ง)			เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน (วินาที)			ความสำเร็จในการพิสูจน์ตัวตน (%)		
	วันแรก	15 วัน	เฉลี่ย	วันแรก	15 วัน	เฉลี่ย	วันแรก	15 วัน	เฉลี่ย
ตารางกริดแบบมีจุดอ้างอิง	2.83	4.37	3.60	63.73	54.67	59.20	70.00	36.67	53.33
ตารางกริดแบบไม่มีจุดอ้างอิง	3.10	4.47	3.78	72.73	60.37	66.55	60.00	36.67	48.33
P-value	0.662	0.862	0.651	0.472	0.510	0.341	0.662	0.862	0.651
ผู้ใช้สร้างรหัสผ่านเอง	2.13	3.40	2.77	48.90	45.30	47.10	80.00	56.67	68.33
ระบบสุ่มรหัสผ่านให้	3.80	5.43	4.62	87.57	69.73	78.65	50.00	16.67	33.33
P-value	0.005	0.000	0.000	0.001	0.006	0.000	0.005	0.000	0.000

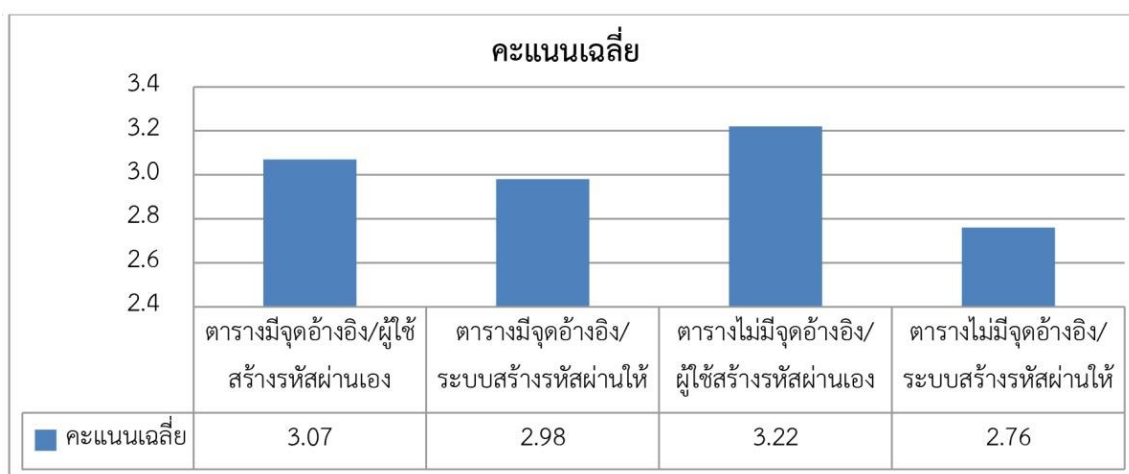
ผลการทดลองทั้ง 2 ครั้ง (หลังจากสร้างรหัสผ่านทันที และหลังจากสร้างรหัสผ่าน 15 วัน) สามารถนำมาวิเคราะห์ทางสถิติเพื่อหาความแตกต่างของกลุ่มการทดลองในด้านประสิทธิภาพการใช้งานได้

ดังตารางที่ 3

ตารางที่ 3 แสดงค่าเฉลี่ยของผลการทดลองด้านประสิทธิภาพความปลอดภัย สามารถสรุปได้ว่าปัจจัยรูปแบบตารางกริดไม่ได้ส่งผลต่อจำนวนครั้ง

ที่ใช้โครงกรรมพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้โครงกรรมพิสูจน์ตัวตน และความสำเร็จในการโครงกรรมพิสูจน์ตัวตน ขณะที่รูปแบบการได้มาของรหัสผ่านกลับส่งผลต่อจำนวนครั้งที่ใช้โครงกรรมพิสูจน์ตัวตนอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$) โดยรหัสผ่านที่ผู้ใช้สร้างเอง (mean = 2.77, S.D. = 2.280) จะมีจำนวนครั้งที่ใช้ในการโครงกรรมพิสูจน์ตัวตนน้อยกว่ารหัสผ่านที่ระบบสร้างให้ (mean = 4.62, S.D. = 2.108) ในด้านเวลาเฉลี่ยที่ใช้โครงกรรมพิสูจน์ตัวตนก็ส่งผลอย่างมี

นัยสำคัญทางสถิติ ($p < 0.05$) โดยรหัสผ่านที่ผู้ใช้สร้างเอง (mean = 47.10, S.D. = 29.546) จะใช้เวลาจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนน้อยกว่ารหัสผ่านที่ระบบสร้างให้ (mean = 78.65, S.D. = 46.779) และความสำเร็จในการพิสูจน์ตัวตนก็ได้ผลกระทบบอย่างมีนัยสำคัญทางสถิติเช่นเดียวกัน ($p < 0.05$) โดยรหัสผ่านที่ผู้ใช้สร้างเอง (68.33 %) มีความสำเร็จในการพิสูจน์ตัวตนมากกว่ารหัสผ่านที่ระบบสร้างให้ (33.33 %)



รูปที่ 2 ค่าสถิติของความพึงพอใจเฉลี่ยที่ผู้ใช้มีต่อระบบของแต่ละกลุ่มการทดลอง ชี้ให้เห็นว่ากลุ่มที่ผู้เข้าร่วมการทดลองสร้างรหัสผ่านบนตารางกริดแบบไม่มีจุดอ้างอิงและผู้เข้าร่วมการทดลองสร้างรหัสผ่านเองมีค่าเฉลี่ยความพึงพอใจสูงสุด ขณะที่กลุ่มการทดลองที่สร้างรหัสผ่านบนตารางกริดแบบไม่มีจุดอ้างอิงและระบบสร้างรหัสผ่านให้ค่าเฉลี่ยความพึงพอใจน้อยสุด

3.3 ความถี่ของการเลือกวางตำแหน่งรูปภาพบนตารางกริด

ในส่วนนี้จะกล่าวถึงการวิเคราะห์ตำแหน่งบนตารางที่ถูกเลือกใช้เพื่อวางรูปภาพรหัสผ่านแยกตามปัจจัยการใช้ตารางกริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิง และปัจจัยการได้มาของรหัสผ่านแบบผู้ใช้สร้างเองกับระบบสร้างรหัสผ่านให้เพื่อชี้ให้เห็นถึงการกระจายตัวของการสร้างรหัสผ่าน ดังตารางที่ 4 - 8

ตารางที่ 4 แสดงข้อมูลร้อยละของการเลือกตำแหน่งบนตารางกริดทุกกลุ่มการทดลอง ชี้ให้เห็นว่าผู้เข้าร่วมการทดลองมีแนวโน้มในการเลือกตำแหน่งมุมของตารางและตรงกลางของตารางในการสร้างรหัสผ่าน โดยตำแหน่งที่อยู่มุมบนซ้ายของตารางจะถูกเลือกใช้มากที่สุด (73.33 %) รองลงมาคือมุมล่างขวา (56.67 %) และอันดับสามคือมุมบนขวากับตำแหน่งกึ่งกลางของตาราง (43.33 %)

ตารางที่ 4 ข้อมูลร้อยละของการเลือกตำแหน่งบน
ตารางกริดทุกกลุ่มการทดลอง

73.33	38.33	10.00	21.67	43.33
11.67	35.00	11.67	18.33	13.33
13.33	15.00	43.33	16.67	10.00
10.00	15.00	20.00	23.33	6.67
41.67	13.33	11.67	26.67	56.67

ตารางที่ 5 ข้อมูลร้อยละของการเลือกตำแหน่งบน
ตารางกริดที่มีจุดอ้างอิง

70.00	36.67	13.33	30.00	50.00
10.00	26.67	10.00	23.33	23.33
10.00	6.67	33.33	16.67	6.67
13.33	20.00	16.67	16.67	6.67
46.67	16.67	10.00	23.33	63.33

ตารางที่ 6 ข้อมูลร้อยละของการเลือกตำแหน่งบน
ตารางกริดที่ไม่มีจุดอ้างอิง

76.67	40.00	6.67	13.33	36.67
13.33	43.33	13.33	13.33	3.33
16.67	23.33	53.33	16.67	13.33
6.67	10.00	23.33	30.00	6.67
36.67	10.00	13.33	30.00	50.00

ตารางที่ 7 ข้อมูลร้อยละของการเลือกตำแหน่งบน
ตารางกริดที่ผู้เข้าร่วมการทดลองสร้าง
รหัสผ่านเอง

73.33	43.33	6.67	16.67	33.33
13.33	53.33	10.00	23.33	10.00
10.00	13.33	53.33	20.00	13.33
0.00	16.67	23.33	33.33	0.00
13.33	6.67	16.67	40.00	56.67

ตารางที่ 5 แสดงข้อมูลร้อยละของการเลือกตำแหน่งบนตารางกริดที่มีจุดอ้างอิง ซึ่งชี้ให้เห็นว่าผู้เข้าร่วมการทดลองมีแนวโน้มในการเลือกตำแหน่งมุมของตารางในการสร้างรหัสผ่าน โดยตำแหน่งที่อยู่มุมบนซ้ายของตารางจะถูกเลือกใช้มากที่สุด (70.00 %) รองลงมาคือมุมล่างขวา (63.33 %) และอันดับสามคือมุมบนขวา (43.33 %)

ตารางที่ 6 แสดงข้อมูลร้อยละของการเลือกตำแหน่งบนตารางกริดที่ไม่มีจุดอ้างอิง ซึ่งชี้ให้เห็นว่า

ผู้เข้าร่วมการทดลองมีแนวโน้มในการเลือกตำแหน่งมุมและตำแหน่งกึ่งกลางของตารางในการสร้างรหัสผ่าน โดยตำแหน่งที่อยู่มุมบนซ้ายของตารางจะถูกเลือกใช้มากที่สุด (76.67 %) รองลงมาคือตำแหน่งกึ่งกลางของตาราง (53.33 %) และอันดับสามคือมุมล่างขวา (50.00 %)

ตารางที่ 7 แสดงข้อมูลร้อยละของการเลือกตำแหน่งบนตารางกริดที่ผู้เข้าร่วมการทดลอง

สร้างรหัสผ่านเอง ซึ่งให้เห็นว่าผู้เข้าร่วมการทดลองมีแนวโน้มในการเลือกตำแหน่งมุมและตำแหน่งกึ่งกลางของตารางลักษณะทแยงมุมบนซ้ายไปยังมุมล่างขวาในการสร้างรหัสผ่าน โดยตำแหน่งที่อยู่มุมบนซ้ายของตารางจะถูกเลือกใช้มากที่สุด (73.33 %) รองลงมาคือตำแหน่งมุมล่างขวา (56.67 %) และอันดับสามคือตำแหน่งกึ่งกลางของตารางและตำแหน่งระหว่างมุมบนซ้ายกับกึ่งกลาง (53.33 %)

ตารางที่ 8 ข้อมูลร้อยละของการเลือกตำแหน่งบนตารางกริดที่ผู้เข้าร่วมการทดลองได้รับรหัสผ่านจากระบบ

73.33	33.33	13.33	26.67	53.33
10.00	16.67	13.33	13.33	16.67
16.67	16.67	33.33	13.33	6.67
20.00	13.33	16.67	13.33	13.33
70.00	20.00	6.67	13.33	56.67

ตารางที่ 8 แสดงข้อมูลร้อยละของการเลือกตำแหน่งบนตารางกริดที่ผู้เข้าร่วมการทดลองได้รับรหัสผ่านจากระบบ ซึ่งให้เห็นว่าผู้เข้าร่วมการทดลองมีแนวโน้มในการเลือกตำแหน่งมุมและตำแหน่งกึ่งกลางของตารางในการสร้างรหัสผ่าน โดยตำแหน่งที่อยู่มุมบนซ้ายของตารางจะถูกเลือกใช้มากที่สุด (73.33 %) รองลงมาคือตำแหน่งมุมล่างซ้าย (70.00 %) และอันดับสามคือตำแหน่งมุมล่างขวาของตาราง (56.67 %)

4. อภิปรายผลและวิจารณ์

งานวิจัยนี้ได้ใช้เทคนิคการมีจุดอ้างอิงบนตารางกริดเข้ามาใช้ประกอบการออกแบบรหัสผ่าน ซึ่งสอดคล้องกับงานวิจัยที่นำเอาจุดอ้างอิงมาใช้เป็นจุดช่วยจำเพื่อให้ผู้ใช้สามารถจำรหัสผ่านได้ง่ายขึ้นและเพิ่มประสิทธิภาพด้านการใช้งาน [3,4] ลักษณะของจุดอ้างอิงที่ใช้จะเป็นลักษณะที่สามารถนำมาเกี่ยวข้องกับการสร้างรหัสผ่านในเชิงความหมายได้ ประกอบกับการสร้างรหัสผ่านเป็นลักษณะการวาดลงบนตารางจึงอาจเป็นอีกสาเหตุหนึ่งที่ทำให้ผู้ใช้สามารถใช้ประโยชน์จากจุดอ้างอิงได้อย่างมีประสิทธิภาพ แต่ในงานวิจัยนี้ลักษณะของการสร้างรหัสผ่านเป็นการนำเอารูปภาพมาวางบนตารางกริด ซึ่งการจะสร้างรหัสผ่านให้มีความเกี่ยวข้องกับจุดอ้างอิงบนตารางในเชิงความหมายนั้นอาจทำให้ยาก จึงอาจเป็นสาเหตุให้ผู้ใช้ไม่สามารถใช้ประโยชน์จากจุดช่วยจำได้เท่าที่ควร ดังนั้นงานวิจัยนี้แสดงให้เห็นว่าปัจจัยรูปแบบตารางกริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิงไม่ได้ส่งผลต่อประสิทธิภาพการใช้งานโปรแกรมพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแตกต่างกัน

ในด้านความถี่ของตำแหน่งบนตารางที่ถูกเลือกใช้พบว่าโดยส่วนใหญ่ผู้เข้าร่วมการทดลองมีแนวโน้มเลือกตำแหน่งที่อยู่มุมตารางและตำแหน่งตรงกลางโดยมุมบนซ้ายเป็นตำแหน่งที่ถูกเลือกใช้มากที่สุด (73.33 %) อย่างไรก็ตาม แนวโน้มการเลือกตำแหน่งส่วนใหญ่ของผู้เข้าร่วมการทดลองสามารถสรุปได้เป็น 2 รูปแบบใหญ่ คือ แบบตำแหน่งมุมร่วมกับตำแหน่งกึ่งกลางของตาราง และแบบแนวทแยงมุมจากมุมบนซ้ายไปยังมุมล่างขวาร่วมกับตำแหน่งมุมตาราง ทั้งสองรูปแบบอาจจะเป็นตำแหน่งที่สามารถจดจำได้ง่ายส่งผลให้การเลือกตำแหน่งของผู้เข้าร่วมการทดลองมีรูปแบบออกมาอย่างชัดเจน เพราะฉะนั้นหากต้องการยกระดับความปลอดภัยด้วยการใช้ตารางกริดที่มีขนาดใหญ่ขึ้นอาจจะช่วยเพิ่มการป้องกันการโจรกรรมได้ไม่มากนัก ขณะ

เดียวกันการมีรูปแบบที่ชัดเจนอาจจะส่งผลต่อการโจรกรรมรหัสผ่านที่นักโจรกรรมสามารถคาดเดาตำแหน่งเหล่านี้ได้ง่ายขึ้นเช่นกัน

ในด้านข้อเสนอแนะของผู้เข้าร่วมการทดลองที่เห็นตรงกันมากที่สุดคือการลดรายละเอียดของภาพลงเนื่องจากรูปที่ใช้มีรายละเอียดมากเกินไปทำให้จำสับสนและควรเลือกใช้รูปภาพที่มีความแตกต่างอย่างชัดเจน ส่วนความเห็นอื่นๆ เช่น การมีข้อได้รูป การใช้ภาพที่มีขนาดใหญ่และชัดเจนกว่านี้

รหัสผ่านรูปภาพในปัจจุบันมีการศึกษาวิจัยหลากหลายรูปแบบเพื่อจุดประสงค์นำมาใช้ในการพิสูจน์ตัวตน และในปัจจุบันรหัสผ่านรูปภาพก็เริ่มมีบทบาทมากขึ้นดังจะเห็นได้จากเทคโนโลยีที่ใช้งานในชีวิตประจำวันไม่ว่าจะเป็นบนอุปกรณ์สมาร์ตโฟนที่ใช้ระบบปฏิบัติการแอนดรอยด์ (Android) ที่มีการใช้รหัสผ่านรูปภาพเช่นกัน

5. สรุปผลการศึกษา

งานวิจัยนี้ได้ศึกษาปัจจัยที่ส่งผลต่อประสิทธิภาพการใช้งาน ความปลอดภัย และความพึงพอใจที่ผู้ใช้มีต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพบนตารางกริด โดยปัจจัยที่ใช้ในการศึกษาประกอบด้วยปัจจัยรูปแบบตาราง กริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิงบนตารางกริด และปัจจัยการได้มาของรหัสผ่านแบบผู้ใช้สร้างรหัสผ่านเองกับระบบสร้างรหัสผ่านให้ จากผลการทดลองสามารถสรุปได้ดังนี้

5.1 ด้านประสิทธิภาพการใช้งานพบว่ารูปแบบตารางกริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิงไม่ได้ส่งผลต่อจำนวนครั้ง เวลาเฉลี่ย และความสำเร็จที่ใช้พิสูจน์ตัวตนแตกต่างกัน ขณะที่รูปแบบการได้มาของรหัสผ่านแบบผู้ใช้สร้างเองกับแบบระบบสร้างรหัสผ่านให้กลับส่งผลต่อจำนวนครั้ง เวลาเฉลี่ย และความสำเร็จในการพิสูจน์ตัวตนแตกต่างกัน โดยรหัสผ่านที่

ผู้ใช้สร้างเองส่งผลให้ผู้เข้าร่วมการทดลองใช้จำนวนครั้ง และเวลาเฉลี่ยในการพิสูจน์ตัวตนน้อยกว่ารหัสผ่านที่ได้รับจากระบบ รหัสผ่านที่ผู้ใช้สร้างเอง (80.00 %) จะมีอัตราความสำเร็จในการพิสูจน์ตัวตนสูงกว่ารหัสผ่านที่ได้รับจากระบบ (46.67 %)

5.2 ด้านประสิทธิภาพความปลอดภัยพบว่ารูปแบบตารางกริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิงไม่ได้ส่งผลต่อจำนวนครั้ง เวลาเฉลี่ย และความสำเร็จที่ใช้โจรกรรมพิสูจน์ตัวตนแตกต่างกัน ขณะที่รูปแบบการได้มาของรหัสผ่านแบบผู้ใช้สร้างเองกับแบบระบบสร้างรหัสผ่านให้กลับส่งผลต่อจำนวนครั้ง เวลาเฉลี่ย และความสำเร็จในการโจรกรรมพิสูจน์ตัวตนแตกต่างกัน โดยรหัสผ่านที่ผู้ใช้สร้างเองส่งผลให้ผู้เข้าร่วมการทดลองใช้จำนวนครั้งและเวลาเฉลี่ยในการโจรกรรมพิสูจน์ตัวตนน้อยกว่ารหัสผ่านที่ได้รับจากระบบ และรหัสผ่านที่ผู้ใช้สร้างเอง (68.33 %) สร้างอัตราความสำเร็จในการโจรกรรมพิสูจน์ตัวตนสูงกว่ารหัสผ่านที่ได้รับจากระบบ (33.33 %)

5.3 ด้านความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อการใช้ระบบพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพบนตารางกริด ใช้แบบสอบถามหลังจากทดลองครั้งแรกที่ผู้ใช้เข้าร่วมการทดลองลงทะเบียนสร้างรหัสผ่าน ผลการวิเคราะห์พบว่าปัจจัยการได้มาของรหัสผ่านแบบผู้ใช้สร้างรหัสผ่านเองส่งผลต่อความพึงพอใจระบบมากกว่ารหัสผ่านที่ระบบสร้างให้ ขณะที่ปัจจัยการใช้ตารางกริดแบบมีจุดอ้างอิงกับไม่มีจุดอ้างอิงไม่ได้ส่งผลต่อความพึงพอใจที่ผู้ใช้มีต่อระบบในด้านของอิทธิพลร่วมของทั้ง 2 ปัจจัย ก็พบว่าไม่ส่งผลต่อคะแนนความพึงพอใจที่ผู้ใช้มีต่อระบบเช่นกัน จากผลการวิเคราะห์ความพึงพอใจของผู้เข้าร่วมการทดลองสามารถสรุปโดยรวมได้ว่าผู้ใช้เข้าร่วมการทดลองมีความพึงพอใจมากกับระบบรหัสผ่านรูปภาพแบบกริด

6. แนวทางการวิจัยในอนาคต

6.1 ทดลองกับผู้เข้าร่วมการทดลองในระยะเวลานานขึ้นเพื่อวิเคราะห์ประสิทธิภาพในระยะยาว

6.2 พัฒนาวิธีการป้องกันการสร้างรหัสผ่านที่ผู้เข้าร่วมการทดลองมีแนวโน้มในการสร้างรหัสผ่านที่มีรูปแบบการวางที่ชัดเจนในด้านความปลอดภัยจากการคาดเดาได้ง่าย ได้แก่ ในตำแหน่งที่คาดเดาง่ายใช้เทคนิคการทำให้ภาพโปร่งแสงมากกว่าตำแหน่งอื่นเป็นต้น

6.3 การใช้จุดอ้างอิงบนตารางกริดที่เป็นรูปแบบอื่นนอกจากจุดสีดำ เช่น การใช้ภาพวัตถุที่มีความหมายที่สามารถนำมาเกี่ยวข้องกับการสร้างรหัสผ่าน

7. รายการอ้างอิง

- [1] Adams, A. and Sasse, M.A., 1999, Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures, Commun. ACM 42: 41-46.
- [2] Feldmeier, D. and Karn, P., 1989, UNIX password security-ten years later, pp. 44-63, In Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology.
- [3] Suo, X., Zhu, Y. and Owen, G.S., 2005, Graphical passwords: A survey, pp. 463-472, In Proceedings of the 21st Annual Computer Security Applications Conference.
- [4] Blonder, G.E., 1996, Graphical Passwords, pp. 216-220, In Bower, G.H., Karlin, M.B. and Dueck, A. (Eds.), 1975, Comprehension and Memory for Pictures: Memory and Cognition 3, Lucent Technologies, Inc., New Jersey.
- [5] Lashkari, A.H., 2010, A New Algorithm for Graphical User Authentication Based on Rotation and Resizing, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur.
- [6] Dhamija, R. and Perrig, A., 2000, Déjà vu: A User Study Using Images for Authentication, In Proceedings of 9th USENIX Security Symposium.
- [7] Passfaces Corporation, A Real User, Available Source: <http://www.realuser.com>, August 1, 2013,
- [8] Farnaz, T., Maslin, M. and Azizah, A.M., 2013, An enhancement on Passface graphical password authentication, J. Basic Appl. Sci. Res. 3: 135-141.
- [9] วชิรินทร์ มธรรสพงศ์พันธ์ และณัฐชนน หงส์วริทธิ์ธร, 2556, การศึกษาปัจจัยที่มีอิทธิพลต่อการใช้งานได้และความปลอดภัยของรหัสผ่านแบบการ์ดตูน, ว.เทคโนโลยีสารสนเทศ 9(1): 24-33.
- [10] อนุพงศ์ อธิวงค์วิวัฒน์ และณัฐชนน หงส์วริทธิ์ธร, 2556, งานวิจัยเชิงสำรวจถึงปัจจัยในการออกแบบรหัสผ่านรูปภาพแบบกริด, น. 462-471, การประชุมวิชาการเสนอผลงานวิจัยระดับบัณฑิตศึกษาแห่งชาติครั้งที่ 29, มหาวิทยาลัยแม่ฟ้าหลวง, เชียงราย.
- [11] เจริญ ตูลย์ราชันชัย และณัฐชนน หงส์วริทธิ์ธร, 2556, การศึกษาจนวนภาพที่ระลึกได้ที่มีการ

- แสดงภาพแบบเรียงแถวและแบบตาราง, น. 472-480, การประชุมวิชาการเสนอผลงานวิจัยระดับบัณฑิตศึกษาแห่งชาติครั้งที่ 29, มหาวิทยาลัยแม่ฟ้าหลวง, เชียงราย.
- [12] เกรียงไกร มะโนใจ และณัฐรณนธ์ หงส์วิทธิ์ธร, 2556, อิทธิพลของรูปแบบกริดและรูปแบบภาพที่มีต่อการจดจำรูปภาพ, น. 453-461, การประชุมวิชาการเสนอผลงานวิจัยระดับบัณฑิตศึกษาแห่งชาติครั้งที่ 29, มหาวิทยาลัยแม่ฟ้าหลวง, เชียงราย.
- [13] Tao, H. and Adams, C., 2006, Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Network Security 7: 273-292.
- [14] Lin, D., Dunphy, P., Olivier, P. and Yan, J., 2007, "Background-DAS": Do background images improve "Draw a Secret" graphical passwords?", 14th ACM Conference on Computer and Communications Security, Alexandria, Virginia.
- [15] Partha, P.R., 2012, Ray's scheme: Graphical password based hybrid authentication system for smart hand held devices, Int. J. Comp. Trends Technol. 3: 235-241.
- [16] Majid, A., Douglas, S. and Behzad, M., 2013, Usability and Security of Gaze-Based Graphical Grid Passwords, , pp. 17-33, Lecture Notes in Computer Science [Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers], Springer, Okinawa, Japan.