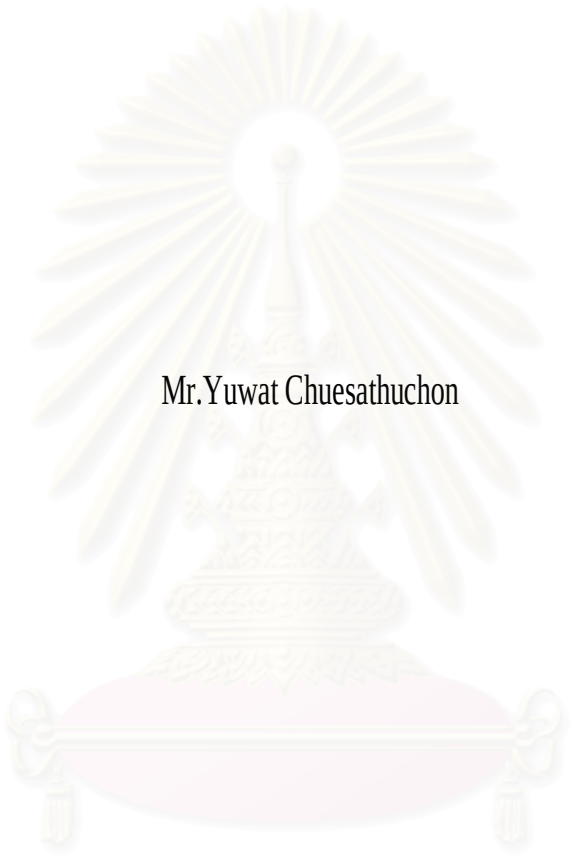
การออกแบบและพัฒนาซอฟต์แวร์รหัสผ่านแบบรูปภาพโดยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง

นายยุวัฒน์ เชื้อสาธุชน

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

THE DESIGN AND DEVELOPMENT OF VISUAL PASSWORD SOFTWARE USING CHALLENGE-RESPONSE AUTHENTICATION

Mr.Yuwat Chuesathuchon



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2007

หัวข้อวิทยานิพนธ์	การออกแบบและพัฒนาซอฟต์แวร์รหัสผ่านแบบรูปภาพโดยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง
โดย	นายยุวัฒน์ เชื้อสาธุชน
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ธงชัย โรจน์กังสดาล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... อาจารย์ที่ปรึกษา
(อาจารย์ ธงชัย โรจน์กังสดาล)

..... กรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.เฉลิมเอก อินทนากรวิวัฒน์)

ยุวัฒน์ เชื้อสาธุชน : การออกแบบและพัฒนาซอฟต์แวร์รหัสผ่านแบบรูปภาพโดยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง. (THE DESIGN AND DEVELOPMENT OF VISUAL PASSWORD SOFTWARE USING CHALLENGE-RESPONSE AUTHENTICATION) อ. ที่ปรึกษา : อ. ธงชัย โรจน์กังสดาล, 89 หน้า.

การพิสูจน์ตัวตนแบบรหัสผ่านเป็นสิ่งที่ใช้ในชีวิตประจำวัน แต่มีปัญหาเรื่องการจดจำ การพิสูจน์ตัวตนแบบรูปภาพจึงถูกนำมาใช้ เนื่องจากการศึกษาพบว่ามนุษย์สามารถจดจำรูปภาพได้ดีกว่าตัวอักษร การพิสูจน์ตัวตนแบบรูปภาพแบ่งออกเป็น 2 ประเภทตามลักษณะการพิสูจน์ตัวตนคือ เทคนิคการวิเคราะห์และเทคนิคการกระทำซ้ำ งานวิจัยชิ้นนี้เป็นแบบเทคนิคการวิเคราะห์ ลักษณะของเทคนิคการวิเคราะห์คือผู้ใช้ต้องทำการวิเคราะห์และเลือกรูปภาพจากชุดรูปภาพให้ถูกต้อง โดยในแต่ละรอบของการพิสูจน์ตัวตน คำตอบที่ได้ไม่จำเป็นต้องเหมือนกัน ขึ้นอยู่กับการวิเคราะห์ของผู้ใช้ นอกจากนี้ในงานวิจัยยังใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองร่วมด้วย ลักษณะการพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองคือ มีการโต้ตอบกันระหว่างสองฝั่ง ฝั่งแรกทำการส่งคำถามท้าทาย ฝั่งที่สองต้องทำการตอบสนองให้ถูกต้อง สำหรับงานวิจัยนี้มีลักษณะการทำงานคือ ผู้ใช้ทำการลงทะเบียนเลือกคำสำคัญของตนเองจากฐานข้อมูล แต่ละคำประกอบไปด้วยภาพประจำคำสำคัญซึ่งมีลักษณะบ่งบอกถึงคำสำคัญนั้นประมาณ 4 รูป ในการพิสูจน์ตัวตน ซอฟต์แวร์ทำการสุ่มรูปภาพและคำถามท้าทายอย่างละ 1 ชุด ภายในรูปภาพสุ่มจะมีรูปภาพของผู้ใช้ปนอยู่ สิ่งที่ผู้ใช้ต้องทำคือ การเลือกรูปภาพจากชุดภาพสุ่มตามลักษณะของคำถามท้าทายให้ถูกต้อง การพิสูจน์ตัวตนจะเสร็จสมบูรณ์

ภาควิชา.....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต.....
สาขาวิชา...วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา.....2550.....

4870382021: MAJOR COMPUTER SCIENCE
KEY WORD: SECURITY / VISUAL PASSWORD / CHALLENGE-RESPONSE AUTHENTICATION

YUWAT CHUESATHUCHON : THE DESIGN AND DEVELOPMENT OF VISUAL PASSWORD SOFTWARE USING CHALLENGE-RESPONSE AUTHENTICATION. THESIS ADVISOR : THONGCHAI ROJKANGSADAN, 89 pp.

Password authentication is necessary in our life, but a lot of users have trouble memorizing passwords. Visual passwords come to solve this problem. According to research, human can remember image better than text. There are two techniques of visual passwords which are recognition-based and recall-based. This research is recognition-based where the user has to recognize his correct images in a set. For this type of authentication, the behavior is that the ordering of the authentication answer does not have to be the same in each trial. It depends on the user's recognition. Challenge-response authentication is incorporated in this research. The behavior is the response between two parties: one challenge with a question and the other must respond with a correct answer. In this research, the authentication process starts with the user choosing and registering his keywords from the database. Each keyword consists of four images. Next, in the authentication phase, the software randomizes and creates an image set and challenges the user with a question for authentication. The image set contains both the user's images and random images. The authentication completes when the user selects the correct image pattern with respect to the challenge question.

Department……Computer Engineering…...Student's Signature.....
Field of Study……Computer Science.....Advisor's Signature.....
Academic Year.....2007.....

กิตติกรรมประกาศ

ขอบคุณอาจารย์ธงชัย โรจน์กังสดาล อาจารย์ที่ปรึกษาวิทยานิพนธ์ของข้าพเจ้าที่ทำให้วิทยานิพนธ์นี้สำเร็จลุลวงไปด้วยดี แนวคิด และ คำแนะนำของอาจารย์ช่วยให้วิทยานิพนธ์นี้ขับเคลื่อนไปข้างหน้าด้วยความสม่ำเสมอ ขอบคุณอาจารย์ที่ช่วยดูแลข้าพเจ้ามาตลอดระยะเวลา 3 ปี สิ่งใดที่ข้าพเจ้ากระทำผิดต่ออาจารย์ไว้ข้าพเจ้ากราบขออภัย กราบขอบพระคุณอาจารย์เป็นอย่างสูงไว้ ณ ที่นี้ด้วย

กราบขอบพระคุณ อาจารย์ ดร.ยรรยง เต็งอำนวย ประธานกรรมการสอบ อาจารย์จารุมาตร ปิ่นทอง และอาจารย์ ดร.เฉลิมเอก อินทนากรวิวัฒน์ กรรมกการสอบของข้าพเจ้าที่กรุณาได้ให้คำแนะนำทำให้งานวิจัยชิ้นนี้ถูกต้องและสมบูรณ์มากยิ่งขึ้น ขอกราบขอบพระคุณอาจารย์ทุกท่านไว้ ณ ที่นี้

ขอขอบพระคุณอาจารย์ทุกท่านที่ได้ให้ความรู้แก่ข้าพเจ้า ทั้งในเรื่องการเรียน ทั้งในเรื่องชีวิต นับเป็นสิ่งล้ำค่ามากสำหรับข้าพเจ้า ข้าพเจ้าจะนำความรู้ต่างๆที่ท่านอาจารย์ได้สอนไปใช้ให้เกิดประโยชน์สูงสุดในชีวิตประจำวันต่อไป

ขอบคุณนิสิตวิชา Computer Security ภาคต้นปี 2550 ที่ตั้งใจรับฟังงานวิทยานิพนธ์ของข้าพเจ้าพร้อมทั้งให้คำแนะนำ แนวคิดอีกเป็นจำนวนมาก ทำให้งานวิจัยชิ้นนี้เปี่ยมไปด้วยมิตรภาพที่อบอุ่น

ขอบคุณ เอย ที่คอยผลักดันให้ข้าพเจ้าทำวิทยานิพนธ์สำเร็จลุล่วงได้ทันเวลา

ขอบคุณ เอ และพี่กฤดิสำหรับคำปรึกษาดีๆในเรื่องสถิติและการทำกราฟ

ขอบคุณ อร และเอกเทศ สำหรับคำช่วยเหลือทางด้านภาษาอังกฤษที่ยอดเยี่ยม

ขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ ที่หอพักที่ทำให้ชีวิตในระดับปริญญาโทเต็มไปด้วยเสียงหัวเราะและมิตรภาพที่อบอุ่นด้วยดีเสมอมา

ขอขอบพระคุณ คุณพ่อ คุณแม่ที่เข้าใจข้าพเจ้า และคอยสนับสนุนข้าพเจ้าไม่ว่าข้าพเจ้าจะทำอะไร คุณความดีของวิทยานิพนธ์ฉบับนี้ ขอมอบเป็นเครื่องบูชาคุณบิดา มารดา ไว้ ณ โอกาสนี้

สารบัญ

หน้า

หน้า

หน้า

ภาพประกอบ หน้า

ภาพประกอบ หน้า

ภาพประกอบ หน้า

สารบัญตาราง

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน ระบบการพิสูจน์ตัวตน (Authentication) ที่มีการใช้งานอย่างแพร่หลายคือ รหัสผ่าน (Password) เนื่องจากไม่จำเป็นต้องใช้อุปกรณ์อื่นเพิ่มเติม แต่ปัญหาที่เกิดขึ้นก็คือ รหัสผ่านที่จดจำได้ง่ายนั้น ส่วนใหญ่เป็นรหัสผ่านที่ไม่ปลอดภัย คือสามารถถูกคาดเดาหรือโจมตีจากทางผู้ไม่ประสงค์ดีได้ง่าย ส่วนรหัสผ่านที่ดีก็มีปัญหาในการจดจำ จนในบางครั้งส่งผลให้ผู้ใช้งานต้องจดรหัสผ่านลงในกระดาษ ซึ่งเป็นสิ่งที่ไม่สมควรทำอย่างยิ่งในแง่ของความปลอดภัย

รหัสผ่านแบบรูปภาพจึงถูกนำมาใช้เพื่อช่วยแก้ไขปัญหาในเรื่องความจำของมนุษย์ เพราะจากการศึกษาพบว่ามนุษย์สามารถจดจำรูปภาพได้ดีกว่าตัวอักษร งานวิจัยด้านรหัสผ่านแบบรูปภาพในปัจจุบันแบ่งออกเป็น 2 กลุ่มตามลักษณะการพิสูจน์ตัวตน คือเทคนิคการวิเคราะห์ (Recognition Based) และเทคนิคการกระทำซ้ำ (Recall Based) แต่ถ้าผู้ใช้ใช้แต่เพียงรูปภาพเพียงอย่างเดียว จากขนาดของรูปภาพที่ใหญ่กว่าตัวอักษรตามอัตราส่วนและหน้าจอคอมพิวเตอร์ซึ่งตั้งอยู่ในลักษณะเกือบตั้งฉากจึงสามารถมองเห็นได้ง่ายจากระยะไกล การโจมตีแบบมองข้ามไหล่ (Shoulder Surfing) จึงสามารถกระทำได้โดยง่าย

นอกจากนี้ปัญหาสปายแวร์ก็กำลังระบาดหนัก เพราะมีอินเตอร์เน็ตเป็นช่องทางการแพร่เชื้อที่สะดวกสบาย ความสามารถของสปายแวร์ก็ถูกพัฒนาให้สูงขึ้น ไม่ว่าจะเป็นการดักแป้นพิมพ์ การดักตำแหน่งการเคลื่อนไหวหรือการกดของเมาส์ การถ่ายภาพหน้าจอ หรือแม้กระทั่งการแสดงภาพหน้าจอของเป้าหมายแบบทันทีทันใด การนำวิธีพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง (Challenge-response authentication) มาร่วมใช้งานด้วยจึงเกิดขึ้น

งานวิจัยชิ้นนี้ผู้ใช้จะมีชุดคำสำคัญ (Keyword) ของตัวเองเพื่อใช้ในการพิสูจน์ตัวตน โดยซอฟต์แวร์จะทำการแสดงรูปภาพมาชุดหนึ่งและแสดงคำถามท้าทาย 1 คำถาม (Challenge) ผู้ใช้ทำการตอบสนองโดยเลือกรูปภาพตามคำสั่งนั้นให้ถูกต้อง (Response) ถือว่าผ่านการพิสูจน์ตัวตน

1.2 วัตถุประสงค์ของการวิจัย

ออกแบบและพัฒนาซอฟต์แวร์รหัสผ่านแบบรูปภาพโดยนำเอาการพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองมาใช้ร่วมก่อให้เกิดความปลอดภัยมากขึ้นต่อสปายแวร์ การโจมตีจากพจนานุกรม และ การโจมตีแบบมองข้ามไหล่ สามารถเลือกระดับความปลอดภัยได้

1.3 ขอบเขตของการวิจัย

1.3.1 มีคำสำคัญในระบบ 1000 คำ

1.3.2 มีระดับความปลอดภัย 3 ระดับ

- ระดับต่ำ – คำสำคัญส่วนตัว 4 คำ
- ระดับกลาง – คำสำคัญส่วนตัว 6 คำ
- ระดับสูง – คำสำคัญส่วนตัว 8 คำ

1.3.3 มีคำถามท้าทาย 7 คำถาม

- เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกติดกัน 1 ตำแหน่ง
- เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกไม่ติดกันเลย
- เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกติดกัน 1 ตำแหน่ง
- เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกไม่ติดกันเลย
- เลือกรูปภาพส่วนตัวทั้งหมดโดยต้องมีอยู่ทั้งสองแถว
- ไม่เลือกรูปภาพส่วนตัว 1 รูป
- ไม่เลือกรูปภาพส่วนตัว 2 รูป

1.4 ขั้นตอนการวิจัย

1.4.1 ศึกษางานวิจัยของรหัสผ่านแบบรูปภาพและการพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง

1.4.2 ออกแบบซอฟต์แวร์รหัสผ่านแบบรูปภาพโดยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง

1.4.3 สร้าง ทดสอบและปรับปรุงซอฟต์แวร์ตามความเหมาะสม

1.4.4 สรุปผลการวิจัยและจัดทำรายงานวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ซอฟต์แวร์รหัสผ่านแบบรูปภาพที่สามารถใช้งานได้ง่าย

1.5.2 เพื่อเป็นแนวทางในการพัฒนาระบบรหัสผ่านแบบรูปภาพต่อไป

1.5.3 ช่วยลดปัญหาการโจมตีเช่น การโจมตีแบบมองข้ามไหล่ การโจมตีโดยใช้พจนานุกรม การดักข้อมูลภายในเครื่องของสปายแวร์เป็นต้น

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

2.1.1 รหัสผ่านแบบรูปภาพ (Visual Password)

รหัสผ่านแบบรูปภาพ [1] ถูกนำเสนอขึ้นมาเนื่องจากการศึกษาพบว่ามนุษย์มีความสามารถในการจดจำรูปภาพได้มหาศาล [2][3] ในการทดลองมนุษย์สามารถจดจำและวิเคราะห์รูปภาพได้จำนวนตั้งแต่ร้อยถึงพันรูปได้ [4][5] และการจดจำรูปภาพของมนุษย์มีประสิทธิภาพมากกว่าการจดจำตัวอักษร [6] ในปัจจุบันรหัสผ่านแบบรูปภาพแบ่งตามเทคนิคที่ใช้ได้เป็น 2 กลุ่มคือ

1. **เทคนิคการวิเคราะห์** (Recognition Based) วิธีการคือแสดงรูปภาพขึ้นมาจำนวนหนึ่งโดยจะมีรูปภาพที่ผู้ใช้ได้เลือกไว้ก่อนผสมอยู่ด้วย การพิสูจน์ตัวตนจะเสร็จสมบูรณ์ถ้าหากว่าผู้ใช้สามารถเลือกรูปภาพของตัวเองได้ครบขั้นตอนที่กำหนดไว้

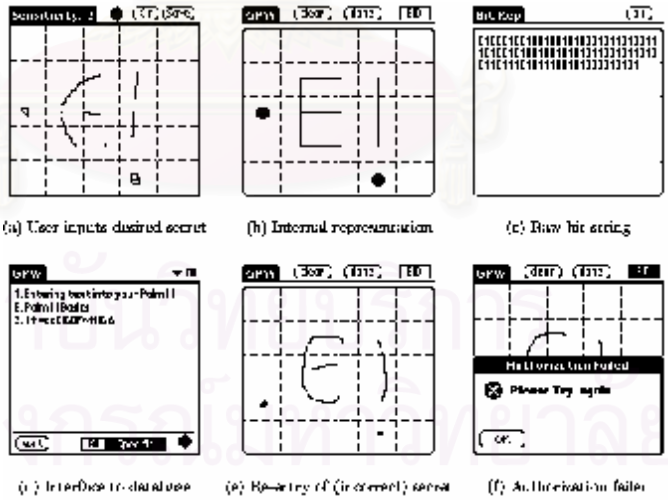
ตัวอย่างรหัสผ่านแบบรูปภาพที่ใช้เทคนิคนี้เช่น งานวิจัยเรื่อง Passwords You'll Never Forget, but Can't Recall ของ W. Daphna และ K. Scott [7] ที่ทำการฝึกผู้ใช้ให้วิเคราะห์รูปภาพชุดขนาด 100-200 รูปจากฐานข้อมูล 20000 รูป ใช้เวลา 1-3 เดือนผลปรากฏว่ากว่า 90% ของผู้ใช้สามารถผ่านการพิสูจน์ตัวตนได้ดังแสดงในรูปที่ 2.1

รูปที่ 2.1 รูปภาพบางส่วนที่ใช้ในการฝึก

อีกตัวอย่างคือ Passfaces [8] ของบริษัท Real User ถูกพัฒนาขึ้นจากสมมุติฐานที่ว่า มนุษย์สามารถจดจำรูปภาพใบหน้าของมนุษย์ได้ง่ายกว่ารูปภาพอื่นๆ ขั้นตอนการทำงานคือผู้ใช้เลือกใบหน้าจากฐานข้อมูลจำนวน 4 รูป วิธีการพิสูจน์ตัวตนคือจะมีรูปใบหน้าขึ้นมาทีละ 9 รูปโดยจะมีใบหน้าที่ผู้ใช้เลือกอยู่ 1 รูป ให้ผู้ใช้เลือกใบหน้าของผู้ใช้จนครบ 4 รอบถือว่าผ่านการพิสูจน์ตัวตนดังแสดงในรูปที่ 2.2

รูปที่ 2.2 หน้าจอในการพิสูจน์ตัวตนของ Passfaces

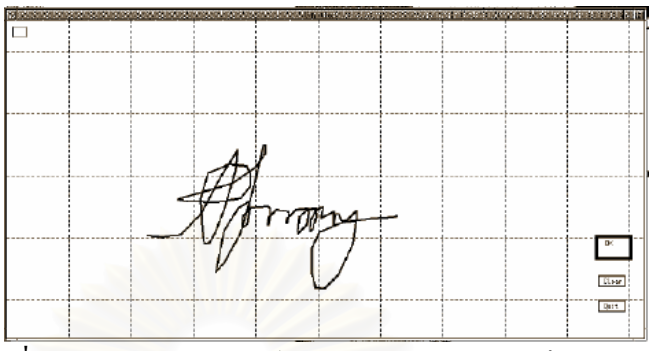
2. **เทคนิคการกระทำซ้ำ** (Recall Based) วิธีการคือให้ผู้ใช้ทำการกระทำสิ่งที่ผู้ใช้ได้ลงทะเบียนไว้อีกครั้งเพื่อเป็นการพิสูจน์ตัวตน ตัวอย่างเช่นเทคนิค Draw-a-Secret (DAS) ของ I. Jermyn และคณะ [9] ที่ให้ผู้ใช้สร้างรหัสผ่านของตัวเองโดยการวาดเส้นลงในตาราง 2 มิติซึ่งจะเก็บลักษณะการวาดไว้ เมื่อจะทำการพิสูจน์ตัวตนก็ให้ผู้ใช้ทำการวาดรหัสผ่านลงในตารางอีกครั้ง ถ้าหากตำแหน่งและลำดับการวาดเหมือนเดิมก็แสดงว่าผ่านการพิสูจน์ตัวตนดังแสดงในรูปที่ 2.3



รูปที่ 2.3 หน้าจอต่างๆของ DAS

อีกเทคนิคหนึ่งคือ การวาดลายเซ็นด้วยเมาส์ ของ A. F. Syukri และคณะ [10] ที่มีลักษณะคล้ายกับ DAS แต่จะแตกต่างตรงที่ให้ผู้ใช้งานวาดลายเซ็นด้วยเมาส์ ก่อนจะทำการจัดเก็บรายละเอียดของลายเซ็นจะผ่านกระบวนการปรับปรุงลายเซ็น (Normalize) เสียก่อน และในขั้นตอนของการพิสูจน์ตัวตนเมื่อผู้ใช้งานทำการวาดลายเซ็นเรียบร้อยแล้วก็จะมีการปรับปรุงลายเซ็นก่อน

อีกครั้งแล้วจึงนำไปเปรียบเทียบกับลายเซ็นเดิมดังแสดงในรูปที่ 2.4



รูปที่ 2.4 หน้าจอการพิสูจน์ตัวตนของการวาดลายเซ็นด้วยเมาส์

2.1.2 **การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง** (Challenge-response Authentication)

การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง คือโปรโตคอลในการพิสูจน์ตัวตนรูปแบบหนึ่ง [11] ลักษณะการทำงานจะแบ่งออกเป็น 2 ฝั่งโดยเริ่มจากฝั่งหนึ่งทำการแสดงคำถามท้าทายออกไป อีกฝั่งหนึ่งจะต้องทำการตอบคำถามที่ถูกต้องกลับมา สามารถแบ่งได้เป็น 2 ชนิดตามเทคนิคที่ใช้ดังนี้

1. **เทคนิคแบบไม่เข้ารหัส** (Non-cryptographic techniques) การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองที่พื้นฐานที่สุดก็คือระบบรหัสผ่าน (Password) คือมีการถามหารหัสผ่าน ผู้ใช้ก็จะต้องทำการใส่รหัสผ่านที่ถูกต้องลงไป

แน่นอนว่าระบบรหัสผ่านธรรมดาสามารถถูกดักฟัง (Eavesdrop) ได้ง่ายวิธีการแก้ไขก็คือการใช้รหัสผ่านแบบเป็นชุด (Multiple passwords) โดยรหัสผ่านแต่ละตัวจะมีสิ่งที่ระบุถึงรหัสผ่านนั้นๆอยู่ ในขั้นตอนการพิสูจน์ตัวตนระบบก็จะทำการให้ผู้ใช้ใส่รหัสผ่านโดยที่จะระบุว่ารหัสผ่านที่จะให้ใส่เป็นรหัสผ่านตัวไหน

นอกจากจะใช้ในเรื่องของรหัสผ่านแล้ว การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองยังถูกใช้ในการยืนยันบางสิ่งบางอย่าง ตัวอย่างเช่น CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) [12] ถูกใช้ในเว็บเพื่อยืนยันว่าบุคคลที่ใช้งานอยู่เป็นคนจริงๆ วิธีการคือแสดงรูปภาพตัวอักษรที่ทำการบิดเบี้ยวออกมา แล้วให้ผู้ใช้ทำการบอกว่าตัวอักษรที่บิดเบี้ยวนั้นคืออะไร โดยการบิดเบี้ยวของตัวอักษรถูกออกแบบมาให้การรับรู้ตัวอักษร (Optical Character Recognition) ทำได้ยาก เพื่อป้องกันโปรแกรมคอมพิวเตอร์ปลอมเป็นมนุษย์

2. **เทคนิคแบบเข้ารหัส** (Cryptographic techniques) การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองแบบไม่เข้ารหัสถือว่าเพียงพอในอดีต แต่เมื่อมีอินเตอร์เน็ตเข้ามา การส่งถ่ายข้อมูลโดยไม่มีการเข้ารหัสข้อมูลก็ถือว่าค่อนข้างมีความเสี่ยง การเข้ารหัสจึงถูกนำมาใช้โดยเทคนิคที่ได้รับความนิยมนั้นก็คือ การพิสูจน์ตัวตนแบบสองทาง (Two-way authentication)

หลักการคือทั้ง 2 ฝั่งจะต้องมีกุญแจลับ (Secret key) ที่ใช้งานร่วมกันก่อน กระบวนการเริ่มจากฝั่งหนึ่งทำการใช้กุญแจลับเข้ารหัสตัวเลขสุ่ม แล้วส่งไปยังอีกฝั่งอีกฝั่งเมื่อได้รับก็ทำการถอดรหัสด้วยกุญแจลับแล้วนำตัวเลขสุ่มไปกระทำกระบวนการบางอย่างที่ตกลงกันไว้ตั้งแต่ต้นแล้วเข้ารหัสด้วยกุญแจลับตัวเดิม ส่งกลับไปให้ฝั่งเริ่มต้นเมื่อฝั่งตั้งต้นได้รับก็ถอดรหัสดูแล้วตรวจสอบว่าเลขสุ่มนั้นได้ถูกกระทำการตามกระบวนการที่ตกลงกันไว้หรือไม่

2.1.3 SSL (Secure Socket Layer)

SSL คือโปรโตคอลในการพิสูจน์ใช้สำหรับเพิ่มความปลอดภัยในการสื่อสารผ่านเว็บโดยมีการเข้ารหัส [13][14] กระบวนการพิสูจน์ตัวตนและลายเซ็นดิจิตอลเป็นส่วนประกอบ

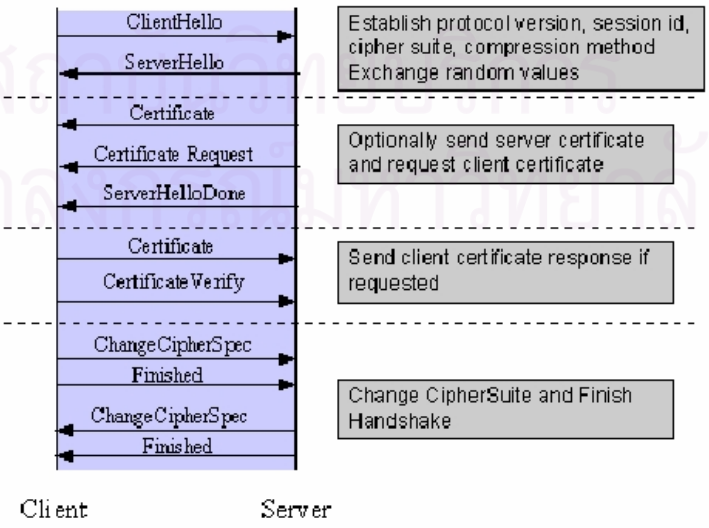
วิธีการทำงานของ SSL แบ่งออกเป็น 4 ขั้นตอนดังแสดงในรูปที่ 2.5 ดังนี้

ขั้นตอนที่1 ไคลเอนท์และเซิร์ฟเวอร์ประกาศวิธีเข้ารหัส การย่อยข้อความและลายเซ็นดิจิตอลที่รองรับ

ขั้นตอนที่2 การพิสูจน์ตัวตนของเซิร์ฟเวอร์ต่อไคลเอนท์

ขั้นตอนที่3 การพิสูจน์ตัวตนของไคลเอนท์ต่อเซิร์ฟเวอร์ (ถ้าจำเป็น)

ขั้นตอนที่4 ไคลเอนท์และเซิร์ฟเวอร์ตกลงวิธีการเข้ารหัส การย่อยข้อความและลายเซ็นดิจิตอลที่จะใช้



รูปที่ 2.5 กระบวนเริ่มต้นติดต่อการสื่อสารของโปรโตคอล SSL

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 **แบบแผนเพิ่มความแข็งแกร่งให้กับรหัสผ่านเพื่อป้องกันสปายแวร์** (A Password Scheme Strongly Resitant to Spyware) **โดย** Dawei Hong, Shushung Man, Barbra Hawes, Manton Matthews [15]

งานวิจัยนี้เสนอวิธีป้องกันสปายแวร์ของระบบรหัสผ่าน โดยนำรหัสผ่านและรูปภาพมาใช้งานร่วมกัน โดยมีขั้นตอนการทำงานดังนี้

1. การสร้างรหัสผ่าน ผู้ใช้ทำการเลือกรูปภาพ 4 รูปจากฐานข้อมูลเพื่อจะใช้เป็นรหัสผ่านแบบรูปภาพ โดยแต่ละรูปจะมีลักษณะแตกต่างกันออกไป 4 ลักษณะดังแสดงในรูปที่ 2.6 ซึ่งผู้ใช้ต้องทำการใส่รหัสให้แก่รูปภาพแต่ละรูปและแต่ละลักษณะ

รูปที่ 2.6 ตัวอย่างลักษณะที่แตกต่างกันออกไปทั้ง 4 แบบของแต่ละรูป

2. การพิสูจน์ตัวตน ระบบทำการแสดงรูปภาพออกมา 121 รูปดังแสดงในรูปที่ 2.7 โดยรูปภาพที่แสดงจะทำการสุ่มรูปภาพที่ผู้ใช้เลือกจำนวน 4 รูปรวมอยู่ด้วย ผู้ใช้งานต้องทำการเลือกรูปภาพของตัวเองและใส่รหัสของรูปภาพที่เลือกให้ถูกต้อง

รูปที่ 2.7 หน้าจอการพิสูจน์ตัวตนของระบบ

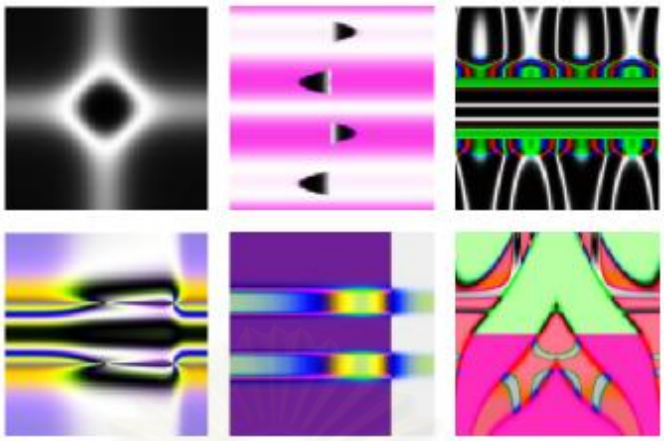
2.2.2 **เดจา วู : การศึกษาการใช้รูปภาพในการพิสูจน์ตัวตน** (déjà vu: A User Study Using Images for Authentication) **โดย** Rachna Dhamija, Adrian Perrig [16]

งานวิจัยนี้ทำการเสนอว่าการพิสูจน์ตัวตนด้วยการวิเคราะห์ (Recognize-base) ดีกว่ารหัสผ่านแบบเดิม (Recall-base) โดยได้แบ่งขั้นตอนการทำงานออกเป็น 3 ช่วงดังนี้

1. การเลือกรูปภาพ ผู้ใช้ทำการเลือกรูปภาพจากชุดของรูปภาพที่เตรียมไว้ รูปภาพที่ใช้ในงานวิจัยนี้เป็นรูปเชิงความหมายดังแสดงในรูปที่ 2.8 โดยผู้วิจัยให้เหตุผลว่าเพื่อป้องกันผู้ใช้งานจดรหัสผ่านรูปภาพลงกระดาษ

2. การสร้างความคุ้นเคย เพื่อให้เกิดความคุ้นเคยกับรูปภาพที่เลือกไว้ ระบบจะทำการแสดงรูปภาพสุ่มปนกับรูปภาพที่ผู้ใช้เลือก แล้วให้ผู้ใช้ทำการเลือกรูปภาพของตัวเองออกมา

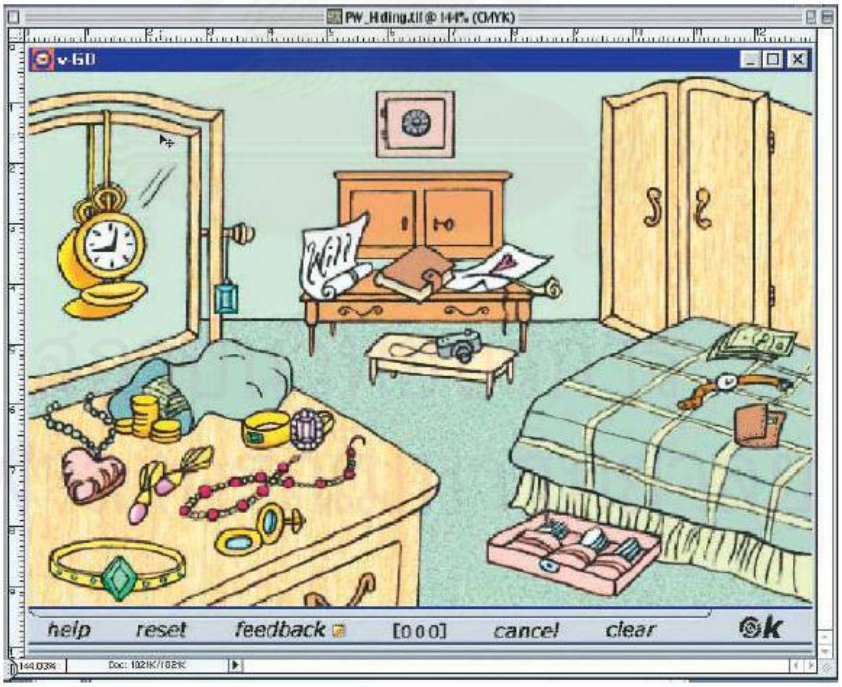
3. การพิสูจน์ตัวตน ระบบทำการแสดงรูปภาพสุ่มที่มีรูปภาพของผู้ใช้รวมอยู่ หากผู้ใช้สามารถเลือกรูปภาพของตัวเองได้จนครบถือว่าผ่านการพิสูจน์ตัวตน



รูปที่ 2.8 รูปภาพเชิงความหมายที่ใช้ในเดจา วู

2.2.3 **ตรรกะผ่าน** (Passlogix) **โดย** www.passlogix.com [17]

วิธีนี้ใช้การสร้างสถานที่จำลองขึ้นมาแสดงออกมาในรูปแบบรูปภาพ โดยใช้หลักการทำซ้ำอย่างเป็นลำดับขึ้นตอนในการพิสูจน์ตัวตนตัวอย่างเช่น การผสมมิกเซอร์ในบาร์เครื่องดื่ม การทำอาหารในห้องครัว ผู้ใช้จะต้องจำสิ่งที่ตัวเองทำไว้ตอนลงทะเบียนและกระทำซ้ำเมื่อต้องการเข้าสู่ระบบดังแสดงในรูปที่ 2.9

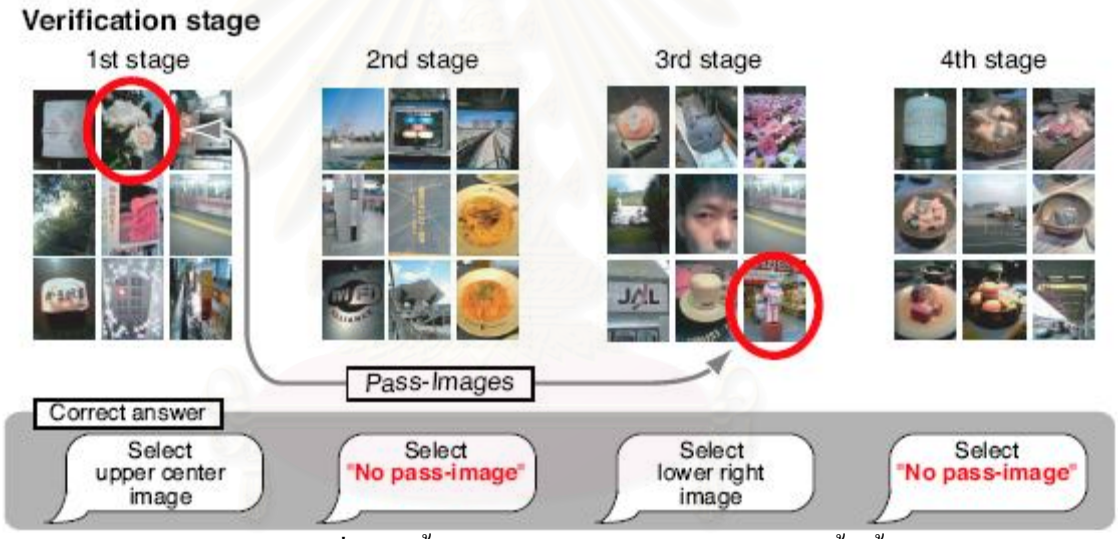


รูปที่ 2.9 ตัวอย่างสถานที่จำลองที่ใช้ในการพิสูจน์ตัวตนของ Passlogix

2.2.4 **การพิสูจน์ตัวตนแบบรูปภาพโดยใช้ภาพโปรดบนโทรศัพท์มือถือ** (Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images) **โดย** Tetsuji TAKADA **และ** Hideki KOIKE [18]

งานวิจัยชิ้นนี้ยอมให้ผู้ใช้งานสามารถใช้รูปภาพของตัวเองในการพิสูจน์ตัวตนได้ โดยในขั้นตอนของการพิสูจน์ตัวตนจะถูกแบ่งออกเป็นรอบๆ โดยแต่ละรอบอาจจะมีรูปของผู้ใช้ปรากฏอยู่หรือไม่ก็ได้ ถ้าหากมีผู้ใช้ก็ต้องเลือกรูปภาพของตัวเอง แต่ถ้าหากไม่มีผู้ใช้ก็ไม่ต้องเลือกรูปใด การพิสูจน์ตัวตนจะสำเร็จก็ต่อเมื่อผู้ใช้สามารถผ่านการพิสูจน์ตัวตนทุกรอบได้อย่างถูกต้องดังแสดงในรูปที่ 2.10

การที่ยอมให้ใช้รูปภาพของตัวเองในระบบมีข้อดีในการจดจำได้ง่ายก็จริง แต่ข้อเสียก็คือถ้าหากเป็นคนที่รู้จักกับผู้ใช้อาจจะสามารถคาดเดารูปภาพที่เป็นรหัสผ่านได้ง่าย



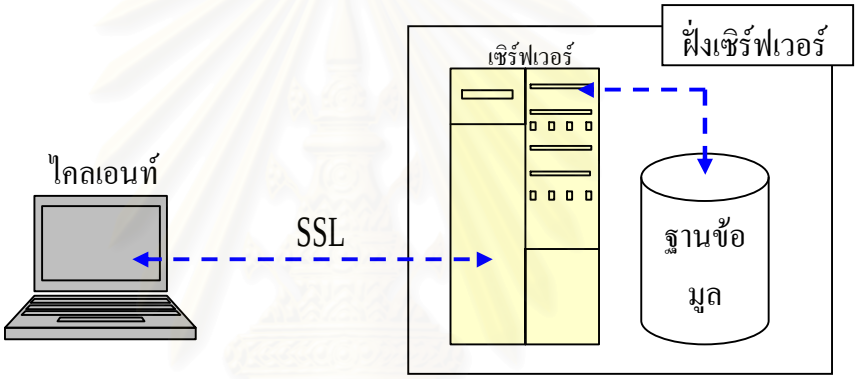
รูปที่ 2.10 ขั้นตอนการพิสูจน์ตัวตนของงานวิจัยชิ้นนี้

บทที่ 3
การพิสูจน์ตัวตนของรหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนอง

ในบทนี้จะกล่าวถึงโครงสร้างของซอฟต์แวร์รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนองรวมไปถึงรายละเอียดของรูปภาพที่จัดเก็บในฐานข้อมูล ตลอดจนเครื่องมือที่ใช้พัฒนา

3.1 โครงสร้างของซอฟต์แวร์

ซอฟต์แวร์ที่สร้างขึ้นทำงานบนเว็บ คือผู้ใช้ที่อยู่ฝั่งไคลเอนท์ (Client) ร้องขอเข้าไปที่เว็บเซิร์ฟเวอร์ (Web Server) เพื่อทำการพิสูจน์ตัวตน โดยจะมีฐานข้อมูลคอยส่งข้อมูลให้ระยะ ซึ่งการติดต่อสื่อสารทั้งหมดจะกระทำผ่านโปรโตคอล SSL เพื่อความปลอดภัยดังแสดงในรูปที่ 3.1



รูปที่ 3.1 โครงสร้างของซอฟต์แวร์ทำงานบนเว็บ

3.2 ลักษณะของรูปภาพและฐานข้อมูล

3.2.1 **ลักษณะของรูปภาพ** รูปภาพทั้งหมดได้มาจากการค้นหาในอินเตอร์เน็ต แต่ละรูปจะมีขนาด 100x100 พิกเซล โดยมีชนิดของรูปภาพที่รองรับ 2 ชนิดคือ GIF (Graphics Interchange Format) และ JPEG (Joint Photographic Experts Group) โดยแต่ละรูปมีรายละเอียดดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 คุณสมบัติของรูปภาพแต่ละรูป

คุณสมบัติ	**คำอธิบาย**
รหัสประจำภาพ	รหัสประจำตัวของรูปภาพแต่ละรูปตัวอย่างเช่น 0001, 0002, 0003
ชื่อรูป	รูปภาพแต่ละรูปชื่ออะไร
กลุ่ม	รูปภาพรูปนั้นอยู่ในกลุ่มไหน
คำสำคัญ	ลักษณะเด่น หรือ คำจำกัดความของรูปภาพนั้น

กลุ่มของคำสำคัญแบ่งได้เป็น 37 กลุ่มตามลักษณะของคำสำคัญดังนี้

1. เครื่องประดับ (accessory) มีคำสำคัญ 40 คำ
2. ท่าทางและความรู้สึก (action&feeling) มีคำสำคัญ 107 คำ
3. สัตว์น้ำ (anm_aquatic) มีคำสำคัญ 16 คำ
4. สัตว์ปีก (anm_bird) มีคำสำคัญ 11 คำ
5. แมลง (anm_insect) มีคำสำคัญ 19 คำ
6. สัตว์ลึกลับ สัตว์ในตำนาน (anm_mythical) มีคำสำคัญ 6 คำ
7. สัตว์เลื้อยคลาน (anm_reptile) มีคำสำคัญ 10 คำ
8. สัตว์บก (anm_terrestial) มีคำสำคัญ 27 คำ
9. เครื่องนอน (bedroom_set) มีคำสำคัญ 10 คำ
10. อุปกรณ์ทำความสะอาด (cleaner_set) มีคำสำคัญ 10 คำ
11. สิ่งก่อสร้าง (construct) มีคำสำคัญ 13 คำ
12. เครื่องสำอางและผลิตภัณฑ์ในห้องน้ำ (cosmetic&bath) มีคำสำคัญ 10 คำ
13. โดเรมอน (doraemon) มีคำสำคัญ 14 คำ
14. อุปกรณ์อิเลคโทรนิค (electronic) มีคำสำคัญ 14 คำ
15. ความบันเทิง (entertain) มีคำสำคัญ 4 คำ
16. ครอบครัว (family) มีคำสำคัญ 5 คำ
17. อาหาร (food) มีคำสำคัญ 83 คำ
18. นักฟุตบอล (football_player) มีคำสำคัญ 60 คำ
19. ผลไม้ (fruit) มีคำสำคัญ 33 คำ
20. เฟอร์นิเจอร์ (furniture) มีคำสำคัญ 12 คำ
21. อวัยวะของมนุษย์ (human_body) มีคำสำคัญ 19 คำ
22. อุปกรณ์ทันสมัย (IT) มีคำสำคัญ 68 คำ
23. ผลิตภัณฑ์สำหรับเด็ก (kid_set) มีคำสำคัญ 10 คำ
24. เครื่องครัว (kitchen_set) มีคำสำคัญ 15 คำ
25. ดนตรี (music) มีคำสำคัญ 11 คำ
26. ธรรมชาติ (natural) มีคำสำคัญ 20 คำ
27. อาชีพ (occupation) มีคำสำคัญ 67 คำ
28. สถานที่ (place) มีคำสำคัญ 53 คำ
29. ห้องต่างๆ (room) มีคำสำคัญ 12 คำ
30. สัญลักษณ์และภาษา (sign&language) มีคำสำคัญ 33 คำ

31. กีฬา (sport) มีคำสำคัญ 32 คำ
32. อุปกรณ์การเรียน (student_set) มีคำสำคัญ 13 คำ
33. นักเทนนิส (tennis_player) มีคำสำคัญ 60 คำ
34. อุปกรณ์ช่าง (tool) มีคำสำคัญ 2 คำ
35. การคมนาคม (transportation) มีคำสำคัญ 27 คำ
36. ผัก (vegetable) มีคำสำคัญ 6 คำ
37. เสื้อผ้า (cloth) มีคำสำคัญ 35 คำ

คำสำคัญแต่ละคำจะประกอบไปด้วยรูปภาพประจำตัวประมาณ 4 รูปโดยที่รูปภาพไม่จำเป็นต้องคล้ายคลึงกันแต่จะต้องมีความหมายเดียวกันเพื่อป้องกันการใช้คอมพิวเตอร์วิเคราะห์ลักษณะชุดของภาพดังแสดงในรูปที่ 3.2 รวมแล้วมีคำสำคัญในระบบทั้งหมด 1000 คำและรูปภาพทั้งหมด 4027 รูป

รูปที่ 3.2 ตัวอย่างรูปภาพประจำตัวของคำสำคัญ “hippo”

3.2.2 **ฐานข้อมูล** ฐานข้อมูลที่ใช้แบ่งออกเป็นสองกลุ่มคือ ฐานข้อมูลของสมุดบันทึกออนไลน์ซึ่งใช้เป็นระบบตัวอย่างของซอฟต์แวร์ ชื่อตารางจะขึ้นต้นด้วย app_ และฐานข้อมูลของซอฟต์แวร์การพิสูจน์ตัวตนเอง โดยมีทั้งหมด 8 ตารางดังนี้

1. ตาราง app_blog เก็บบทความของผู้ใช้
2. ตาราง app_comment เก็บความคิดเห็นของผู้อื่นที่มีต่อบทความ
3. ตาราง gallery เก็บรายละเอียดของรูปภาพ
4. ตาราง kgroup เก็บรายละเอียดของกลุ่มของคำสำคัญ
5. ตาราง kword เก็บรายละเอียดของคำสำคัญ
6. ตาราง profile เก็บรายละเอียดและข้อมูลการเข้าสู่ระบบของผู้ใช้
7. ตาราง question เก็บรายละเอียดของคำถามท้าทาย
8. ตาราง ukey เก็บคำสำคัญของผู้ใช้

รายละเอียดของแต่ละตารางแสดงในพจนานุกรมข้อมูล (Data Dictionary) ได้ดังตารางที่ 3.2 ถึงตารางที่ 3.9

ตารางที่ 3.2 พจนานุกรมข้อมูลของตาราง app_blog

ชื่อตาราง : app_blog		
คำอธิบาย : เก็บบทความของผู้ใช้		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
ID	Integer(3)	รหัสบทความ
UID	Integet(3)	รหัสผู้ใช้
TITLE	Varchar(50)	ชื่อบทความ
TIMEST	Varchar(15)	เวลาที่บันทึกบทความ
BODY	Text	เนื้อหาของบทความ

ตารางที่ 3.3 พจนานุกรมข้อมูลของตาราง app_comment

ชื่อตาราง : app_comment		
คำอธิบาย : เก็บความคิดเห็นของผู้อื่นที่มีต่อบทความ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
ID	Integer(3)	รหัสความคิดเห็น
BID	Integer(3)	รหัสบทความ
UID	Integer(3)	รหัสผู้ใช้
NAME	Varchar(50)	ชื่อผู้แสดงความคิดเห็น
TIMEST	Varchar(15)	เวลาที่บันทึกความคิดเห็น
BODY	Text	เนื้อหาของความคิดเห็น

ตารางที่ 3.4 พจนานุกรมข้อมูลของตาราง gallery

ชื่อตาราง :gallery		
คำอธิบาย : เก็บรายละเอียดของรูปภาพ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
PID	Integer(4)	รหัสรูปภาพ
PNAME	Varchar(30)	ชื่อไฟล์รูปภาพ
NAME	Varchar(25)	รหัสรูปภาพ
KID	Integer(4)	รหัสคำสำคัญของรูปภาพ

ตารางที่ 3.5 พจนานุกรมข้อมูลของตาราง kgroup

ชื่อตาราง : kgroup		
คำอธิบาย : เก็บรายละเอียดของกลุ่มของคำสำคัญ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
GID	Integer(2)	รหัสกลุ่มคำสำคัญ
NAME	Varchar(15)	ชื่อกลุ่มคำสำคัญ

ตารางที่ 3.6 พจนานุกรมข้อมูลของตาราง kword

ชื่อตาราง : kword		
คำอธิบาย : เก็บรายละเอียดของคำสำคัญ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
GID	Integer(2)	รหัสกลุ่มคำสำคัญ
KWORD	Varchar(25)	ชื่อคำสำคัญ
KID	Integer(4)	รหัสคำสำคัญ

ตารางที่ 3.7 พจนานุกรมข้อมูลของตาราง profile

ชื่อตาราง : profile		
คำอธิบาย : เก็บรายละเอียดและข้อมูลการเข้าสู่ระบบของผู้ใช้		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
NAME	Varchar(20)	ชื่อผู้ใช้
UID	Integer(3)	รหัสผู้ใช้
LEVEL	Integer(1)	ระดับความปลอดภัย
ANSSTYLE	Integer(1)	รูปแบบของตารางคำตอบ
LOGIN_MISS	Integer(1)	จำนวนครั้งการเขาสู่ระบบผิดพลาด
LOGIN_SURF	Integer(1)	จำนวนครั้งการเข้าสู่ระบบ
ADMIN	Char(2)	ตำแหน่งผู้ดูแลระบบ

ตารางที่ 3.8 พจนานุกรมข้อมูลของตาราง question

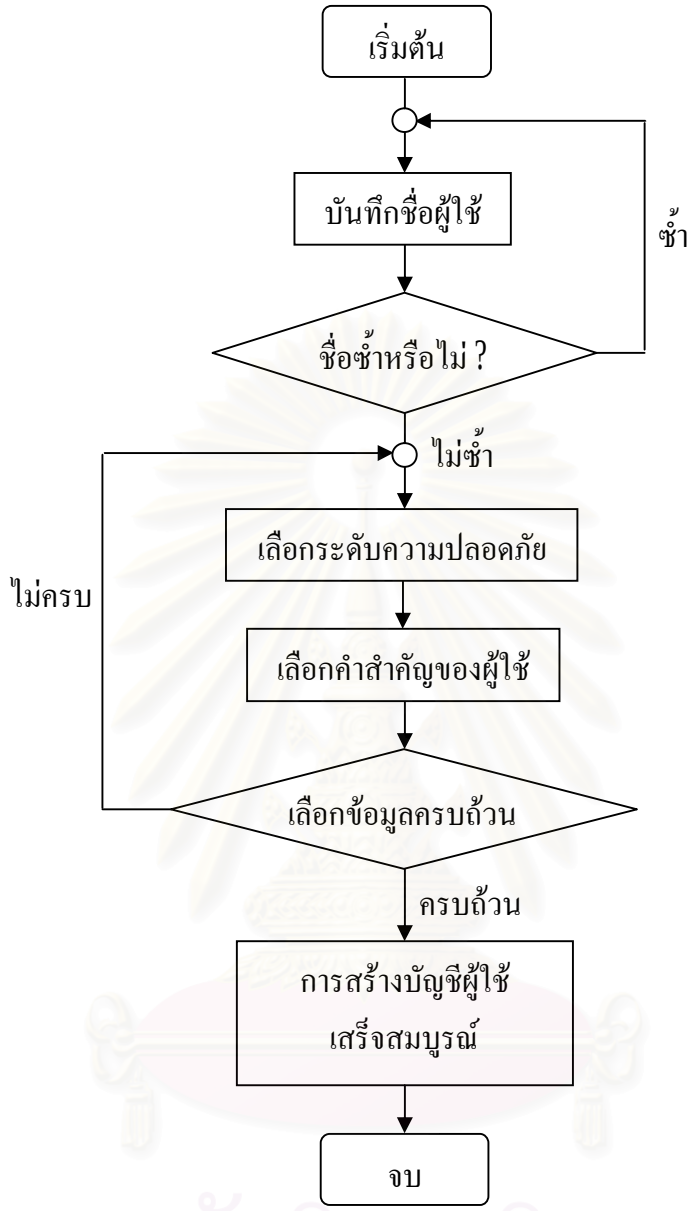
ชื่อตาราง : question		
คำอธิบาย : เก็บรายละเอียดของคำถามท้าทาย		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
QID	Integer(2)	รหัสคำถาม
USRCODE	Varchar(5)	รหัสตรวจสอบความถูกต้องของคำตอบ
DETAIL	Text	คำถามท้าทาย

ตารางที่ 3.9 พจนานุกรมข้อมูลของตาราง ukey

ชื่อตาราง : ukey		
คำอธิบาย : เก็บคำสำคัญของผู้ใช้		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
UID	Integer(3)	รหัสผู้ใช้
NO	Integer(1)	ลำดับรหัสคำสำคัญของผู้ใช้
KID	Integer(4)	รหัสคำสำคัญ

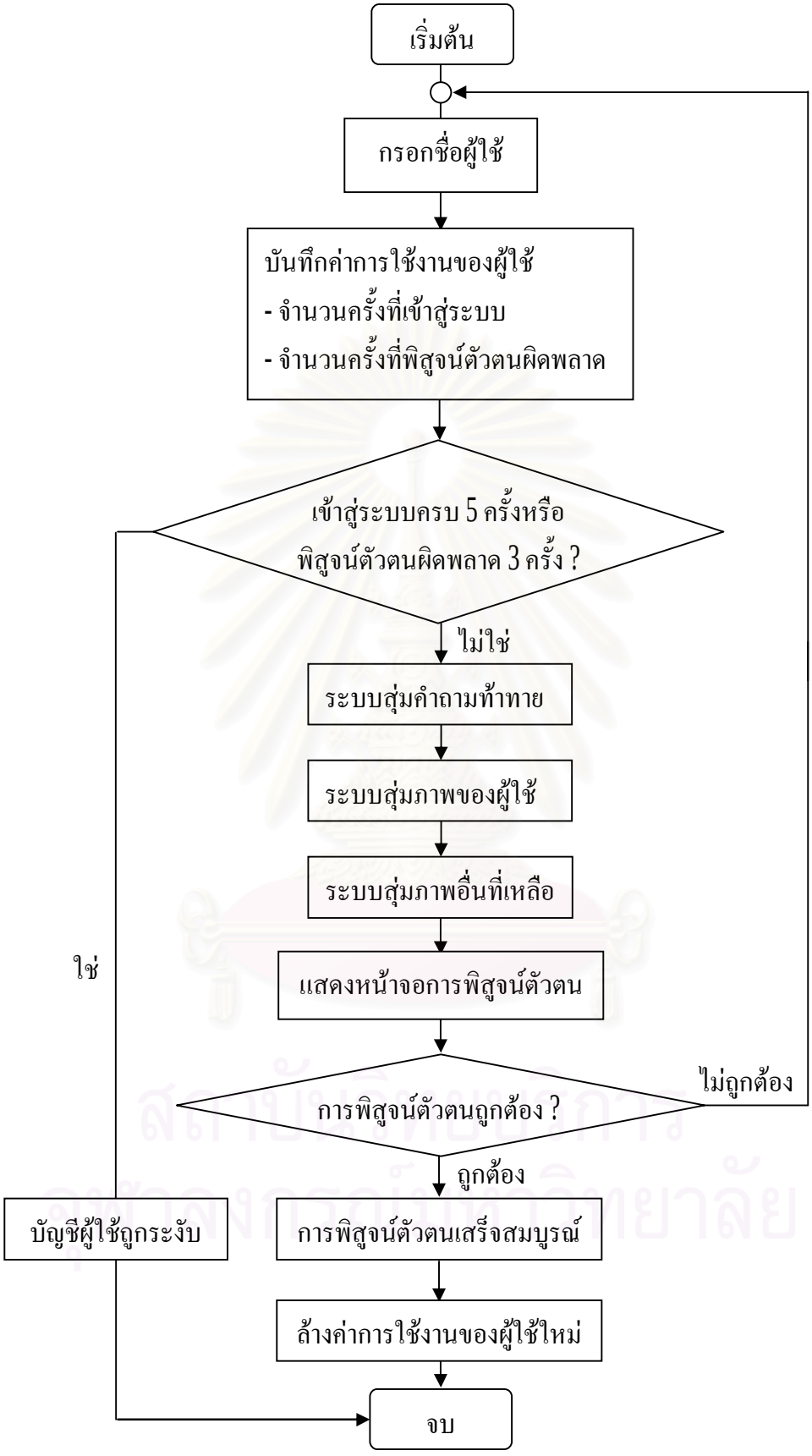
3.3 ขั้นตอนการทำงานของซอฟต์แวร์

3.3.1 **การสร้างบัญชีผู้ใช้** ก่อนที่ผู้ใช้จะทำการใช้งานซอฟต์แวร์ได้นั้น จำเป็นต้องทำการสร้างบัญชีผู้ใช้ก่อน เพื่อใช้ในการเก็บข้อมูลต่างๆของผู้ใช้ คำสำคัญที่ผู้ใช้เลือก รวมไปถึงใช้ในการบันทึกพฤติกรรมในการเข้าสู่ระบบของผู้ใช้ โดยการสร้างบัญชีผู้ใช้มีขั้นตอนการทำงานดังนี้



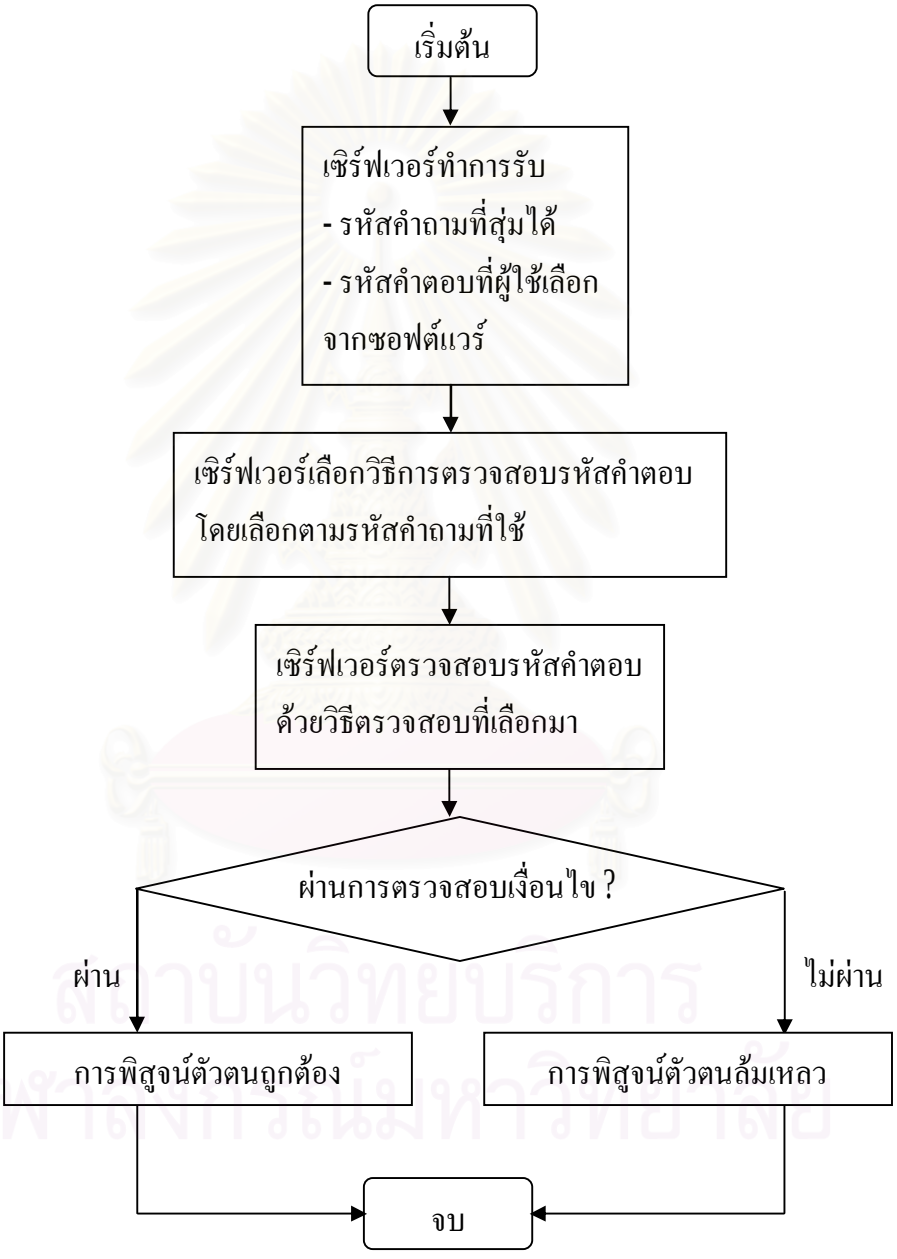
รูปที่ 3.3 กระแสงานของการสร้างบัญชีผู้ใช้

3.3.2 **การพิสูจน์ตัวตน** ขั้นตอนนี้ถือเป็นขึ้นตอนที่สำคัญที่สุดของซอฟต์แวร์ เนื่องจากว่าเป็นขั้นตอนที่นำแนวคิดของการพิสูจน์ตัวตนแบบรูปภาพโดยใช้คำถามท้าทายตอบสนองมาใช้ นอก จากนี้ในขั้นตอนของการพิสูจน์ตัวตนยังมีการเพิ่มเติมระบบตรวจสอบพฤติกรรมการพิสูจน์ตัวตนของผู้ใช้งาน เพื่อต้านทานต่อการลักลอบนำภาพที่ใช้ในการพิสูจน์ตัวตนไปวิเคราะห์เพื่อหาคำสำคัญของผู้ใช้อีกด้วย



รูปที่ 3.4 กระแสงานของการพิสูจน์ตัวตน

3.3.3 **การตรวจสอบความถูกต้องของการพิสูจน์ตัวตน** หลังจากที่ทำการพิสูจน์ตัวตนแล้ว ขั้นตอนต่อมาเซิร์ฟเวอร์จะนำข้อมูลที่ผู้ใช้พิสูจน์ตัวตนมาตรวจสอบเพื่อบอกว่าการพิสูจน์ตัวตนในรอบนั้นถูกต้องสมบูรณ์หรือไม่ โดยขั้นตอนของการตรวจสอบความถูกต้องของการพิสูจน์ตัวตนมีดังนี้

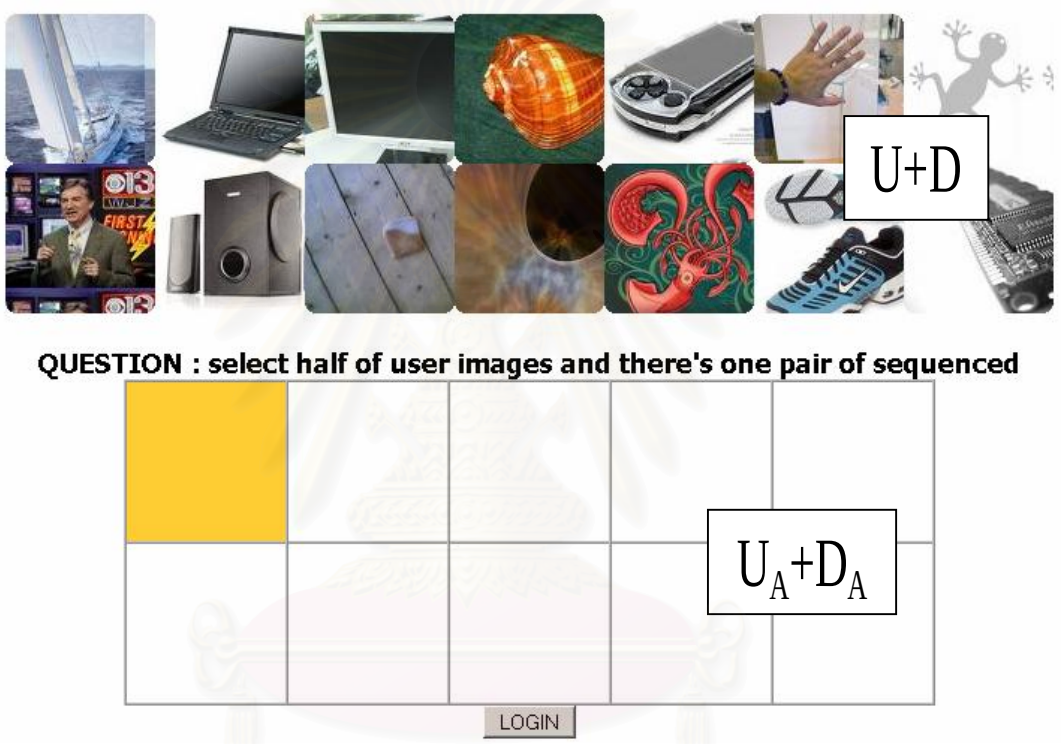


รูปที่ 3.5 กระแสงานของการตรวจสอบความถูกต้องของการพิสูจน์ตัวตน

3.4 การวิเคราะห์ความปลอดภัยของคำสำคัญ

3.4.1 **คำถามท้าทาย** หน้าที่ของคำถามท้าทายคือ กำหนดเงื่อนไขสำหรับการเลือกรูปภาพในขั้นตอนของการพิสูจน์ตัวตนให้กับผู้ใช้ ซึ่งคำถามจะออกมาในลักษณะสุ่ม ทำให้ในแต่ละรอบของการพิสูจน์ตัวตน คำตอบของผู้ใช้ย่อมแตกต่างกันออกไป

ก่อนที่จะเป็นเรื่องของคำถามท้าทายทั้ง 7 ในเบื้องต้นจำเป็นต้องทราบถึงส่วนประกอบของหน้าจอการพิสูจน์ตัวตน คำศัพท์และสูตรที่จำเป็นต้องใช้ก่อนดังนี้



รูปที่ 3.6 ตัวอย่างหน้าจอการพิสูจน์ตัวตน

ชุดรูปภาพที่ใช้ในการพิสูจน์ตัวตนนั้นประกอบไปด้วยรูปภาพของผู้ใช้ (U) และรูปภาพอื่นๆ (D) ผสมกันอยู่โดยขนาดของ U นั้นจะไม่แน่นอนขึ้นอยู่กับคำถามท้าทายในรอบนั้นๆ ในบางเงื่อนไขของคำถามท้าทายให้ผู้ใช้ทำการเลือกรูปภาพของผู้ใช้เพียงครึ่งเดียว (H)

การพิสูจน์ตัวตนจะกระทำได้โดยการเลือกรูปจากชุดรูปภาพด้านบนลงในกล่องคำตอบซึ่งกล่องคำตอบก็จะประกอบไปด้วยรูปภาพของผู้ใช้ที่ถูกเลือก (U_A) และรูปภาพอื่นๆที่ถูกเลือก (D_A) ซึ่งเป็นเซตย่อยของ U และ D อีกทีหนึ่ง

กล่องคำตอบประกอบไปด้วยแถว 2 แถวด้วยกันคือ แถวที่ 1 (R1) และแถวที่ 2 (R2) ซึ่งรูปภาพอื่นๆที่ถูกเลือกนั้นสามารถแบ่งออกเป็น 2 ชุดตามแถวได้เป็น รูปภาพอื่นๆที่ถูกเลือกแถวที่ 1 (D1) และรูปภาพอื่นๆที่ถูกเลือกแถวที่ 2 (D2)

ตารางที่ 3.10 ตารางคำศัพท์ในหน้าจอการพิสูจน์ตัวตน

คำศัพท์	ตัวย่อ	ความหมาย
User image	U	รูปภาพของผู้ใช้
User image in Answer box	UA	รูปภาพของผู้ใช้ในกล่องคำตอบ
Decoy image	D	รูปภาพอื่นๆ
Decoy image in Answer box	DA	รูปภาพอื่นๆในกล่องคำตอบ
Half of User image	H	ครึ่งหนึ่งของรูปภาพของผู้ใช้
Decoy image in Answer box row 1	D1	รูปภาพอื่นๆในแถวแรกของกล่องคำตอบ
Decoy image in Answer box row 2	D2	รูปภาพอื่นๆในแถวที่สองของกล่องคำตอบ
Answer box row 1	R1	แถวแรกของกล่องคำตอบ
Answer box row 2	R2	แถวที่สองของกล่องคำตอบ
Answer box	A	กล่องคำตอบ

วิธีการคำนวณเซตคำตอบที่ถูกต้องในคำถามท้าทาย เริ่มต้นจากการเลือกเซตรูปภาพที่เป็นไปได้ลงในกล่องคำตอบแล้วทำการสลับตำแหน่งหาคำตอบที่เป็นไปได้ทั้งหมดในกล่องคำตอบ ซึ่งจำเป็นต้องใช้สมการทางสถิติสองตัวในการเลือกรูปภาพและเรียงรูปภาพคือ การจัดหมู่ (combination) และการเรียงสับเปลี่ยน (permutation) ตามลำดับ

$$\text{การจัดหมู่} = {}^{n}C_{r} = \frac{n!}{(n-r)!\,r!}$$

สมการที่ 3.1 การจัดหมู่

$$\text{การเรียงสับเปลี่ยน} = {}^{n}p_{r} = \frac{n!}{(n-r)!}$$

สมการที่ 3.2 การเรียงสับเปลี่ยน

คำถามท้าทายในซอฟต์แวร์มีทั้งหมด 7 คำถาม ประกอบด้วย

1. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกติดกัน 1 ตำแหน่ง คำถามนี้สามารถสุ่มรูปภาพส่วนตัวทั้งหมดได้ตั้งแต่ตั้งแต่ 2 รูป – 7 รูป แนวคิดคือเลือกรูปภาพส่วนตัวทั้งหมดและรูปภาพอื่นๆลงในกล่องคำตอบให้เต็มก่อน ต่อมาจับรูปภาพอื่นๆจัดแถวตอนเรียงหนึ่งแล้วคิดการเรียง หลังจากนั้นจับรูปภาพส่วนตัวผูกติดกันหนึ่งคู่ แล้วคิดการเรียงรูปภาพส่วนตัวจากช่องว่างระหว่างรูปภาพอื่นๆ และสุดท้ายคิดการเรียงสลับตำแหน่งกันของรูปภาพส่วนตัวที่ผูกติดกันไว้

เซตคำตอบของคำถามท้าทายที่ 1 = $({}^{U}C_{U}\,{}^{D}C_{DA})({}^{DA}p_{DA}\,{}^{DA+1}p_{U-1}\,{}^{2}p_{2})$

สมการที่ 3.3 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 1

2. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกไม่ติดกันเลย คำถามนี้สามารถสุ่มรูปภาพส่วนตัวได้ตั้งแต่ตั้งแต่ 2 รูป – 7 รูป แนวคิดคือเลือกรูปภาพส่วนตัวทั้งหมดและรูปภาพอื่นๆลงในกล่องคำตอบให้เต็มก่อน ต่อมาจับรูปภาพอื่นๆจัดแถวตอนเรียงหนึ่งแล้วคิดการเรียงแล้วคิดการเรียงรูปภาพส่วนตัวจากช่องว่างระหว่างรูปภาพอื่นๆอีกครั้งหนึ่ง

เซตคำตอบของคำถามท้าทายที่ 2 = $({}^{U}C_{U}\,{}^{D}C_{DA})({}^{DA}p_{DA}\,{}^{DA+1}p_{U})$

สมการที่ 3.4 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 2

3. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกติดกัน 1 ตำแหน่ง คำถามนี้สามารถสุ่มรูปภาพส่วนตัวได้ 3 แบบคือ 4, 6 และ 8 รูป แนวคิดคือเลือกรูปภาพส่วนตัวครึ่งนึงและรูปภาพอื่นๆลงในกล่องคำตอบให้เต็มก่อน จับรูปภาพอื่นๆจัดแถวตอนเรียงหนึ่งแล้วคิดการเรียง หลังจากนั้นจับรูปภาพส่วนตัวคู่นึงผูกติดกันไว้แล้วคิดการเรียงของรูปภาพส่วนตัวที่เป็นไปได้ในช่องว่างระหว่างรูปภาพอื่นๆ และสุดท้ายคิดการเรียงสลับกันของรูปภาพส่วนตัวที่ผูกกันไว้

เซตคำตอบของคำถามท้าทายที่ 3 = $({}^{U}C_{H}\,{}^{D}C_{DA})({}^{DA}p_{DA}\,{}^{DA+1}p_{H-1}\,{}^{2}p_{2})$

สมการที่ 3.5 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 3

4. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกไม่ติดกันเลย คำถามนี้สามารถสุ่มรูปภาพส่วนตัวได้ 3 แบบคือ 4, 6 และ 8 รูป แนวคิดคือเลือกรูปภาพส่วนตัวครึ่งนึงและรูปภาพ

อื่นๆลงในกล่องคำตอบให้เต็มก่อน จับรูปภาพอื่นๆจัดแถวตอนเรียงหนึ่งแล้วคิดการเรียง แล้วคิดการเรียงของรูปภาพส่วนตัวที่เป็นไปได้ในช่องว่างระหว่างรูปภาพอื่นๆ

เซตคำตอบของคำถามท้าทายที่ 4 = $({}^{U}C_{H}\ {}^{D}C_{DA})({}^{DA}p_{DA}\ {}^{DA+1}p_{H})$

สมการที่ 3.6 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 4

5. เลือกรูปภาพส่วนตัวทั้งหมดโดยต้องมีอยู่ทั้งสองแถว คำถามนี้สามารถสุ่มรูปภาพส่วนตัวได้ตั้งแต่ตั้งแต่ 2 รูป – 7 รูป คำถามนี้แยกคิดเป็นกรณีโดยไล่ไปตั้งแต่กรณีทีแถวแรกมีรูปภาพส่วนตัว 1 รูปไปจนถึงแถวแรกมีรูปภาพส่วนตัว U-1 รูป ส่วนการเรียงสับเปลี่ยนก็ทำทีละแถวเช่นกัน

เซตคำตอบของคำถามท้าทายที่ 5 = $\sum_{i=1}^{U-1}\{\ ({}^{U}C_{i}\ {}^{D}C_{D1})({}^{U-i}C_{U-i}\ {}^{D-D1}C_{D2})\ ({}^{R1}p_{R1}\ {}^{R2}p_{R2})\ \}$

สมการที่ 3.7 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 5

6. ไม่เลือกรูปภาพส่วนตัว 1 รูป คำถามนี้สามารถสุ่มรูปภาพส่วนตัวได้ตั้งแต่ตั้งแต่ 2 รูป – 7 รูป แนวคิดคือเลือกรูปภาพส่วนตัว U-1 รูปและรูปภาพอื่นๆที่เหลือเติมกล่องคำตอบให้เต็มแล้วทำการเรียงทีเดียวทั้งกล่องคำตอบ

เซตคำตอบของคำถามท้าทายที่ 6 = $({}^{U}C_{U-1}\ {}^{D}C_{DA})({}^{A}p_{A})$

สมการที่ 3.8 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 6

7. ไม่เลือกรูปภาพส่วนตัว 2 รูป คำถามนี้สามารถสุ่มรูปภาพส่วนตัวได้ตั้งแต่ตั้งแต่ 2 รูป – 7 รูป แนวคิดคือเลือกรูปภาพส่วนตัว U-2 รูปและรูปภาพอื่นๆที่เหลือเติมกล่องคำตอบให้เต็มแล้วทำการเรียงทีเดียวทั้งกล่องคำตอบ

เซตคำตอบของคำถามท้าทายที่ 7 = $({}^{U}C_{U-2}\ {}^{D}C_{DA})({}^{A}p_{A})$

สมการที่ 3.9 สูตรการคำนวณหาเซตคำตอบที่ถูกต้องของคำถามท้าทายที่ 7

3.4.2 **ลักษณะการต้านทานสปาย์แวร์**

ขั้นตอนการพิสูจน์ตัวตนของงานวิจัยชิ้นนี้ถูกออกแบบให้สามารถต้านทานสปายแวร์ได้ แม้ว่าสปาย์แวร์จะสามารถดักข้อมูลระหว่างไคลเอนท์และเซิร์ฟเวอร์ ดักการกดแป้นพิมพ์ของผู้ใช้ ดักการเคลื่อนที่และการกดของเมาส์ หรือแม้กระทั่งสามารถดูจอภาพของผู้ใช้ได้ ด้วยคุณสมบัติต่อไปนี้

1. คำถามท้าทาย จะถูกสุ่มออกมาในแต่ละรอบโดยคำถามที่แตกต่างกันออกไป
2. เนื่องจากคำสำคัญมีรูปภาพประจำตัว 4 ภาพดังนั้นการพิสูจน์ตัวตนแต่ละรอบรูปภาพประจำคำสำคัญก็จะถูกสุ่มออกมาเช่นเดียวกัน

จากคุณสมบัติดังกล่าวนั้นก็คือคุณสมบัติสุ่มนั้นเอง ถ้าหากว่าสปาย์แวร์ทำการดักข้อมูลไปได้ก็จะได้เพียงข้อมูลในการพิสูจน์ตัวตนครั้งนั้นๆเพียงครั้งเดียว เพราะในการพิสูจน์ตัวตนครั้งต่อไปคำถามท้าทายและรูปภาพประจำคำสำคัญก็จะทำการสุ่มใหม่อีกครั้ง

ถึงแม้ว่าคำถามท้าทายหรือรูปภาพประจำคำสำคัญจะแสดงออกมาด้วยวิธีการสุ่ม แต่สำหรับผู้ใช้แล้วการพิสูจน์ตัวตนก็สามารถทำได้ไม่ยาก เพราะสิ่งที่ผู้ใช้ต้องจำก็มีเพียงคำสำคัญของตัวเองเท่านั้น

บทที่ 4

การทำงานของรหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนอง

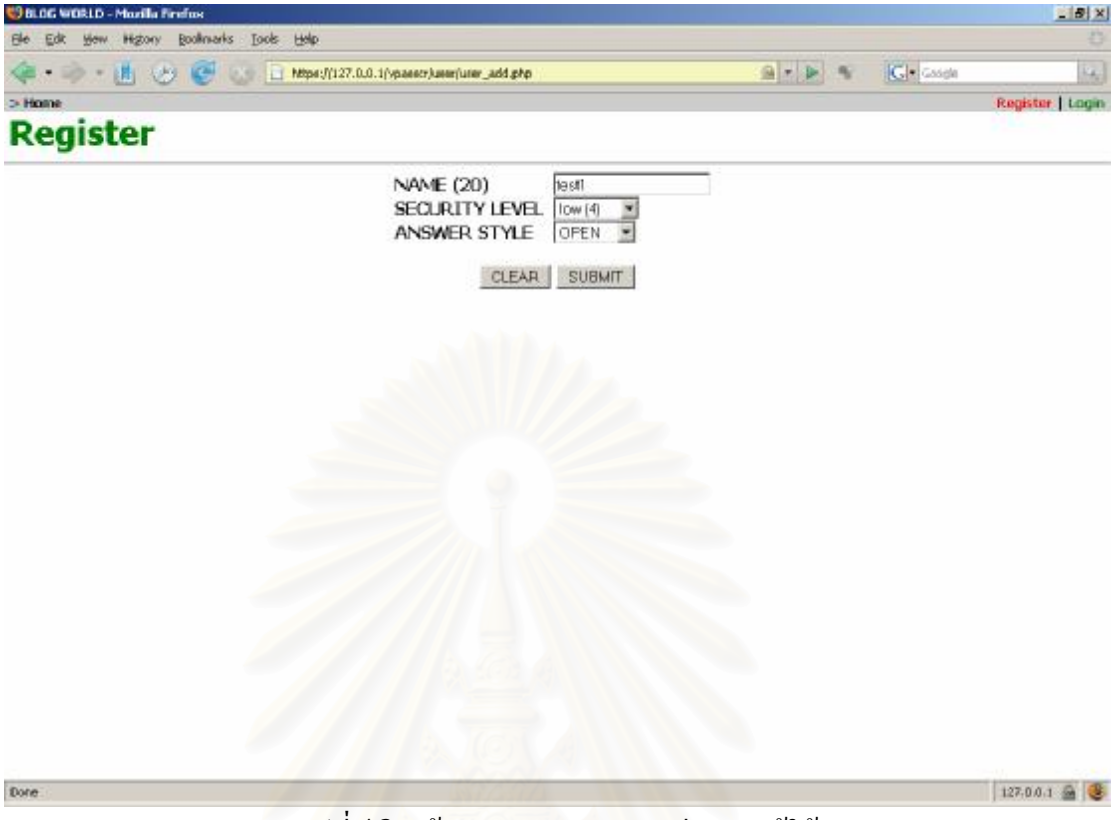
งานวิจัยนี้เสนออีกแนวทางในการพิสูจน์ตัวตนของรหัสผ่านแบบรูปภาพ โดยนำคำถามท้าทาย-ตอบสนองมาใช้ในการพิสูจน์ตัวตน

4.1 ขั้นตอนการทำงาน

4.1.1 **การสร้างคำสำคัญส่วนตัว** เริ่มต้นด้วยการเลือกเมนู Register ทางด้านขวาบนของหน้าจอดังแสดงในรูปที่ 4.1

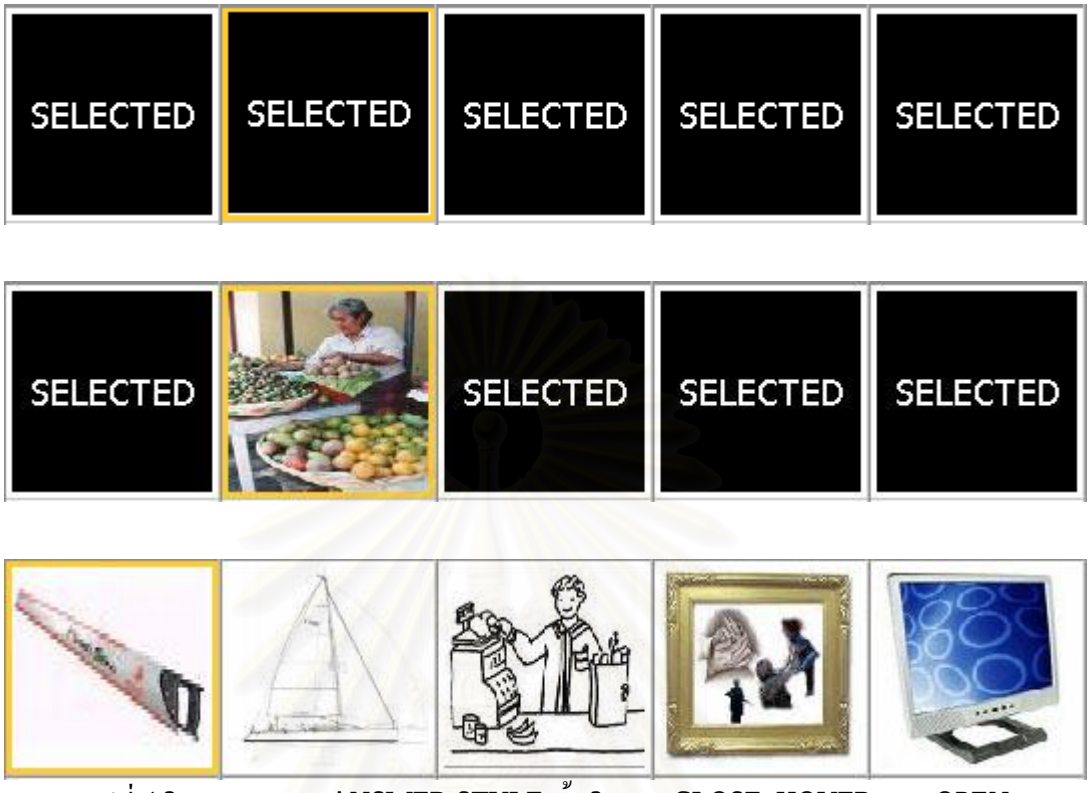
รูปที่ 4.1 ตัวอย่างหน้าจอการสร้างคำสำคัญส่วนตัว

หน้าจอถัดมาเป็นการกรอกรายละเอียดของผู้ใช้โดยมีรายละเอียดดังนี้



รูปที่ 4.2 หน้าจอการกรอกรายละเอียดของผู้ใช้

1. NAME (20) ชื่อบัญชีผู้ใช้ ความยาวไม่เกิน 20 ตัวอักษร
2. SECURITY LEVEL ระดับความปลอดภัยของบัญชีผู้ใช้ หรือจำนวนคำสำคัญของผู้ใช้ ซึ่งมีผลโดยตรงกับการพิสูจน์ตัวตน ถ้าหากผู้ใช้มีระดับความปลอดภัยสูง รูปภาพที่ใช้ในการพิสูจน์ตัวตนก็จะถูกสุ่มออกมามากกว่าผู้ใช้ที่มีระดับความปลอดภัยต่ำ ซึ่งทำให้การพยายามเข้าสู่ระบบของผู้ไม่ประสงค์ดีทำได้ลำบาก ระดับความปลอดภัยแบ่งออกเป็น 3 ระดับดังนี้
   - low (4) ความปลอดภัยระดับต่ำ ผู้ใช้มีคำสำคัญ 4 คำ
   - basic (6) ความปลอดภัยระดับกลาง ผู้ใช้มีคำสำคัญ 6 คำ
   - high (8) ความปลอดภัยระดับสูง ผู้ใช้มีคำสำคัญ 8 คำ
3. ANSWER STYLE ลักษณะของกล่องคำตอบในหน้าจอการพิสูจน์ตัวตน จุดประสงค์คือใช้ซ่อนรูปภาพที่ผู้ใช้เลือก เพื่อต้านทานการโจมตีแบบมองข้ามไหล่ มี 3 แบบดังนี้
   - CLOSE ไม่ทำการแสดงรูปภาพที่เลือกแล้วในกล่องคำตอบ
   - HOVER จะทำการแสดงรูปภาพที่เลือกแล้วในกล่องคำตอบ เมื่อนำเมาส์ไปวางไว้บนรูปนั้นๆ
   - OPEN ไม่ป้องกันการโจมตีแบบมองข้ามไหล่ แสดงรูปภาพที่เลือกทั้งหมดในกล่องคำตอบ

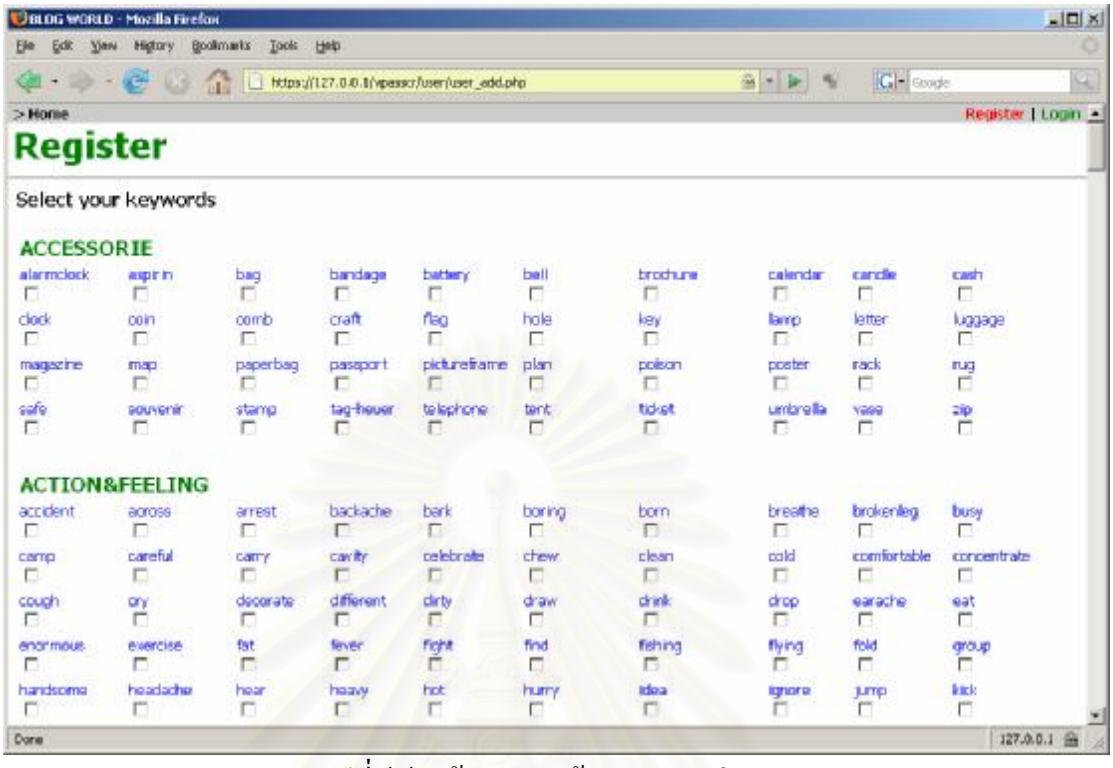


รูปที่ 4.3 ลักษณะของ ANSWER STYLE ทั้ง 3 แบบ CLOSE, HOVER และ OPEN

ถ้าหากกรอกข้อมูลผิดพลาด ต้องการล้างข้อมูลที่กรอกให้เลือกที่ปุ่ม CLEAR ทางด้านล่างของจอภาพ หรือ ถ้าหากกรอกข้อมูลครบถ้วนต้องการยืนยันให้กดปุ่ม SUBMIT

ในกรณีที่ผู้ใช้ไม่กรอกชื่อหรือกรอกชื่อที่มีอยู่แล้วในระบบแล้วกดปุ่ม SUBMIT ซอฟต์แวร์จะย้อนกลับมาที่หน้ากรอกรายละเอียดของผู้ใช้ใหม่โดยอัตโนมัติ

ต่อมาเป็นการเลือกคำสำคัญส่วนตัว คำสำคัญจะถูกแบ่งออกเป็นหมวดหมู่ด้วยตัวหนังสือขนาดใหญ่สีเขียวดังแสดงในรูปที่ 4.4



รูปที่ 4.4 หน้าจอการสร้างคำสำคัญส่วนตัว

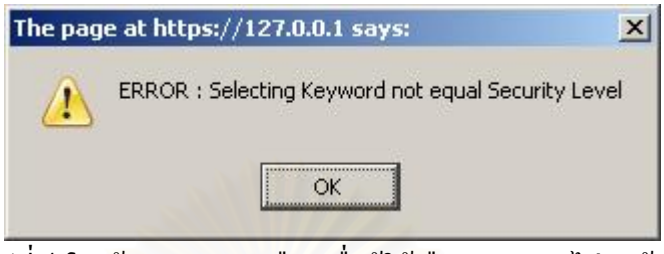
หากต้องการทราบว่าคำสำคัญประกอบไปด้วยรูปภาพอะไรบ้าง ให้ทำการเลือกที่คำสำคัญที่ต้องการทราบ จะปรากฏหน้าจอใหม่แสดงรูปภาพของคำสำคัญขึ้นมาดังแสดงในรูปที่ 4.5

รูปที่ 4.5 หน้าจอแสดงรูปภาพของคำสำคัญ alarmclock

ถ้าหากต้องการคำสำคัญคำไหนให้เลือกที่กล่องสี่เหลี่ยมใต้คำสำคัญคำนั้น หากต้องการเลือกคำสำคัญใหม่ทั้งชุดให้เลือกที่ปุ่ม CLEAR ด้านล่างสุดของจอภาพ หรือถ้าเลือกคำสำคัญครบแล้วให้เลือกที่ปุ่ม SUBMIT ปุ่มถัดมา

ในกรณีที่ไม่เลือกคำสำคัญ, เลือกคำสำคัญไม่ครบหรือเลือกคำสำคัญเกินจากระดับความ

ปลอดภัยของผู้ใช้ ซอฟต์แวร์จะแสดงข้อความเตือนดังรูปที่ 4.6 แล้วย้อยกลับไปหน้าเลือกคำสำคัญอีกครั้ง



รูปที่ 4.6 หน้าจอแสดงคำเตือนเมื่อผู้ใช้เลือกคำสำคัญไม่ถูกต้อง

เมื่อเลือกคำสำคัญส่วนตัวเรียบร้อยแล้ว ซอฟต์แวร์จะทำการแสดงรูปภาพประจำคำสำคัญที่ผู้ใช้ได้เลือก โดยแต่ละคำจะมีรูปภาพประจำคำอยู่ 4 รูป เพื่อให้ผู้ใช้เกิดความคุ้นเคยกับรูปภาพชุดดังกล่าวดังแสดงในรูปที่ 4.7 คำสำคัญที่ผู้ใช้เลือกคือ alarmclock, aspirin, bag และ bandage

รูปที่ 4.7 ตัวอย่างหน้าจอแสดงรูปภาพประจำคำสำคัญที่ผู้ใช้เลือก

เมื่อดูรูปภาพของคำสำคัญเป็นที่เรียบร้อยแล้ว ให้กดปุ่ม OK ทางด้านล่างสุดของจอภาพเพื่อสิ้นสุดการสร้างคำสำคัญส่วนตัว ซอฟต์แวร์จะพามาที่หน้าการเข้าสู่ระบบเป็นขั้นตอนต่อไป

4.1.2 **การเข้าสู่ระบบ** ในหน้าแรกของซอฟต์แวร์ให้เลือกที่เมนู Login ทางด้านขวาบนเพื่อทำการเข้าสู่ระบบดังแสดงในรูปที่ 4.8

รูปที่ 4.8 เมนู Login ในหน้าแรกของซอฟต์แวร์

กล่อง LOGIN จะถูกแสดงขึ้นมาบนจอภาพ ทำการกรอกชื่อผู้ใช้ลงในกล่อง name แล้วกดปุ่ม Login ถ้าหากรายชื่อที่กรอกไม่มีอยู่ในระบบ ซอฟต์แวร์จะพาย้อนกลับมาในหน้าจอนี้อีกครั้ง ถ้าหากรายชื่อมีอยู่ในระบบ ซอฟต์แวร์จะพาไปในหน้าจอของการพิสูจน์ตัวตนต่อไป

รูปที่ 4.9 กล่อง Login สำหรับกรอกชื่อผู้ใช้เพื่อเข้าสู่ระบบ

ในหน้าจอของการพิสูจน์ตัวตนจะแบ่งออกเป็น 3 ส่วนใหญ่ๆคือ

1. ชุดรูปภาพสำหรับการพิสูจน์ตัวตน
2. คำถามท้าทาย
3. กล่องคำตอบ

ผู้ใช้มีหน้าที่อ่านเงื่อนไขของคำถามท้าทายแล้วเลือกภาพจากชุดรูปภาพของการพิสูจน์ตัวตนลงในกล่องคำตอบตามเงื่อนไขนั้นๆให้ถูกต้อง

ในชุดรูปภาพสำหรับพิสูจน์ตัวตนนั้นจะประกอบไปด้วยรูปภาพของผู้ใช้และรูปภาพอื่นๆผสมกันอยู่ซึ่งจำนวนของรูปภาพแต่ละชนิดขึ้นอยู่กับคำถามท้าทายที่ใช้ และ ระดับความปลอดภัยของผู้ใช้ดังแสดงในรูปภาพที่ 4.10

รูปที่ 4.10 ตัวอย่างหน้าจอการพิสูจน์ตัวตน

จากรูปภาพที่ 4.10 คำถามท้าทายคือ ให้เลือกรูปภาพทั้งหมดโดยต้องมีอยู่ในทั้งสองแถว รูปภาพส่วนตัวของผู้ใช้ที่เลือกไว้คือ alarmclock, aspirin, bag และ bandage ซึ่งในชุดรูปภาพสำหรับการพิสูจน์ตัวตนชุดนี้ถูกสุ่มออกมาเพียง 3 รูปคือ alarmclock, aspirin และ bag ตามที่ล้อมกรอบไว้ด้วยเส้นประ หน้าที่ของผู้ใช้คือเลือกรูปภาพ 3 รูปนี้ยังไงก็ได้ให้อยู่ในทั้งสองแถว ดังที่แสดงไว้ในช่องคำตอบ ซึ่งได้ทำเส้นประไว้เพื่อให้เห็นตำแหน่งของรูปภาพของผู้ใช้เช่นเดียวกัน

เมื่อเลือกรูปภาพลงในกล่องคำตอบเรียบร้อยแล้วให้ยืนยันโดยกดปุ่ม LOGIN ในกรณีที่ผู้ใช้เลือกภาพไม่ครบแล้วกดปุ่มยืนยัน ซอฟต์แวร์จะพากลับมาที่หน้าพิสูจน์ตัวตนโดยยังคงเก็บสถานะของรูปภาพที่เลือกไปแล้วไว้เพื่อให้ผู้ใช้เลือกต่อได้ ในกรณีที่ผู้ใช้เลือกรูปภาพครบแต่ไม่ตรงกับเงื่อนไขของคำถามท้าทาย ซอฟต์แวร์จะนำผู้ใช้กลับออกสู่หน้าแรกระบบ

หากผู้ใช้เลือกรูปภาพถูกต้องตามเงื่อนไข การเข้าสู่ระบบก็จะเสร็จสมบูรณ์ ซอฟต์แวร์จะนำผู้ใช้ไปสู่หน้าแรกของระบบอีกครั้ง และได้รับสิทธิ์ของผู้ใช้นั้นๆโดยดูได้จากเมนูด้านบนดังแสดงในรูปภาพที่ 4.11

รูปที่ 4.11 เมนูของผู้ใช้ปรากฏขึ้นเมื่อเข้าสู่ระบบสำเร็จ

ตามลำดับขั้นการเข้าสู่ระบบที่พูดมาจะพบว่ามีจุดอ่อนอยู่คือในขั้นตอนของการกรอกชื่อผู้ใช้ ไม่ว่าใครถ้าหากทราบชื่อผู้ใช้ก็สามารถกรอกชื่อผู้ใช้เพื่อเข้าสู่หน้าการพิสูจน์ตัวตนได้ และการที่สามารถเข้าสู่หน้าการพิสูจน์ตัวตนได้หลายๆครั้ง ผู้ไม่ประสงค์ดีสามารถนำเอาชุดรูปภาพการพิสูจน์ตัวตนและคำถามท้าทายไปวิเคราะห์เพื่อหาคำสำคัญของผู้ใช้ออกมาได้ ซอฟต์แวร์จึงได้เพิ่มกฎในการเข้าสู่ระบบ เพื่อรักษาความปลอดภัยขึ้นมาอีก 2 ข้อดังนี้

1. ถ้าหากเข้าหน้าพิสูจน์ตัวตนครบ 5 ครั้งโดยไม่ทำการ LOGIN บัญชีผู้ใช้จะถูกระงับ
2. ถ้าหากพิสูจน์ตัวตนผิดครบ 3 ครั้ง บัญชีผู้ใช้จะถูกระงับ

ซึ่งหากผู้ใช้ตัวจริงๆเข้ามาในระบบแล้วพบว่าระบบถูกระงับอยู่ สามารถติดต่อผู้ดูแลระบบเพื่อยกเลิกการระงับบัญชีผู้ใช้ได้

4.2 เครื่องมือที่ใช้ในการพัฒนา

ผู้วิจัยได้ใช้เครื่องมือในการพัฒนาซอฟท์แวร์ดังนี้

1. พีเอชพี (PHP) รุ่น 4.3.8 สำหรับเป็นภาษาในการเขียนซอฟท์แวร์
2. อาพาเช (Apache) รุ่น 1.3.31 สำหรับเป็นเว็บเซิร์ฟเวอร์
3. มายเอสคิวแอล (MySQL) รุ่น 4.0.20a-nt สำหรับเป็นฐานข้อมูล
4. อีดิทพลัส (EditPlus) รุ่น 2.12(76) สำหรับเป็นเครื่องมือในการพัฒนาซอฟท์แวร์
5. โอเพนเอสเอสแอล (openssl) รุ่น 0.9.8g

บทที่ 5
สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

งานวิจัยนี้ได้พัฒนาการพิสูจน์ตัวตนโดยใช้คำถามท้าทาย-ตอบสนอง โดยนำเสนอในรูปแบบของสมุดบันทึกออนไลน์ มีรูปภาพในระบบทั้งหมด 4027 รูป แบ่งออกเป็น 37 กลุ่ม การพิสูจน์ตัวตนทำได้ง่าย เพราะจากการศึกษาพบว่า มนุษย์สามารถจดจำรูปภาพได้ดีกว่าตัวอักษร สิ่งที่ผู้ใช้ต้องจำคือคำสำคัญของผู้ใช้

การต้านทานสปายแวร์สามารถทำได้เนื่องจากเทคนิคการสุ่ม คำถามท้าทายและรูปภาพที่ใช้ในการพิสูจน์ตัวตนแต่ละรอบจะถูกแสดงออกมาในลักษณะสุ่ม ทำให้คำตอบที่ได้ในแต่ละรอบของการพิสูจน์ตัวตนนั้นแตกต่างกันออกไป

จากการเปรียบเทียบกับรหัสผ่านแบบตัวอักษร เซตคำตอบที่เป็นไปได้ของงานวิจัยน้อยกว่ามากเนื่องจากลักษณะของการพิสูจน์ตัวตน แต่เมื่อเทียบกับรหัสผ่านแบบรูปภาพด้วยกันแล้วรหัสผ่านแบบรูปภาพโดยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองมีข้อได้เปรียบคือจดจำง่ายและต้านทานสปายแวร์ได้

5.2 ปัญหาและอุปสรรค

1. รูปภาพที่นำมาใช้นั้นนำมาจากอินเตอร์เน็ตทั้งหมดซึ่งค่อนข้างใช้เวลามากในการค้นหา อีกทั้งรูปภาพที่ได้มามีความหลากหลายในเรื่องของชนิดภาพ ความละเอียดของภาพ บางคำหาภาพยากทำให้จำนวนภาพของคำนั้นๆไม่ได้ตามเป้าหมายที่วางไว้

2. การแบ่งกลุ่มของคำสำคัญบางกลุ่มอาจจะมีจำนวนคำมาก บางกลุ่มอาจจะมีจำนวนคำน้อย ผู้พัฒนาแบ่งกลุ่มของคำออกโดยยึดตัวเองเป็นหลัก ซึ่งในจุดนี้ยังไม่มีมาตรฐานของการจัดกลุ่มคำมารองรับ

5.3 แนวทางการวิจัยต่อไป

ประเด็นที่งานวิจัยนี้ยังไม่ได้ศึกษา และสามารถทำการวิจัยเพิ่มเติมได้ในอนาคตได้แก่

1. การจัดกลุ่มคำสำคัญ หรือ การจัดกลุ่มภาพ เป็นเรื่องที่ยังไม่มีมาตรฐานออกมา ถ้าหากมีวิธีการจัดกลุ่มที่มีมาตรฐานได้นั้น จะทำให้การพัฒนาการพิสูจน์ตัวตนแบบรูปภาพมีความเป็นระเบียบมากขึ้น
2. การใช้งานซอฟต์แวร์ให้ได้ประสิทธิภาพตามที่วิเคราะห์ ต้องใช้งานภายใต้ขอบเขตของการวิจัยที่กำหนดไว้

5.4 การเปรียบเทียบเซตคำตอบของงานวิจัยกับรหัสผ่านแบบตัวอักษร

ในการเปรียบเทียบในตารางที่ 5.1 มีรายละเอียดดังนี้

- รหัสผ่านแบบตัวอักษรนับอักษรบนแป้นพิมพ์จำนวน 94 ตัวอักษร (ไม่รวม Spacebar)
- งานวิจัยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนองโดยแบ่งความปลอดภัยออกเป็น 3 ระดับ ระดับต่ำ ระดับกลาง และระดับสูง และทดสอบสำหรับระดับความปลอดภัยที่สูงขึ้นไปอีก 3 ระดับคือ ระดับ 10 คำสำคัญ, 20 คำสำคัญ และ 40 คำสำคัญ ตามลำดับ

ตาราง 5.1 ตารางเปรียบเทียบเซตคำตอบของรหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนองกับรหัสผ่านแบบตัวอักษร

ชนิดของรหัสผ่าน	**ระดับความปลอดภัย**											
รหัสผ่านแบบตัวอักษร	4 ตัวอักษร		6 ตัวอักษร		8 ตัวอักษร		10 ตัวอักษร		20 ตัวอักษร		40 ตัวอักษร	
	7.807×10^{7}		6.898×10^{11}		6.096×10^{15}		1.111×10^{20}		2.261×10^{39}		2.969×10^{82}	
รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
ตอบสนอง	**คำ**	**ค่าประมาณ**	**คำ**	**ค่าประมาณ**	**คำ**	**ค่าประมาณ**	**คำ**	**ค่าประมาณ**	**คำ**	**ค่าประมาณ**	**คำ**	**ค่าประมาณ**
1. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกติดกัน 1 ตำแหน่ง	2	1.011×10^{1}	2	1.390×10^{1}	2	1.776×10^{1}	2	2.166×10^{1}	2	4.140×10^{1}	2	8.122×10^{1}
	3	1.950×10^{1}	3	2.720×10^{1}	3	3.500×10^{1}	3	4.285×10^{1}	3	8.250×10^{1}	3	1.622×10^{2}
	4	5.720×10^{1}	4	7.285×10^{1}	4	8.866×10^{1}	4	1.045×10^{2}	4	1.842×10^{2}	4	3.441×10^{2}
			5	3.060×10^{2}	5	3.135×10^{2}	5	3.322×10^{2}	5	4.684×10^{2}	5	7.778×10^{2}
			6	2.652×10^{3}	6	1.776×10^{3}	6	1.495×10^{3}	6	1.380×10^{3}	6	1.882×10^{3}
					7	2.131×10^{4}	7	1.096×10^{4}	7	4.833×10^{3}	7	4.899×10^{3}
					8	1.279×10^{6}	8	1.735×10^{5}	8	2.071×10^{4}	8	1.379×10^{4}
							9	1.406×10^{7}	9	1.132×10^{5}	9	4.231×10^{4}
									10	8.384×10^{5}	10	1.423×10^{5}
									11	9.162×10^{6}	11	5.293×10^{5}
									12	1.710×10^{8}	12	2.198×10^{6}
									13	7.269×10^{9}	13	1.031×10^{7}
									14	1.679×10^{12}	14	5.542×10^{7}
											15	3.465×10^{8}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
1. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกติดกัน 1 ตำแหน่ง (ต่อ)											16	2.573×10^{9}
											17	2.326×10^{10}
											18	2.646×10^{11}
											19	3.953×10^{12}
											20	8.240×10^{13}
											21	2.622×10^{15}
											22	1.477×10^{17}
											23	1.969×10^{19}
											24	1.488×10^{22}
2. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกไม่ติดกันเลย	2	2.527×10^{0}	2	2.781×10^{0}	2	2.961×10^{0}	2	3.095×10^{0}	2	3.450×10^{0}	2	3.691×10^{0}
	3	6.500×10^{0}	3	6.800×10^{0}	3	7.000×10^{0}	3	7.142×10^{0}	3	7.500×10^{0}	3	7.727×10^{0}
	4	2.860×10^{1}	4	2.428×10^{1}	4	2.216×10^{1}	4	2.090×10^{1}	4	1.842×10^{1}	4	1.720×10^{1}
			5	1.530×10^{2}	5	1.045×10^{2}	5	8.305×10^{1}	5	5.205×10^{1}	5	4.093×10^{1}
			6	2.652×10^{3}	6	8.882×10^{2}	6	4.983×10^{2}	6	1.726×10^{2}	6	1.045×10^{2}
					7	2.131×10^{4}	7	5.481×10^{3}	7	6.904×10^{2}	7	2.882×10^{2}
							8	1.735×10^{5}	8	3.452×10^{3}	8	8.624×10^{2}
									9	2.265×10^{4}	9	2.821×10^{3}
									10	2.096×10^{5}	10	1.016×10^{4}
									11	3.054×10^{6}	11	4.071×10^{4}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
2. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกไม่ติดกันเลย (ต่อ)									12	8.551×10^{7}	12	1.832×10^{5}
									13	7.269×10^{9}	13	9.379×10^{5}
											14	5.542×10^{6}
											15	3.850×10^{7}
											16	3.216×10^{8}
											17	3.323×10^{9}
											18	4.410×10^{10}
											19	7.906×10^{11}
											20	2.060×10^{13}
											21	8.740×10^{14}
											22	7.385×10^{16}
											23	1.969×10^{19}
3. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกติดกัน 1 ตำแหน่ง	4	1.853×10^{1}	4	1.854×10^{1}	4	2.009×10^{1}	4	2.214×10^{1}	4	3.435×10^{1}	4	6.050×10^{1}
			6	3.094×10^{1}	6	3.028×10^{1}	6	3.162×10^{1}	6	4.465×10^{1}	6	7.545×10^{1}
					8	5.537×10^{1}	8	5.202×10^{1}	8	6.081×10^{1}	8	9.409×10^{1}
							10	1.064×10^{2}	10	8.985×10^{1}	10	1.201×10^{2}
									12	1.480×10^{2}	12	1.594×10^{2}
									14	2.794×10^{2}	14	2.219×10^{2}
									16	6.248×10^{2}	16	3.268×10^{2}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
3. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกติดกัน 1 ตำแหน่ง (ต่อ)									18	1.725×10^{3}	18	5.134×10^{2}
											20	8.673×10^{2}
											22	1.589×10^{3}
											24	3.193×10^{3}
											26	7.111×10^{3}
											28	1.779×10^{4}
											30	5.080×10^{4}
											32	1.689×10^{5}
4. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกไม่ติดกันเลย	4	4.634×10^{0}	4	3.709×10^{0}	4	3.349×10^{0}	4	3.164×10^{0}	4	2.862×10^{0}	4	2.750×10^{0}
			6	7.735×10^{0}	6	6.056×10^{0}	6	5.270×10^{0}	6	4.059×10^{0}	6	3.593×10^{0}
					8	1.384×10^{1}	8	1.040×10^{1}	8	6.081×10^{0}	8	4.704×10^{0}
							10	2.661×10^{1}	10	9.984×10^{0}	10	6.325×10^{0}
									12	1.850×10^{1}	12	8.859×10^{0}
									14	3.991×10^{1}	14	1.305×10^{1}
									16	1.041×10^{2}	16	2.043×10^{1}
									18	3.451×10^{2}	18	3.423×10^{1}
											20	6.195×10^{1}
											22	1.223×10^{2}
											24	2.661×10^{2}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
4. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกไม่ติดกันเลย (ต่อ)											26	6.465×10^{2}
											28	1.779×10^{3}
											30	5.645×10^{3}
5. เลือกรูปภาพส่วนตัวทั้งหมดโดยต้องมีอยู่ทั้ง 2 แถว	2	3.640×10^{0}	2	4.250×10^{0}	2	4.714×10^{0}	2	5.078×10^{0}	2	6.124×10^{0}	2	6.909×10^{0}
	3	3.640×10^{0}	3	4.533×10^{0}	3	5.238×10^{0}	3	5.803×10^{0}	3	7.485×10^{0}	3	8.793×10^{0}
	4	5.005×10^{0}	4	6.580×10^{0}	4	7.857×10^{0}	4	8.898×10^{0}	4	1.206×10^{1}	4	1.459×10^{1}
			5	1.098×10^{1}	5	1.343×10^{1}	5	1.545×10^{1}	5	2.168×10^{1}	5	2.671×10^{1}
			6	2.013×10^{1}	6	2.496×10^{1}	6	2.895×10^{1}	6	4.130×10^{1}	6	5.129×10^{1}
					7	4.972×10^{1}	7	5.758×10^{1}	7	8.179×10^{1}	7	1.013×10^{2}
							8	1.214×10^{2}	8	1.672×10^{2}	8	2.041×10^{2}
									9	3.527×10^{2}	9	4.180×10^{2}
									10	7.675×10^{2}	10	8.691×10^{2}
									11	1.726×10^{3}	11	1.834×10^{3}
									12	4.028×10^{3}	12	3.929×10^{3}
									13	9.784×10^{3}	13	8.552×10^{3}
											14	1.891×10^{4}
											15	4.256×10^{4}
											16	9.749×10^{4}
											17	2.274×10^{5}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
5. เลือกรูปภาพส่วนตัวทั้งหมดโดยต้องมีอยู่ทั้ง 2 แถว (ต่อ)											18	5.412×10^{5}
											19	1.314×10^{6}
											20	3.261×10^{6}
											21	8.280×10^{6}
											22	2.152×10^{7}
											23	5.741×10^{7}
6. ไม่เลือกรูปภาพส่วนตัว 1 รูป	2	2.275×10^{0}	2	2.125×10^{0}	2	2.062×10^{0}	2	2.031×10^{0}	2	1.990×10^{0}	2	1.986×10^{0}
	3	2.022×10^{0}	3	2.060×10^{0}	3	2.115×10^{0}	3	2.166×10^{0}	3	2.335×10^{0}	3	2.471×10^{0}
	4	2.085×10^{0}	4	2.318×10^{0}	4	2.512×10^{0}	4	2.669×10^{0}	4	3.138×10^{0}	4	3.497×10^{0}
			5	2.884×10^{0}	5	3.288×10^{0}	5	3.614×10^{0}	5	4.584×10^{0}	5	5.335×10^{0}
			6	3.906×10^{0}	6	4.658×10^{0}	6	5.270×10^{0}	6	7.119×10^{0}	6	8.574×10^{0}
					7	7.098×10^{0}	7	8.214×10^{0}	7	1.162×10^{1}	7	1.434×10^{1}
					8	1.164×10^{1}	8	1.365×10^{1}	8	1.983×10^{1}	8	2.478×10^{1}
							9	2.427×10^{1}	9	3.526×10^{1}	9	4.405×10^{1}
							10	4.643×10^{1}	10	6.523×10^{1}	10	8.034×10^{1}
									11	1.255×10^{2}	11	1.500×10^{2}
									12	2.518×10^{2}	12	2.865×10^{2}
									13	5.268×10^{2}	13	5.592×10^{2}
									14	1.153×10^{3}	14	1.114×10^{3}

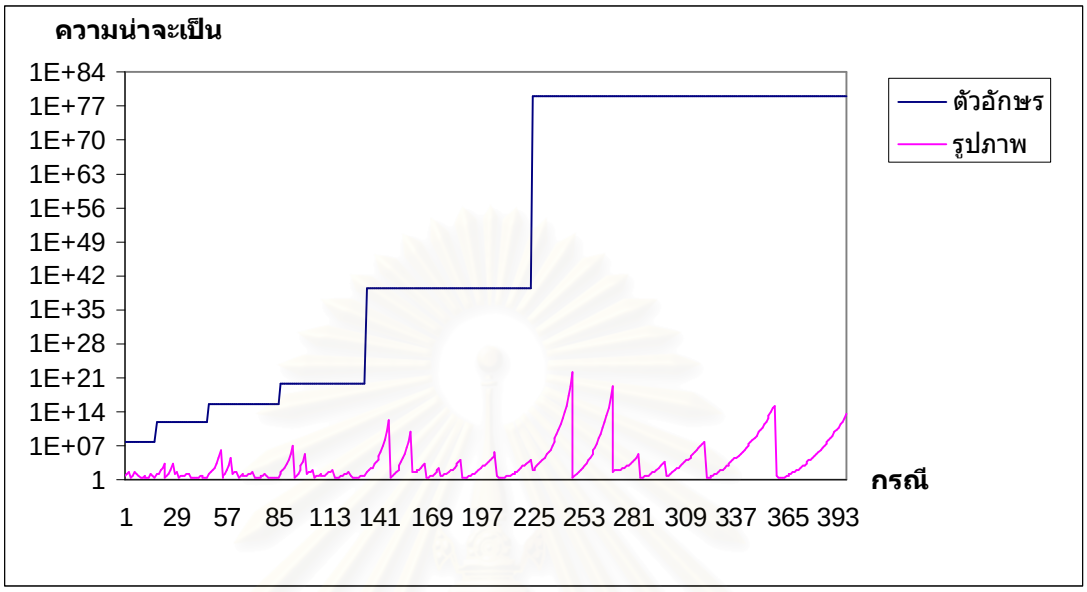
รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
6. ไม่เลือกรูปภาพส่วนตัว 1 รูป (ต่อ)									15	2.649×10^{3}	15	2.270×10^{3}
									16	6.416×10^{3}	16	4.722×10^{3}
									17	1.647×10^{4}	17	1.003×10^{4}
									18	4.510×10^{4}	18	2.180×10^{4}
									19	1.329×10^{5}	19	4.842×10^{4}
									20	4.262×10^{5}	20	1.100×10^{5}
											21	2.562×10^{5}
											22	6.116×10^{5}
											23	1.497×10^{6}
											24	3.767×10^{6}
											25	9.749×10^{6}
											26	2.599×10^{7}
											27	7.151×10^{7}
											28	2.034×10^{8}
											29	5.996×10^{8}
											30	1.835×10^{9}
											31	5.851×10^{9}
											32	1.948×10^{10}
											33	6.802×10^{10}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
6. ไม่เลือกรูปภาพส่วนตัว 1 รูป (ต่อ)											34	2.499×10^{11}
											35	9.711×10^{11}
											36	4.012×10^{12}
											37	1.774×10^{13}
											38	8.467×10^{13}
											39	4.400×10^{14}
											40	2.520×10^{15}
7. ไม่เลือกรูปภาพส่วนตัว 2 รูป	2	1.516×10^{1}	2	1.020×10^{1}	2	8.250×10^{0}	2	7.222×10^{0}	2	5.447×10^{0}	2	4.685×10^{0}
	3	6.066×10^{0}	3	4.533×10^{0}	3	3.928×10^{0}	3	3.611×10^{0}	3	3.072×10^{0}	3	2.852×10^{0}
	4	3.707×10^{0}	4	3.090×10^{0}	4	2.870×10^{0}	4	2.768×10^{0}	4	2.642×10^{0}	4	2.630×10^{0}
			5	2.596×10^{0}	5	2.583×10^{0}	5	2.610×10^{0}	5	2.774×10^{0}	5	2.941×10^{0}
			6	2.500×10^{0}	6	2.662×10^{0}	6	2.811×10^{0}	6	3.297×10^{0}	6	3.693×10^{0}
					7	3.042×10^{0}	7	3.346×10^{0}	7	4.282×10^{0}	7	5.025×10^{0}
					8	3.802×10^{0}	8	4.335×10^{0}	8	5.965×10^{0}	8	7.262×10^{0}
							9	6.069×10^{0}	9	8.815×10^{0}	9	1.101×10^{1}
							10	9.171×10^{0}	10	1.373×10^{1}	10	1.739×10^{1}
									11	2.247×10^{1}	11	2.846×10^{1}
									12	3.855×10^{1}	12	4.808×10^{1}
									13	6.932×10^{1}	13	8.364×10^{1}

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
7. ไม่เลือกรูปภาพส่วนตัว 2 รูป (ต่อ)									14	1.307×10^2	14	1.495×10^2
									15	2.589×10^2	15	2.744×10^2
									16	5.403×10^2	16	5.166×10^2
									17	1.191×10^3	17	9.972×10^2
									18	2.793×10^3	18	1.972×10^3
									19	6.997×10^3	19	4.001×10^3
									20	1.889×10^4	20	8.319×10^3
											21	1.774×10^4
											22	3.883×10^4
											23	8.727×10^4
											24	2.016×10^5
											25	4.791×10^5
											26	1.173×10^6
											27	2.962×10^6
											28	7.728×10^6
											29	2.086×10^7
											30	5.842×10^7
											31	1.700×10^8
											32	5.157×10^8

รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทายตอบสนอง	ระดับต่ำ		ระดับกลาง		ระดับสูง		ระดับ 10		ระดับ 20		ระดับ 40	
	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ	คำ	ค่าประมาณ
7. ไม่เลือกรูปภาพส่วนตัว 2 รูป (ต่อ)											33	1.635×10^{9}
											34	5.437×10^{9}
											35	1.904×10^{10}
											36	7.055×10^{10}
											37	2.780×10^{11}
											38	1.173×10^{12}
											39	5.344×10^{12}
											40	2.651×10^{13}

จากตารางที่ 5.1 เราสามารถสรุปเป็นกราฟได้ดังรูปที่ 5.1



รูปที่ 5.1 กราฟเปรียบเทียบเซตคำตอบของงานวิจัยกับรหัสผ่านแบบรูปภาพ

จากกราฟพบว่าเซตคำตอบของการพิสูจน์ตัวตนแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนองเมื่อเทียบกับรหัสผ่านแบบตัวอักษรแล้วมีค่าน้อยกว่ามากเนื่องจากลักษณะของการพิสูจน์ตัวตน

5.5 การวิเคราะห์ความเสี่ยงจากการดักหน้าจอ

WinVNC [19] คือโปรแกรมตรวจจับหน้าจอผ่านทางระบบเครือข่าย แบ่งออกเป็น 2 ส่วน คือWinVNC เปิดในเครื่องที่ต้องการตรวจจับหน้าจอ และ VNC Viewer ใช้ดูและควบคุมเครื่องที่ตรวจจับผ่านระบบเครือข่าย

ในหัวข้อนี้ WinVNC รุ่น 3.3.3 R7 ถูกมาใช้จำลองเหตุการณ์ที่ผู้ไม่ประสงค์ดีทำการดักหน้าจอในขั้นตอนของการพิสูจน์ตัวตนเพื่อวิเคราะห์ว่าสิ่งที่ผู้ไม่ประสงค์ดีได้รับจากการดักหน้าจอไปนั้นมีอะไรบ้าง

1. ผู้ใช้งาน diew ระดับความปลอดภัย 4 คำสำคัญคือ speaker, shoe, lcd และ monitor

รูปที่ 5.2 ตัวอย่างหน้าจอที่ถูกดักของผู้ใช้งาน diew

สิ่งที่ได้จากการดักหน้าจอ

- จากคำถาม “เลือกรูปภาพทั้งหมด” รูปภาพที่ไม่ถูกเลือก ไม่ใช่รูปภาพของผู้ใช้
- จากจำนวนช่องของกล่องคำตอบ รหัสความปลอดภัยคือ 4
- จากคำถาม “เลือกรูปภาพทั้งหมด” และรหัสความปลอดภัยที่ได้ รูปภาพของผู้ใช้ในกล่องคำตอบที่เป็นไปได้มี 3 กรณีคือ 2, 3 หรือ 4 รูป
- จากคำถาม “มีรูปภาพติดกัน 1 คู่” หากทราบรูปภาพของผู้ใช้ในกล่องคำตอบมีโอกาสที่รูปภาพ 1 ใน 2 รูปที่ขนาบข้างอยู่นั้นจะเป็นรูปภาพของผู้ใช้ด้วย

2. ผู้ใช้งาน test1 ระดับความปลอดภัย 4 คำสำคัญคือ bamboo, broccoli, lettuce, onion

รูปที่ 5.3 ตัวอย่างหน้าจอที่ถูกดักของผู้ใช้งาน test1

สิ่งที่ได้จากการดักหน้าจอ

- จากคำถาม “เลือกรูปภาพทั้งหมด” รูปภาพที่ไม่ถูกเลือก ไม่ใช่รูปภาพของผู้ใช้
- จากจำนวนช่องของกล่องคำตอบ รหัสความปลอดภัยคือ 4
- จากคำถาม “เลือกรูปภาพทั้งหมด” และรหัสความปลอดภัยที่ได้ รูปภาพของผู้ใช้ในกล่องคำตอบที่เป็นไปได้มี 3 กรณีคือ 2, 3 หรือ 4 รูป
- จากคำถาม “รูปภาพไม่ติดกันเลย” หากทราบรูปภาพของผู้ใช้ในกล่องคำตอบ รูปภาพด้านซ้ายและขวาของรูปนั้นไม่ใช่รูปภาพของผู้ใช้

3. ผู้ใช้งาน nbuam ระดับความปลอดภัย 6 คำสำคัญคือ alarmclock, aspirin, bag, bandage, battery, bell

รูปที่ 5.4 ตัวอย่างหน้าจอที่ถูกดักของผู้ใช้งาน nbuam

สิ่งที่ได้จากการดักหน้าจอ

- จากคำถาม “ไม่เลือกรูปภาพ 2 รูป” 2 ใน 6 รูปจากรูปภาพที่ไม่ถูกเลือก คือ รูปภาพของผู้ใช้
- จากจำนวนช่องของกล่องคำตอบ รหัสความปลอดภัยคือ 6
- จากคำถาม “ไม่เลือกรูปภาพ 2 รูป” และรหัสความปลอดภัยที่ได้ รูปภาพของผู้ใช้ในกล่องคำตอบที่เป็นไปได้มี 4 กรณีคือ 0, 1, 2, 3 หรือ 4 รูป

4. ผู้ใช้งาน hardcore ระดับความปลอดภัย 8 คำสำคัญคือ alarmclock, aspirin, bag, bandage, bamboo, broccoli, lettuce และ onion

รูปที่ 5.5 ตัวอย่างหน้าจอที่ถูกดักของผู้ใช้งาน hardcore

สิ่งที่ได้จากการดักหน้าจอ

- จากคำถาม “เลือกรูปภาพทั้งหมด” รูปภาพที่ไม่ถูกเลือก ไม่ใช่รูปภาพของผู้ใช้
- จากจำนวนช่องของกล่องคำตอบ รหัสความปลอดภัยคือ 8
- จากคำถาม “เลือกรูปภาพทั้งหมด” และรหัสความปลอดภัยที่ได้ รูปภาพของผู้ใช้ในกล่องคำตอบที่เป็นไปได้มี 7 กรณีคือ 2, 3, 4, 5, 6, 7 หรือ 8 รูป
- จากคำถาม “เลือกให้อยู่ในทั้ง 2 แถว” และกรณีที่เป็นไปได้ 7 กรณี ที่รูปภาพจะมีได้ในกล่องคำตอบ จำนวนรูปภาพในแต่ละแถวที่เป็นไปได้มีดังนี้

ตารางที่ 5.2 จำนวนรูปภาพในแต่ละแถวที่เป็นไปได้ในคำถามเลือกรูปภาพทั้งหมดใน 2 แถว

จำนวนรูปภาพที่เป็นไปได้	**จำนวนรูปในแถวที่ 1 (รูป)**							**จำนวนรูปในแถวที่ 2 (รูป)**						
ในกล่องคำตอบ	1	2	3	4	5	6	7	1	2	3	4	5	6	7
1. 2 รูป	/							/						
2. 3 รูป	/								/					
		/						/						
3. 4 รูป	/									/				
		/							/					
			/					/						
4. 5 รูป	/										/			
		/								/				
			/						/					
				/				/						
5. 6 รูป	/											/		
		/									/			
			/							/				
				/					/					
					/			/						
6. 7 รูป	/												/	
		/										/		
			/								/			
				/						/				
					/				/					
						/		/						
7. 8 รูป	/													/
		/											/	
			/									/		
				/							/			
					/					/				
						/			/					
							/	/						

จากเหตุการณ์จำลองทั้ง 4 พบว่า ถึงแม้ระดับความปลอดภัยและคำถามท้าทายจะแตกต่างกัน ผู้ไม่ประสงค์ดีก็ไม่สามารถระบุคำสำคัญของผู้ใช้อย่างชัดเจนได้ เนื่องจาก คำสำคัญ, รูปภาพในการพิสูจน์ตัวตน และ คำถามท้าทายถูกแสดงออกมาในลักษณะสุ่ม

5.6 ข้อดีและขีดจำกัดของรหัสผ่านแบบรูปภาพชนิดต่างๆ

Passfaces มีข้อดีคือผู้ใช้สามารถจดจำใบหน้าได้ง่ายแต่จากการวิจัยพบว่าผู้ใช้งานมักจะเลือกใบหน้าที่อยู่ในสายพันธุ์เดียวกับตน ซึ่งอาจถูกเดารหัสผ่านได้ง่าย

Draw-a-Secret (DAS) สามารถใช้งานได้ง่าย แต่การพิสูจน์ตัวตนแต่ละครั้งจะต้องจำลำดับและตำแหน่งการวาดเส้นให้ถูกต้องซึ่งยากแก่การจดจำ

วาดลายเซ็นด้วยเมาส์ ผู้ใช้สามารถจดจำลายเซ็นได้ง่าย แต่ต้องทำการพิสูจน์ตัวตนด้วยเมาส์ซึ่งบางคนอาจจะไม่ถนัดการวาดภาพด้วยเมาส์จึงทำให้เกิดความลำบากในการใช้งาน

déjà vu การใช้งานระบบทำได้ง่าย รูปภาพเชิงความหมายที่นำมาใช้ถึงจะช่วยในการประหยัดพื้นที่ในการเก็บรูปภาพแต่การจดจำรูปภาพทำได้ยาก

รหัสผ่านแบบรูปภาพเพื่อป้องกันสปายแวร์ มีความปลอดภัยที่สูง แต่ต้องมองหารูปภาพของตัวเองจากรูปภาพจำนวน 121 รูปและต้องจดจำรหัสของรูปภาพทั้ง 16 รูปแบบให้ได้นั้นถือว่าทำได้ลำบาก

Passlogix การใช้งานทำได้สะดวกและสามารถจดจำรหัสผ่านได้ง่าย แต่เนื่องจากว่าช่วงของรหัสผ่านที่สร้างได้ขึ้นอยู่กับกิจกรรมที่สามารถกระทำได้บนโลกเสมือนนั้นๆซึ่งยังเป็นมีขีดจำกัดอยู่มาก

การใช้ภาพโปรดของตนบนโทรศัพท์มือถือ วิธีนี้สามารถจดจำรหัสผ่านได้ง่ายมาก แต่ผู้ที่รู้จักกับผู้ใช้ก็สามารถคาดเดารหัสผ่านของผู้ใช้ได้ง่ายเช่นกัน

รหัสผ่านแบบรูปภาพโดยใช้การพิสูจน์ตัวตนแบบคำถามท้าทาย-ตอบสนอง ระบบสามารถต้านทานสปาย์แวร์ได้เนื่องจากคำถามท้าทายและรูปภาพประจำคำสำคัญถูกแสดงออกมาแบบสุ่ม การจดจำทำได้ง่ายเนื่องจากว่าผู้ใช้จดจำเฉพาะคำสำคัญของตัวเอง

รหัสผ่านแบบรูปภาพแต่ละชนิดจะมีลักษณะแตกต่างกันดังแสดงในตารางที่ 5.3 ถึง 5.6

ตารางที่ 5.3 ลักษณะของรหัสผ่านแบบรูปภาพชนิดต่างๆ

ชื่อรหัสผ่านแบบรูปภาพ	การกระทำ		การจดจำได้ง่าย
	เลือกรูปภาพของผู้ใช้	เลือกรูปภาพตามลำดับ	
1. Passfaces	/		/
2. déjà vu	/		
3. Anti-Spyware Visual Password	/	/	
4. Passlogix		/	/
5. User favorite Image for mobile	/		/
6. Visual Password using Challenge-response authentication	/		/

ตารางที่ 5.4 เซตคำตอบของรหัสผ่านแบบรูปภาพชนิดต่างๆ

ชื่อรหัสผ่านแบบรูปภาพ	ช่วงของรหัสผ่าน	คำอธิบาย
1. Passfaces	N^K	N คือ จำนวนภาพในการพิสูจน์ตัวตนแต่ละรอบ, K คือ จำนวนรอบในการพิสูจน์ตัวตน
2. déjà vu	$C_{N,K}$	N คือจำนวนรูปภาพในระบบ, K คือกุญแจรูปภาพของผู้ใช้ในการพิสูจน์ตัวตนผู้ใช้ทำการเลือกรูปภาพที่เป็นกุญแจของตัวเองแบบไม่สนใจลำดับ
3. Anti-Spyware Visual Password	94^K	94 คือจำนวนปุ่มบนแป้นพิมพ์ที่กดได้ (ไม่รวม Spacebar) และ K คือจำนวนตัวอักษรของรหัสผ่าน
4. User favorite Image for mobile	$(N+1)^K$	N คือจำนวนรูปภาพในแต่ละรอบการพิสูจน์ตัวตน ที่ต้องบวก 1 เพราะว่าในแต่ละรอบอาจจะไม่เลือกภาพใดเลยก็ได้, K คือจำนวนรอบในการพิสูจน์ตัวตน

ตารางที่ 5.5 เซตคำตอบของรหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนอง

คำถามท้าทาย	ช่วงของรหัสผ่าน
1. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกติดกัน 1 ตำแหน่ง	$({}^{U+D}p_A) / ({}^{U}C_U \, {}^{D}C_{DA})({}^{DA}p_{DA} \, {}^{DA+1}p_{U-1} \, {}^{2}p_2)$
2. เลือกรูปภาพส่วนตัวทั้งหมดโดยเลือกไม่ติดกันเลย	$({}^{U+D}p_A) / ({}^{U}C_U \, {}^{D}C_{DA})({}^{DA}p_{DA} \, {}^{DA+1}p_U)$
3. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกติดกัน 1 ตำแหน่ง	$({}^{U+D}p_A) / ({}^{U}C_H \, {}^{D}C_{DA})({}^{DA}p_{DA} \, {}^{DA+1}p_{H-1} \, {}^{2}p_2)$
4. เลือกรูปภาพส่วนตัวครึ่งหนึ่งโดยเลือกไม่ติดกันเลย	$({}^{U+D}p_A) / ({}^{U}C_H \, {}^{D}C_{DA})({}^{DA}p_{DA} \, {}^{DA+1}p_H)$
5. เลือกรูปภาพส่วนตัวทั้งหมดโดยต้องมีอยู่ทั้ง 2 แถว	$({}^{U+D}p_A) / \sum_{i=1}^{i-1} \{ ({}^{U}C_i \, {}^{D}C_{D1})({}^{U-i}C_{U-i} \, {}^{D-D1}C_{D2}) ({}^{R1}p_{R1} \, {}^{R2}p_{R2}) \}$
6. ไม่เลือกรูปภาพส่วนตัว 1 รูป	$({}^{U+D}p_A) / ({}^{U}C_{U-1} \, {}^{D}C_{DA})({}^{A}p_A)$
7. ไม่เลือกรูปภาพส่วนตัว 2 รูป	$({}^{U+D}p_A) / ({}^{U}C_{U-2} \, {}^{D}C_{DA})({}^{A}p_A)$

ตารางที่ 5.6 ตารางคำศัพท์ของรหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนอง

คำศัพท์	ตัวย่อ	ความหมาย
User image	U	รูปภาพของผู้ใช้
User image in Answer box	UA	รูปภาพของผู้ใช้ในกล่องคำตอบ
Decoy image	D	รูปภาพอื่นๆ
Decoy image in Answer box	DA	รูปภาพอื่นๆในกล่องคำตอบ
Half of User image	H	ครึ่งหนึ่งของรูปภาพของผู้ใช้
Decoy image in Answer box row 1	D1	รูปภาพอื่นๆในแถวแรกของกล่องคำตอบ
Decoy image in Answer box row 2	D2	รูปภาพอื่นๆในแถวที่สองของกล่องคำตอบ
Answer box row 1	R1	แถวแรกของกล่องคำตอบ
Answer box row 2	R2	แถวที่สองของกล่องคำตอบ
Answer box	A	กล่องคำตอบ

รายการอ้างอิง

[1] Shushuang, M., Dawei, H., Manton, M. A Shoulder-Surfing Resistant Graphical Password Scheme - WIW. Proceedings of International conference on security and management (2003): 105-111.

[2] Haber, R. N. How we remember what we see. Scientific American 222(5): (1997): 104-112.

[3] Standing, L., Conezio, J., Haber, R. N. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. Psychonomic Science 19(2): (1970): 73-74.

[4] Intraub, H. Present rate and the representation of briefly glimpsed pictures in memory. Journal of Experimental Psychology: Human Learning and Memory 6(1): (1980): 1-12.

[5] Paivio, A., Csapo, K. Concrete image and verbal memory codes. Journal of Experimental Psychology 80(2): (1969): 279-285.

[6] Xiaoyuan, S., Ying, Z., G. Scott. O. Graphical Passwords: A Survey. 21st Annual Computer Security Applications Conference (2005): 463-472.

[7] Daphna, W., Scott, K. Passwords You'll Never Forget, but Can't Recall. Proceedings of Conference on Human Factors in Computing Systems (CHI) (2004): 1399-1402.

[8] Welcome to Passfaces (online). แหล่งที่มา : http://www.realuser.com [31 มีนาคม พ.ศ. 2551]

[9] Ian, J., Alain, M., Fabian, M., Michael, K. R., Avi, R. The Design and Analysis of Graphical Passwords. Proceedings of the 8th USENIX Security Symposium (1999).

[10] Deholo, N., Julie, Th. Analyzing User Choice in Graphical Passwords. Technical Report, School of Information Technology and Engineering University of Ottawa: (2004).

[11] Challenge-response authentication - Wikipedia, the free encyclopedia (online). แหล่งที่มา : http://en.wikipedia.org/wiki/Challenge-response_authentication [31 มีนาคม พ.ศ.2551]

[12] CAPTCHA - Wikipedia, the free encyclopedia (online). แหล่งที่มา : http://en.wikipedia.org/wiki/CAPTCHA [31 มีนาคม พ.ศ.2551]

[13] ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน (online). แหล่งที่มา : http://www.thaicert.nectec.or.th/paper/authen/authentication_guide.php [31 มีนาคม พ.ศ. 2551]

[14] SSL และ SSH สำหรับการส่งข้อมูลบน Internet ให้ปลอดภัย (online). แหล่งที่มา : http://www.thaicert.nectec.or.th/paper/encryption/sshl.php [31 มีนาคม พ.ศ.2551]

[15] Dawei, H., Shushuang, M., Barbra, H., Manton, M. A Password Scheme Strongly Resistant to Spyware. Proceedings of International conference on security and management (2004): 94-100.

[16] Rachna, D., Adrian, P. Déjà vu: A User Study Using Images for Authentication. Proceedings of 9th USENIX Security Symposium (2000): 4-4.

[17] Passlogix | Welcome (online). แหล่งที่มา : http://www.passlogix.com [31 มีนาคม พ.ศ. 2551]

[18] Tetsuji, T., Hideki, K. Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images. Human-Computer Interaction with Mobile Devices and Services vol.2795 / 2003, Springer-Verlag GmbH: (2003): 347-351.

[19] WinVNC - The Win32 VNC server (online). แหล่งที่มา : http://www.hep.phy.cam.ac.uk/vnc_docs/winvnc.html [31 มีนาคม พ.ศ.2551]

ภาคผนวก

ภาคผนวก ก

วิธีการใช้ซอฟต์แวร์บล็อกเวิร์ล บีต้า

ในภาคผนวกนี้จะแสดงวิธีใช้งานซอฟต์แวร์บล็อกเวิร์ล บีต้าทั้งหมด การอธิบายหน้าตาของซอฟต์แวร์สำหรับผู้ใช้งานทั่วไป ระบบต่างๆที่ใช้ในซอฟต์แวร์นี้รวมไปถึงหน้าจอสำหรับผู้ดูแลระบบ

ก.1 หน้าหลักของซอฟต์แวร์

หน้าแรกของซอฟต์แวร์ทำการแสดงชื่อบทความใหม่ล่าสุด 11 บทความที่มีอยู่ในฐานข้อมูล โดยจะแบ่งออกเป็น 2 หน้าจอ หน้าจอทางด้านซ้ายแสดงบทความใหม่ล่าสุดพร้อมด้วยเนื้อหาบางส่วน หน้าจอทางขวามือแสดงชื่อบทความ 10 บทความถัดมาดังรูปที่ ก.1

รูปที่ ก.1 หน้าหลักของซอฟต์แวร์บล็อกเวิร์ล บีต้า

ก.2 การลงทะเบียน

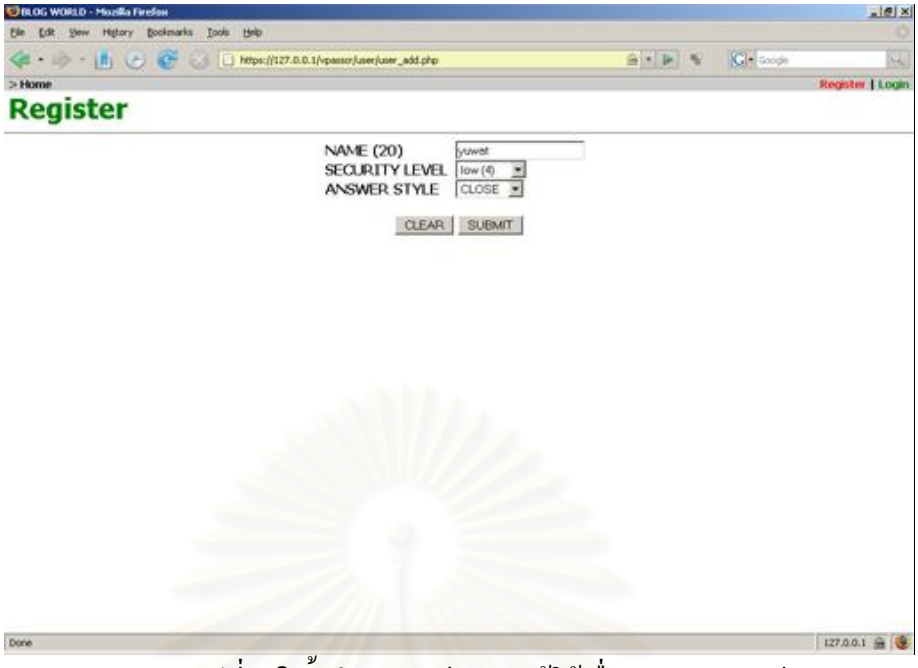
เมื่อเริ่มต้นใช้งาน ผู้ใช้ต้องทำการลงทะเบียนเพื่อสร้างบัญชีผู้ใช้ของตนเองขึ้นมา สำหรับใช้ในการจัดการสมุดบันทึกและแสดงความคิดเห็น โดยมีขั้นตอนดังนี้

1. เลือก Register ที่เมนูด้านบนขวา

รูปที่ ก.2 เมนู Register ในหน้าหลักของซอฟต์แวร์

2. ตั้งค่ารายละเอียดของผู้ใช้งาน มีรายละเอียดดังนี้

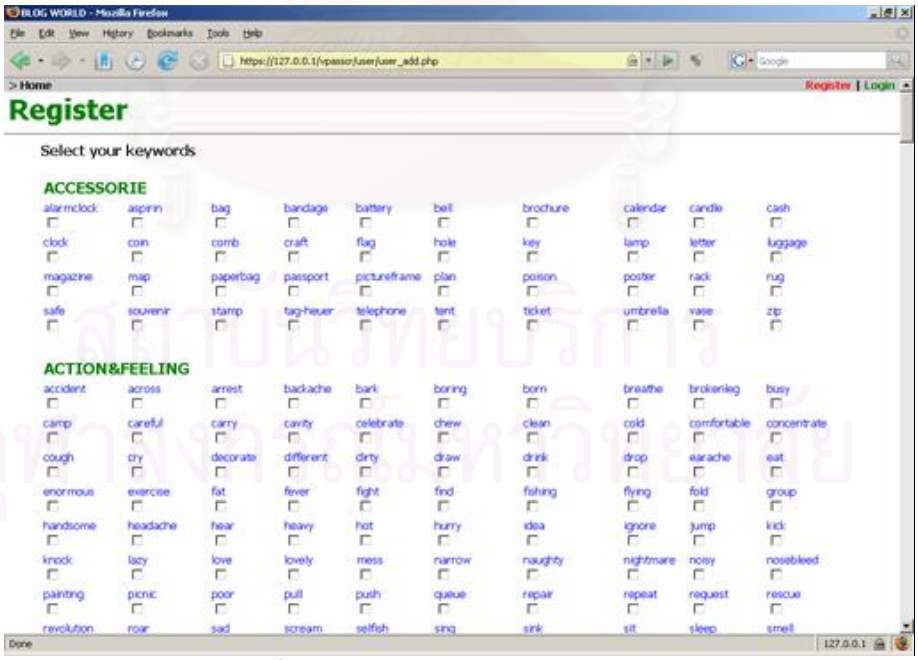
- NAME ชื่อผู้ใช้
- SECURITY LEVEL จำนวนคำสำคัญของผู้ใช้ ระดับแปรผันตามความปลอดภัย
- ANSWER STYLE พฤติกรรมของรูปภาพตอนเข้าสู่ระบบมีด้วยกัน 3 แบบคือ
    - CLOSE แสดงผลรูปภาพที่เลือกแล้วเป็นหน้าจอสีดำมีคำว่า selected
    - HOVER แสดงผลรูปภาพแบบ CLOSE แต่สามารถแสดงรูปภาพออกมาได้เมื่อนำเมาส์ไปวางไว้บนรูปภาพ
    - OPEN ไม่มีการปิดบังรูปภาพที่เลือกไว้



รูปที่ ก.3 ตั้งค่ารายละเอียดของผู้ใช้เมื่อทำการลงทะเบียน

3. เลือกคำสำคัญ โดยมีเมนูควบคุมการทำงานดังนี้

- CLEAR ล้างคำสำคัญที่เลือกทั้งหมด
- SUBMIT ยืนยันการเลือกคำสำคัญ

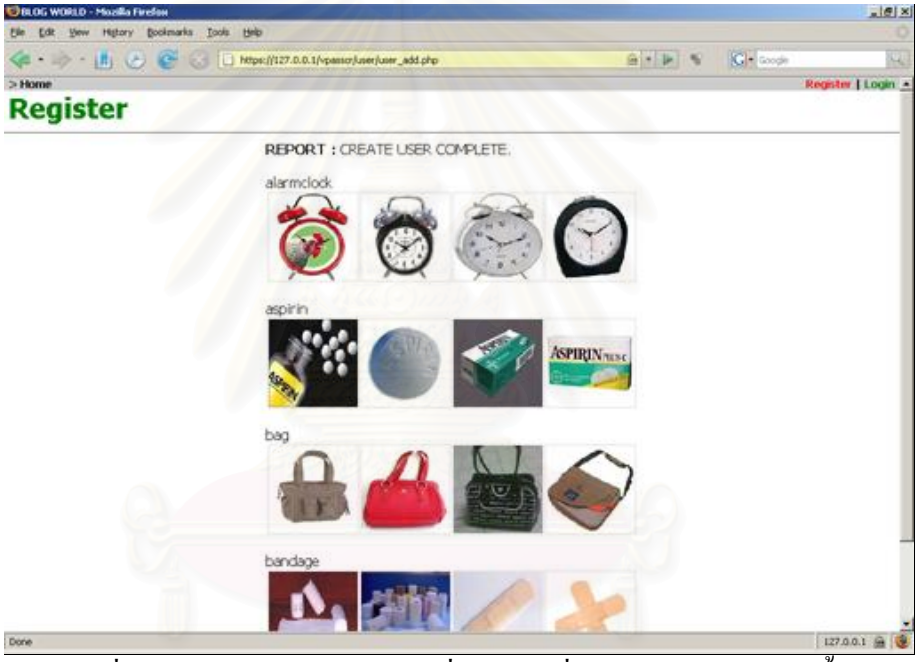


รูปที่ ก.4 หน้าจอเลือกคำสำคัญในการลงทะเบียน

ถ้าหากการเลือกคำสำคัญไม่สมบูรณ์จะแสดงหน้าจอดังนี้

รูปที่ ก.5 แสดงคำเตือนเมื่อเลือกคำสำคัญไม่สมบูรณ์ในการลงทะเบียน

4. เมื่อการลงทะเบียนสำเร็จ ระบบจะแสดงคำสำคัญที่เลือกพร้อมทั้งภาพประกอบ



รูปที่ ก.6 แสดงคำสำคัญและภาพที่ถูกเลือกเมื่อการลงทะเบียนเสร็จสิ้น

ก.3 การเข้าสู่ระบบ

เป็นหัวใจของซอฟต์แวร์ตัวนี้ เนื่องจากใช้รหัสผ่านแบบรูปภาพโดยใช้คำถามท้าทาย-ตอบสนองในการเข้าสู่ระบบ การเข้าสู่ระบบมีขั้นตอนดังนี้

1. ใส่ชื่อผู้ใช้เข้าสู่ระบบ

รูปที่ ก.7 หน้าจอใส่ชื่อผู้ใช้ในการเข้าสู่ระบบ

2. ทำการเลือกรูปภาพตามคำถามที่สุ่มขึ้นมาให้ถูกต้องเพื่อเข้าสู่ระบบ

รูปที่ ก.8 หน้าจอเลือกรูปภาพตามคำถามสุ่มในการเข้าสู่ระบบ

สำหรับคำถามนั้นมีด้วยกัน 7 แบบดังนี้

- เลือกรูปภาพส่วนตัวทั้งหมดแบบติดกัน
- เลือกรูปภาพส่วนตัวทั้งหมดแบบไม่ติดกัน

- เลือกรูปภาพส่วนตัวครึ่งหนึ่งแบบติดกัน
- เลือกรูปภาพส่วนตัวครึ่งหนึ่งแบบไม่ติดกัน
- เลือกรูปภาพส่วนตัวทั้งหมดโดยต้องมีอยู่ทั้ง 2 แถว
- ไม่เลือกรูปภาพส่วนตัว 1 รูป
- ไม่เลือกรูปภาพส่วนตัว 2 รูป

เพื่อความปลอดภัยของการเข้าสู่ระบบ ซอฟต์แวร์ได้มีระบบป้องกันตัวเองใน 2 กรณีคือ

- หากเข้าสู่ระบบผิดติดต่อกัน 3 ครั้ง บัญชีผู้ใช้จะถูกระงับชั่วคราว
- หากใส่ชื่อผู้ใช้เข้ามาสู่ระบบจำนวน 5 ครั้งติดกันโดยไม่พิสูจน์ตัวตน บัญชีผู้ใช้จะถูกระงับชั่วคราว

รูปที่ ก.9 หน้าจอแสดงการระงับผู้ใช้งาน

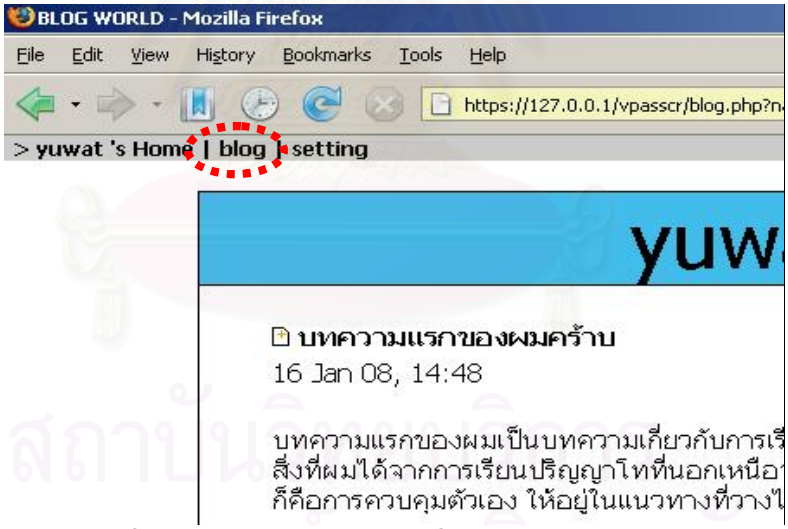
ซึ่งถ้าหากบัญชีผู้ใช้ถูกระงับชั่วคราวแล้ว จำเป็นต้องให้ผู้ดูแลระบบเป็นคนแก้ไขสถานะของบัญชีผู้ใช้ให้กลับมาใช้งานได้ดังเดิม

ก.4 ระบบสมุดบันทึก

ผู้ใช้แต่ละคนจะได้รับพื้นที่สำหรับเขียนบทความหรือเรื่องราวของตัวเอง โดยหน้าจอจะแบ่งออกเป็น 2 ส่วน ทางซ้ายมือจะเป็นบทความของผู้ใช้พร้อมทั้งช่องสำหรับแสดงความคิดเห็น ทางขวามือจะแสดงรายชื่อหัวข้อบทความที่ผู้ใช้เขียนทั้งหมดโดยเรียงจากใหม่สุดไปหาเก่าสุด

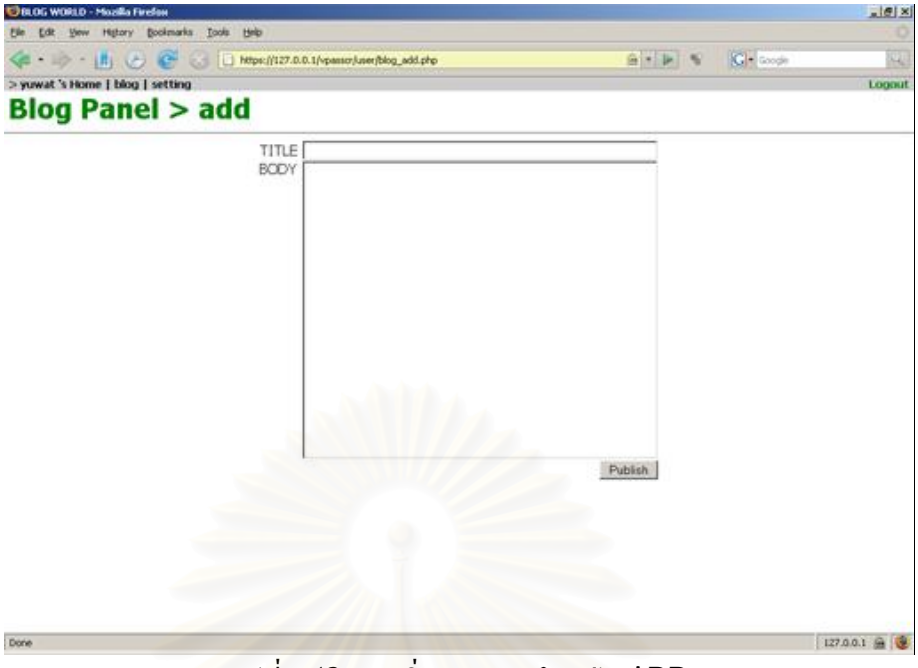
รูปที่ ก.10 หน้าจอหลักของระบบสมุดบันทึก

การแก้ไขบทความ สามารถทำได้โดยเลือกที่เมนู blog ดังรูปที่ ก.11



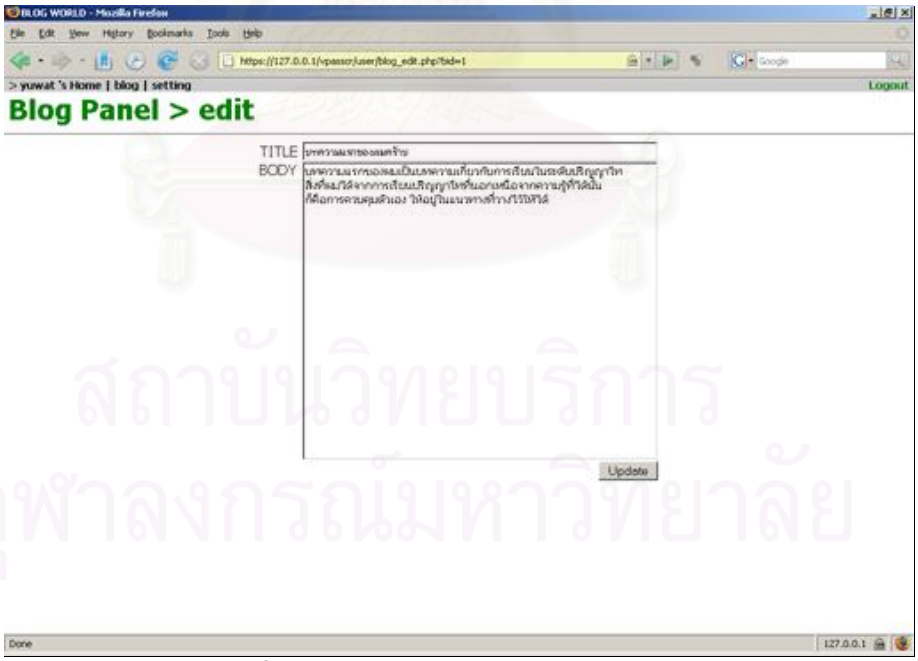
รูปที่ ก.11 การเลือกเมนู blog เพื่อทำการแก้ไขบทความ

การเพิ่มบทความ ทำได้โดยกดปุ่ม ADD การเพิ่มบทความประกอบไปด้วย ชื่อบทความ และ เนื้อหา โดยเนื้อหาสามารถรองรับภาษา HTML ได้



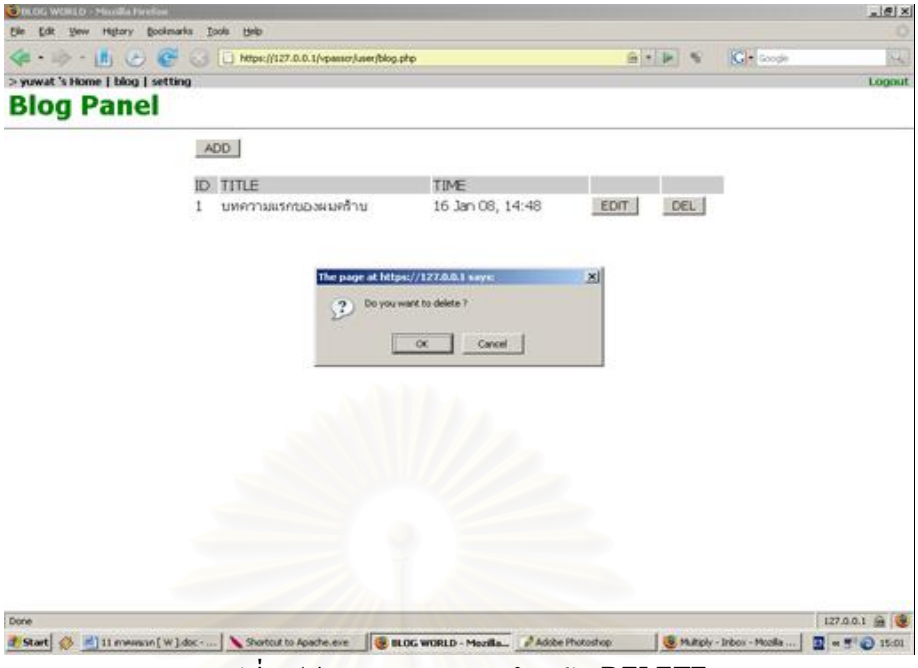
รูปที่ ก.12 การเพิ่มบทความโดยปุ่ม ADD

การแก้ไขบทความ ทำได้โดยกดปุ่ม EDIT โดยลักษณะหน้าจอการแก้ไขจะมีลักษณะเช่นเดียวกับการเพิ่มบทความ



รูปที่ ก.13 การแก้ไขบทความโดยปุ่ม EDIT

การลบบทความ ทำได้โดยกดปุ่ม DEL เมื่อกดแล้วจะมี หน้าจอถามเพื่อความแน่ใจว่าต้องการลบบทความจริงๆหรือไม่ ถ้าหากต้องการลบให้กด OK ถ้าไม่ต้องการลบให้กด Cancel



รูปที่ ก.14 การลบบทความโดยปุ่ม DELETE

การแสดงความคิดเห็น ผู้ใช้สามารถเพิ่ม/แก้ไข/ลบ ความคิดเห็นของตนเองลงในบทความใดๆก็ได้ ส่วนผู้ดูแลระบบสามารถลบความคิดเห็นของใครก็ได้เพียงอย่างเดียว ไม่สามารถแก้ไขความคิดเห็นของคนอื่นได้

รูปที่ ก.15 ผู้ดูแลระบบไม่สามารถแก้ไขความคิดเห็นของคนอื่นได้

ก.5 การปรับแต่งการพิสูจน์ตัวตนของผู้ใช้

การปรับแต่งการพิสูจน์ตัวตนของผู้ใช้ สามารถทำได้โดยการเลือกที่เมนู setting โดยลักษณะการปรับแต่งจะมีขึ้นตอนเหมือนกันกับการลงทะเบียน เพียงแต่ไม่ต้องกรอกชื่อผู้ใช้

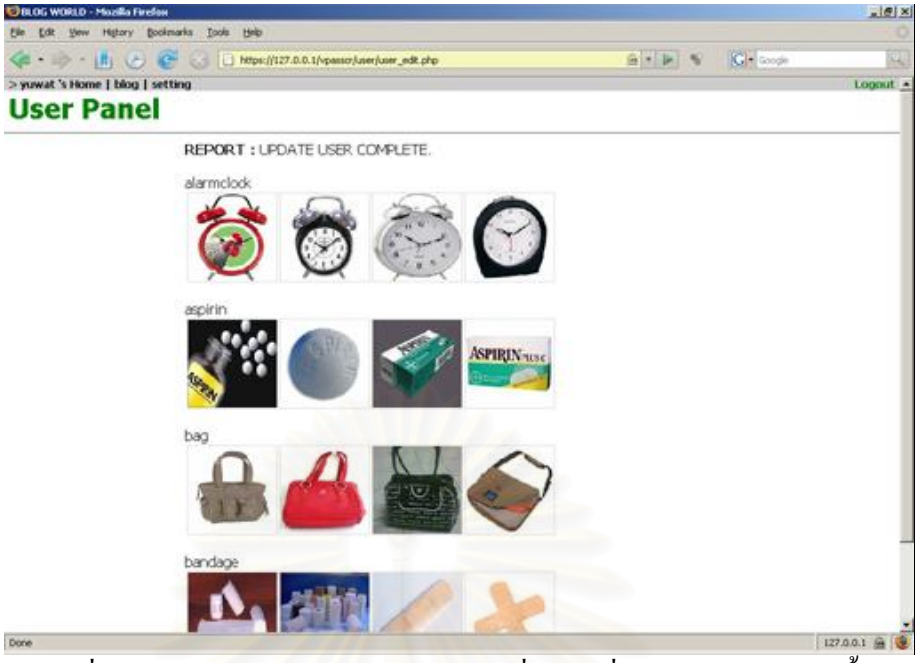
รูปที่ ก.16 หน้าจอการปรับแต่งการพิสูจน์ตัวตนของผู้ใช้

ในหน้าจอการเลือกคำสำคัญจะมีปุ่มที่ใช้ควบคุมการทำงานต่างๆดังนี้

- RESET ล้างการเลือกคำสำคัญที่มีอยู่ทั้งหมด
- DEFAULT เลือกใช้คำสำคัญชุดเดิมกับที่เข้าสู่ระบบเข้ามา
- SUBMIT ยืนยันการเลือกคำสำคัญ

รูปที่ ก.17 ปุ่มที่ใช้ควบคุมการทำงานการปรับแต่งการพิสูจน์ตัวตน

หลังจากที่ยืนยันการเลือกคำสำคัญแล้ว ระบบก็จะแสดงแสดงคำสำคัญที่เลือกพร้อมทั้งภาพประกอบคำสำคัญนั้นออกมา

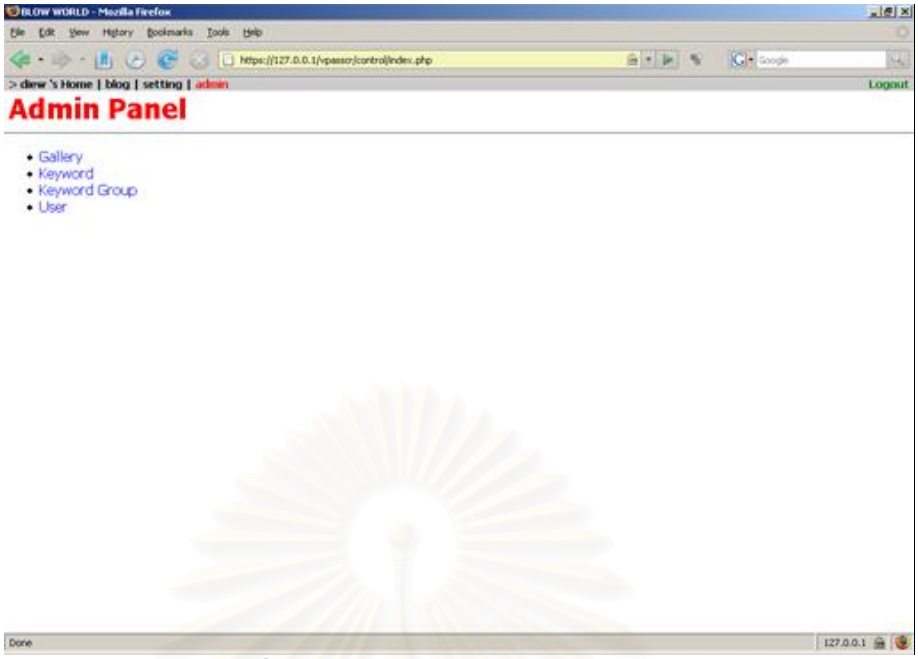


รูปที่ ก.18 หน้าจอแสดงคำสำคัญและภาพที่เลือก เมื่อผู้ใช้ปรับแต่งเสร็จสิ้น

ก.6 เมนูของผู้ดูแลระบบ

ผู้ดูแลระบบสามารถเข้าสู่เมนูของผู้ดูแลระบบได้โดยการเลือกเมนู admin ตัวสีแดง

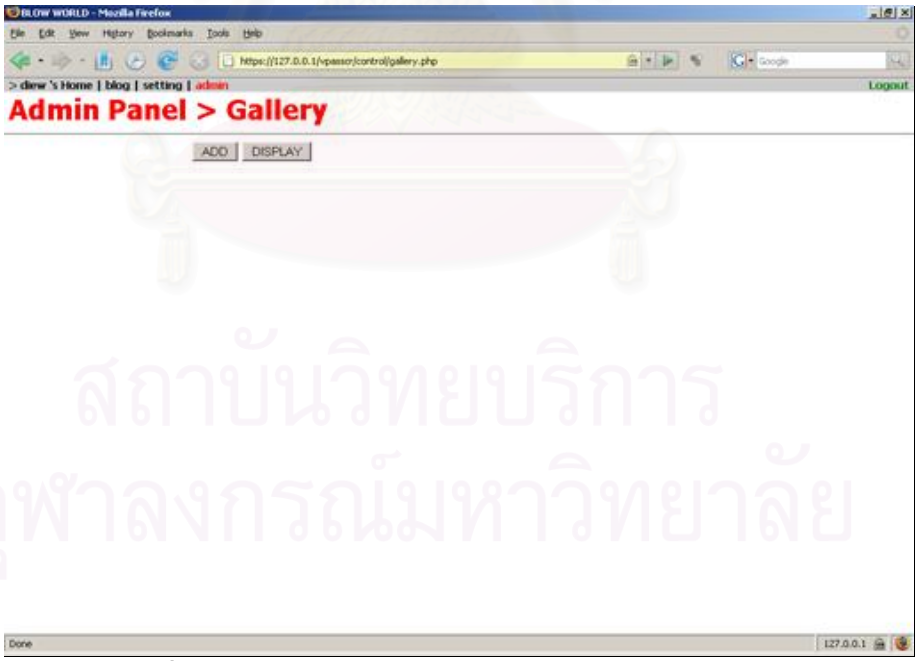
รูปที่ ก.19 หน้าจอแสดงการเข้าถึงเมนู admin



รูปที่ ก.20 หน้าจอหลักของเมนูผู้ดูแลระบบ

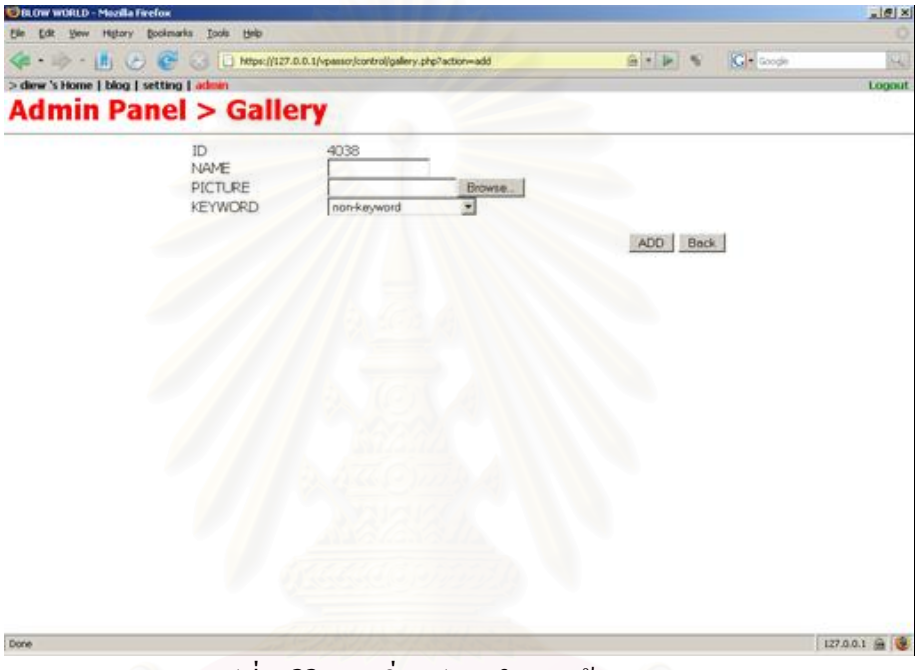
เมนูของผู้ดูแลระบบประกอบไปด้วย

Gallery เมนูสำหรับจัดการรูปภาพทั้งหมดในระบบ คำสั่งทั้งหมดมีดังนี้



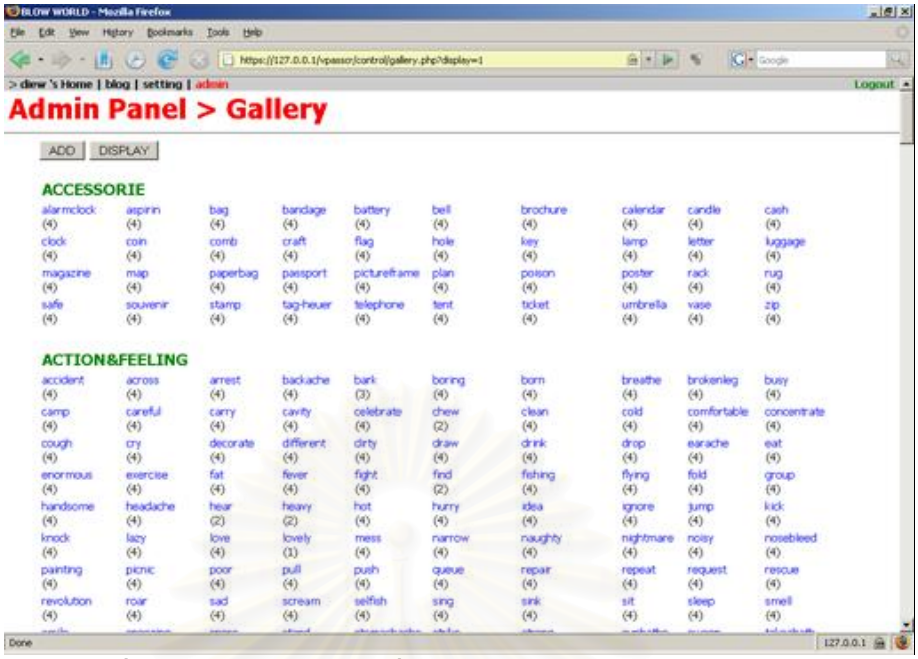
รูปที่ ก.21 หน้าจอหลักการจัดการรูปภาพในเมนูผู้ดูแลระบบ

- ADD ใช้ในการเพิ่มรูปภาพเข้ามาในระบบ เรียกใช้โดยการกดปุ่ม ADD เมื่อกดปุ่ม ADD แล้วกรอกรายละเอียดของรูปภาพที่จะทำการใส่เพิ่มเข้าไปโดยมีรายละเอียดดังนี้
  - NAME ชื่อของรูปภาพ
  - PICTURE ไฟล์รูปภาพที่ต้องการเพิ่ม
  - KEYWORD คำสำคัญของรูปภาพนั้นๆ



รูปที่ ก.22 การเพิ่มรูปภาพในเมนูผู้ดูแลระบบ

เมื่อกดปุ่ม DISPLAY ที่หน้าจอ Gallery ระบบจะแสดงคำสำคัญทั้งหมดออกมาโดยแบ่งออกเป็นกลุ่ม เมื่อเลือกคำสำคัญใดๆ ระบบจะแสดงรูปภาพของคำสำคัญนั้นออกมา ที่ใต้รูปภาพจะมีตัวอักษร E และ X ซึ่งใช้ในการจัดการรูปภาพดังนี้



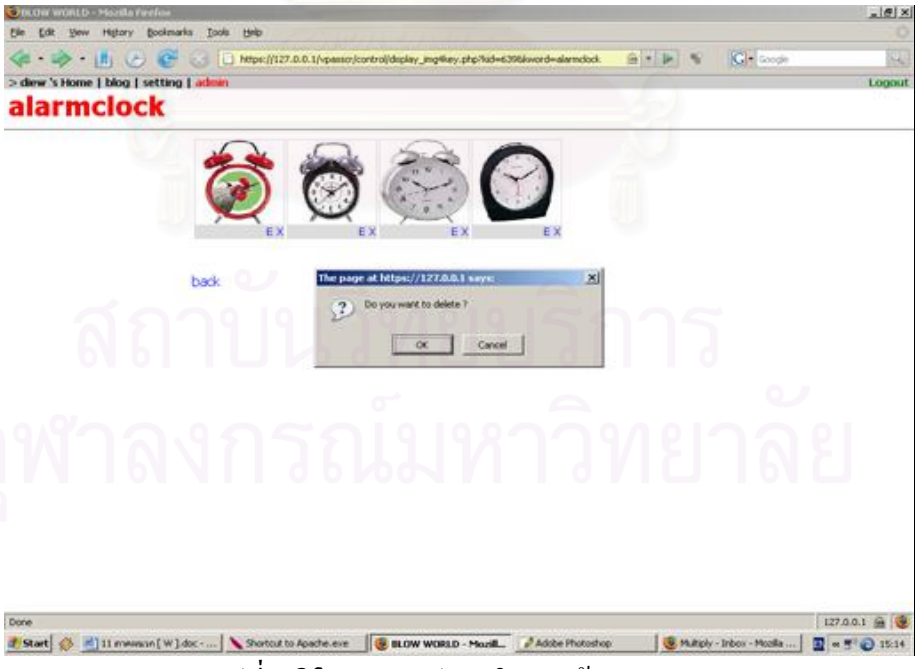
รูปที่ ก.23 หน้าจอ Gallery เมื่อกดปุ่ม DISPLAY ในเมนูผู้ดูแลระบบ

รูปที่ ก.24 หน้าจอการจัดการรูปภาพของคำสำคัญ

- E ใช้ในการแก้ไขรูปภาพในระบบ โดยจะมีรายละเอียดเหมือนกับการเพิ่มรูปภาพในระบบ

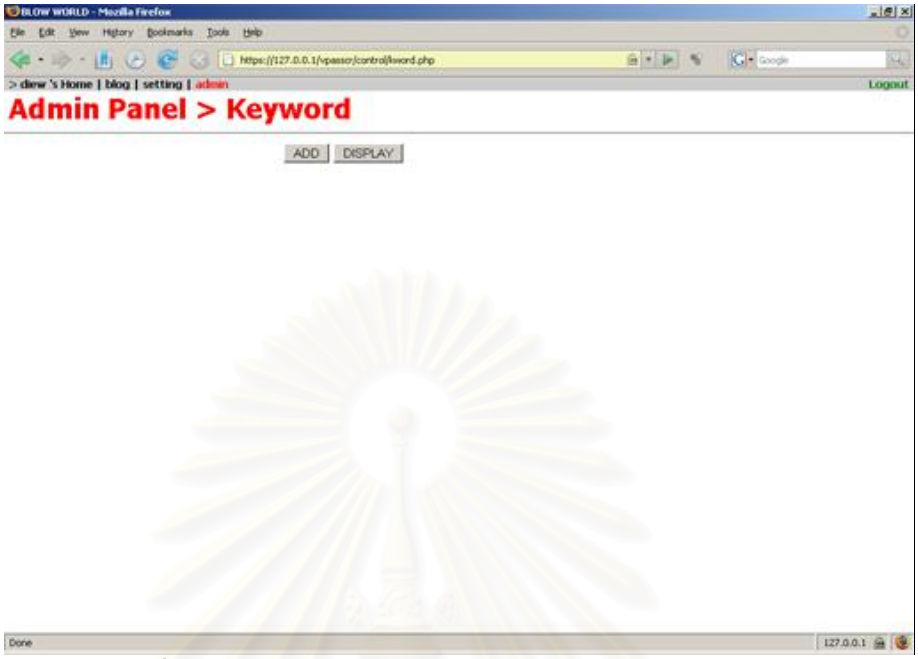
รูปที่ ก.25 การแก้ไขรูปภาพในเมนูผู้ดูแลระบบ

- X ใช้ในการลบรูปภาพในระบบ เมื่อกดจะมีหน้าจอขึ้นมายืนยันกระบวนการ ถ้าหากต้องการลบรูปภาพจริงๆให้เลือก OK หรือถ้าไม่ต้องการลบให้เลือก Cancel



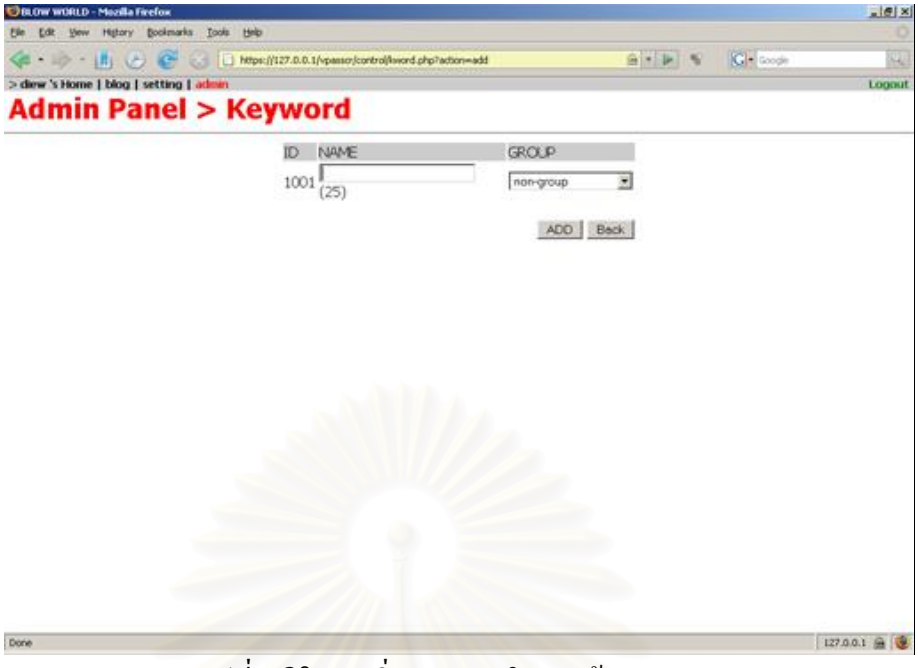
รูปที่ ก.26 การลบรูปภาพในเมนูผู้ดูแลระบบ

Keyword เมนูสำหรับจัดการคำสำคัญในระบบ มีคำสั่งทั้งหมดดังนี้



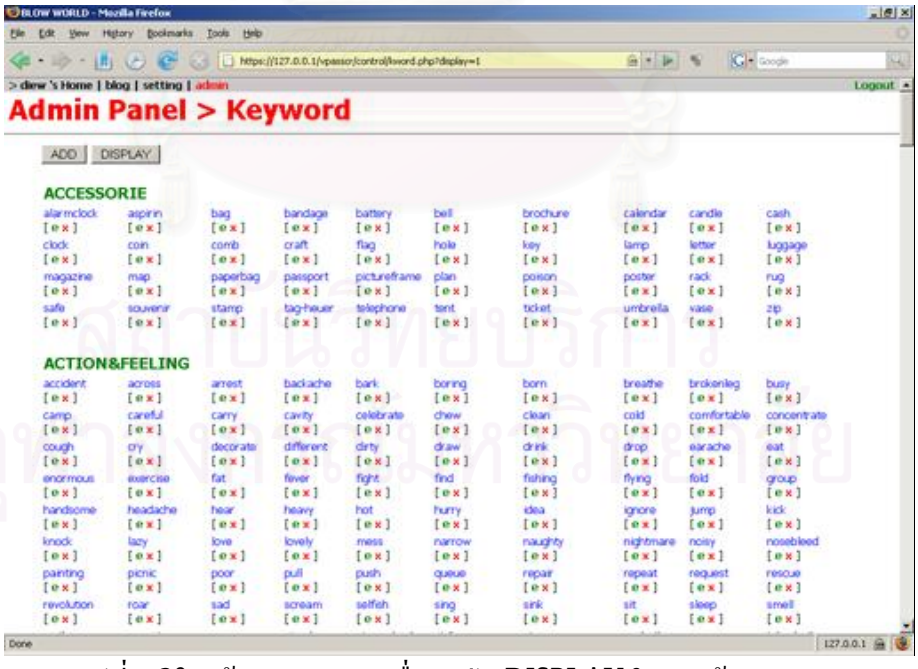
รูปที่ ก.27 หน้าจอหลักการจัดการคำสำคัญในเมนูผู้ดูแลระบบ

- ADD ใช้ในการเพิ่มคำสำคัญเข้ามาในระบบ เรียกใช้โดยการกดปุ่ม ADD เมื่อกดปุ่ม ADD แล้วจะต้องกรอกรายละเอียดของคำสำคัญที่จะทำการใส่เพิ่มเข้าไปโดยมีรายละเอียดดังนี้
  - NAME ชื่อคำสำคัญ
  - GROUP กลุ่มของคำสำคัญ



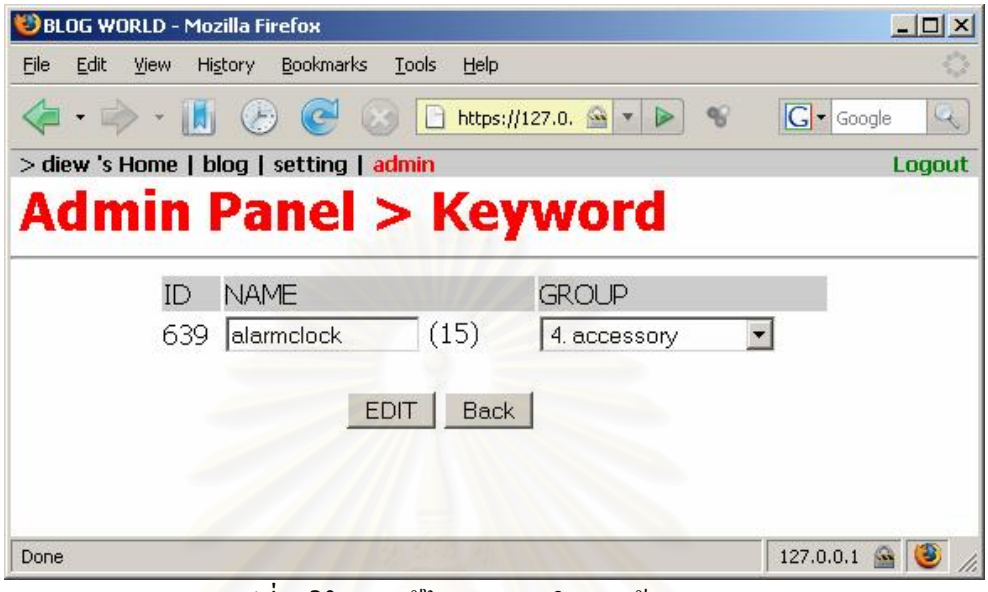
รูปที่ ก.28 การเพิ่มคำสำคัญในเมนูผู้ดูแลระบบ

เมื่อกดปุ่ม DISPLAY ที่หน้าจอ Keyword ระบบจะแสดงคำสำคัญทั้งหมดออกมา โดยแบ่งออกเป็นกลุ่ม ที่ใต้คำสำคัญจะมีตัวอักษร E และ X ซึ่งใช้ในการจัดการคำสำคัญดังนี้



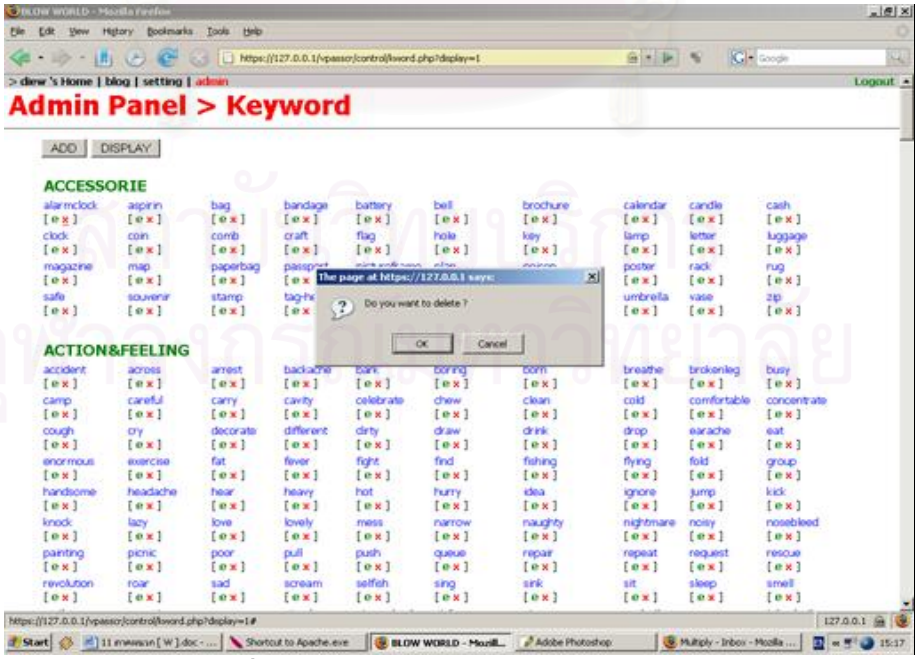
รูปที่ ก.29 หน้าจอคำสำคัญ เมื่อกดปุ่ม DISPLAY ในเมนูผู้ดูแลระบบ

- E ใช้ในการแก้ไขคำสำคัญในระบบ โดยจะมีรายละเอียดเหมือนกับการเพิ่มคำสำคัญในระบบ



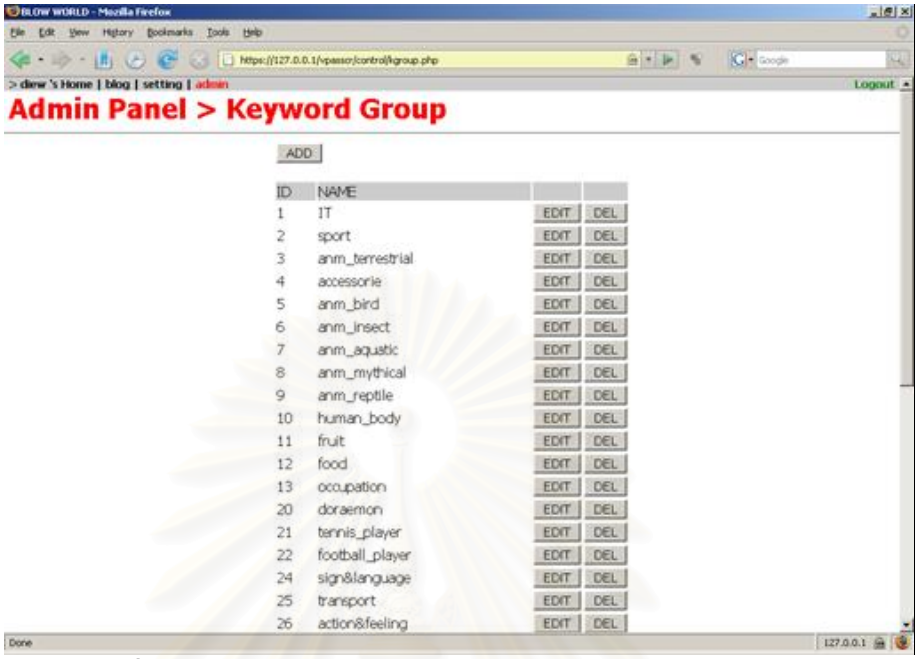
รูปที่ ก.30 การแก้ไขคำสำคัญในเมนูผู้ดูแลระบบ

- X ใช้ในการลบคำสำคัญในระบบ เมื่อกดจะมีหน้าจอขึ้นมายืนยันกระบวนการ ถ้าหากต้องการลบคำสำคัญจริงๆให้เลือก OK หรือถ้าไม่ต้องการลบให้เลือก Cancel



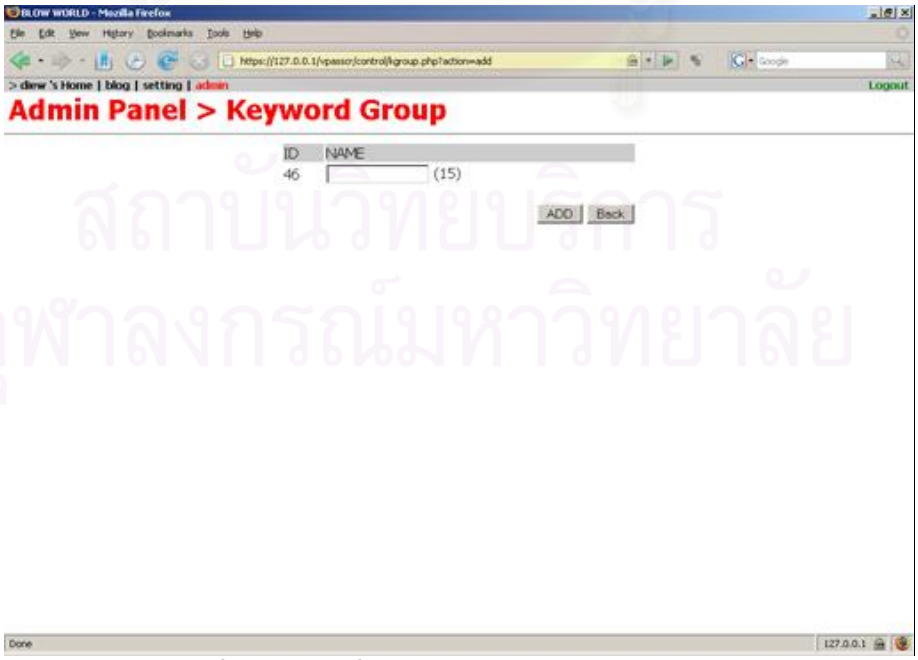
รูปที่ ก.31 การลบคำสำคัญในเมนูผู้ดูแลระบบ

Keyword Group เมนูสำหรับจัดการกลุ่มของคำสำคัญ มีคำสั่งทั้งหมดดังนี้



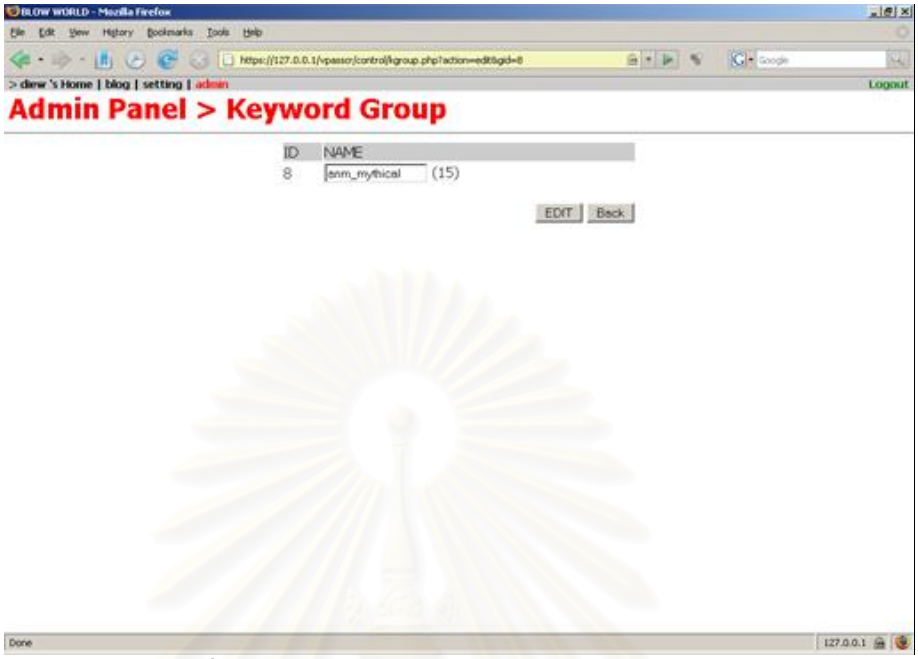
รูปที่ ก.32 หน้าจอหลักการจัดการกลุ่มคำสำคัญในเมนูผู้ดูแลระบบ

- ADD ใช้สำหรับเพิ่มกลุ่มคำสำคัญ โดยจะต้องกรอกรายละเอียดของกลุ่มคำสำคัญดังนี้
  - NAME ชื่อของกลุ่มคำสำคัญ



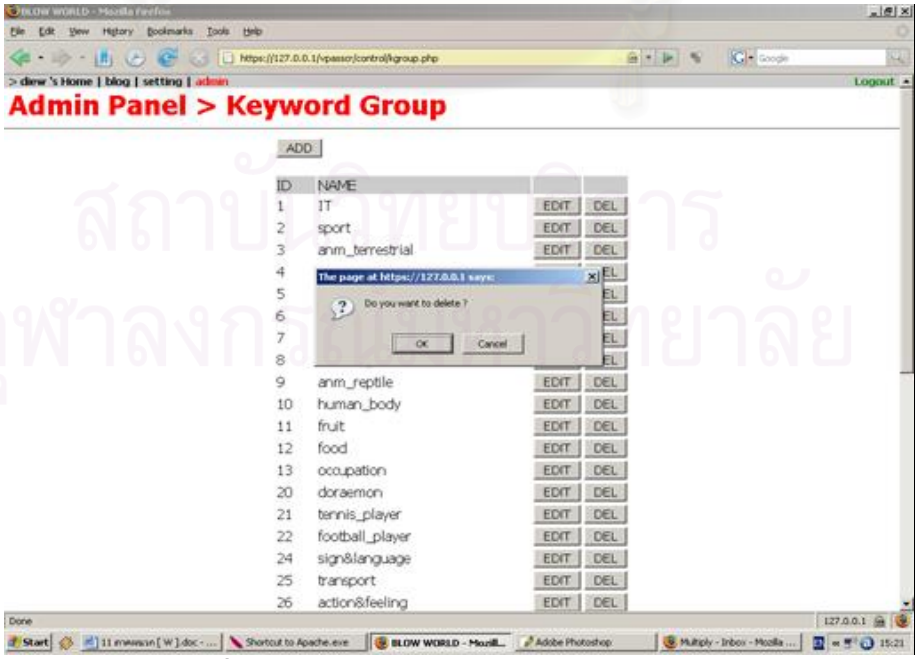
รูปที่ ก.33 การเพิ่มกลุ่มคำสำคัญในเมนูผู้ดูแลระบบ

- EDIT ใช้สำหรับแก้ไขชื่อของกลุ่มคำสำคัญ



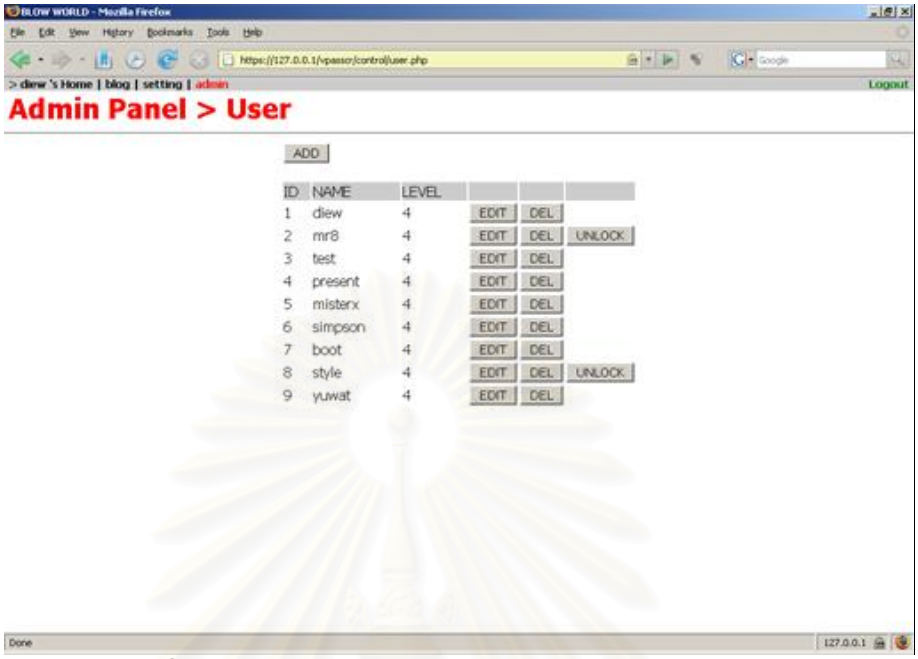
รูปที่ ก.34 การแก้ไขกลุ่มคำสำคัญในเมนูผู้ดูแลระบบ

- DELETE ใช้สำหรับลบชื่อกลุ่มคำสำคัญ เมื่อเลือกแล้วจะมีหน้าจอยืนยันว่าต้องการลบกลุ่มคำสำคัญนั้นจริงๆหรือไม่ ถ้าต้องการลบให้กด OK ถ้าไม่ต้องการลบให้กด Cancel



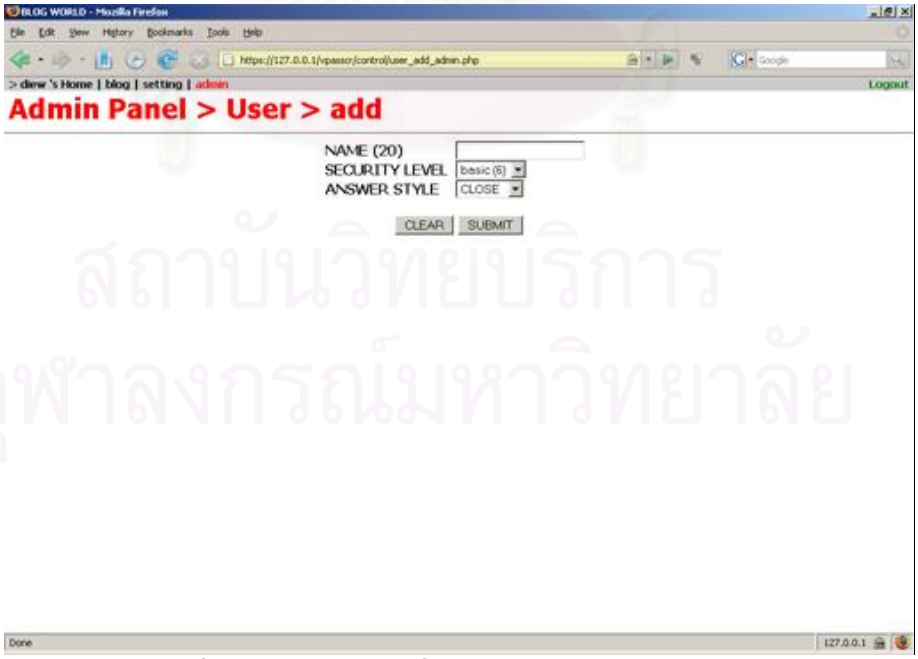
รูปที่ ก.35 การลบกลุ่มคำสำคัญในเมนูผู้ดูแลระบบ

User เมนูสำหรับจัดการสมาชิก มีคำสั่งทั้งหมดดังนี้



รูปที่ ก.36 หน้าจอหลักการจัดการสมาชิกในเมนูผู้ดูแลระบบ

- ADD ใช้สำหรับเพิ่มบัญชีผู้ใช้เข้ามาในระบบ มีลักษณะเหมือนการลงทะเบียนผู้ใช้ในหัวข้อ ก.2

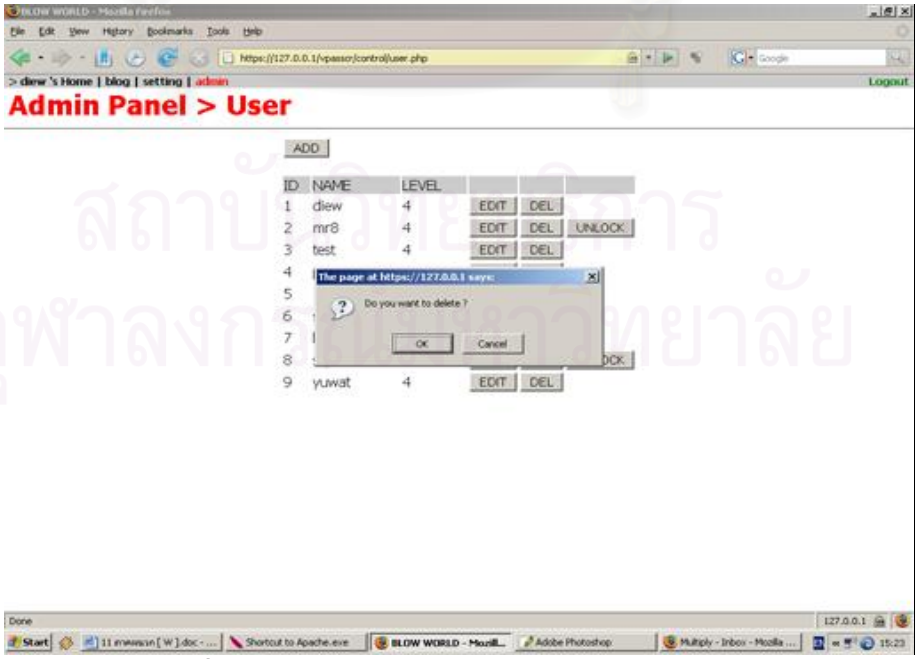


รูปที่ ก.37 หน้าจอการเพิ่มบัญชีผู้ใช้ในเมนูผู้ดูแลระบบ

- EDIT ใช้สำหรับการแก้ไขค่าการพิสูจน์ตัวตนของผู้ใช้ มีลักษณะเหมือนการปรับแต่งการพิสูจน์ตัวตนของผู้ใช้ในหัวข้อ ก.5

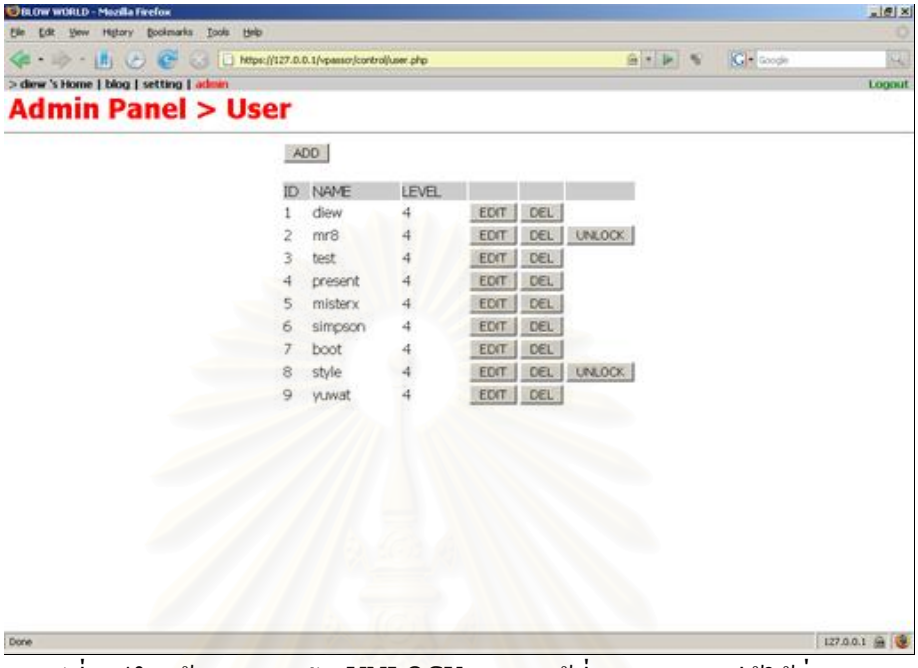
รูปที่ ก.38 หน้าจอการแก้ไขรายละเอียดของบัญชีผู้ใช้ในเมนูผู้ดูแลระบบ

- DELETE ให้ลบบัญชีผู้ใช้ออกจากระบบ โดยจะมีจอยืนยันว่าต้องการลบบัญชีผู้ใช้คนออกจากระบบจริงหรือไม่ ถ้าต้องการลบจริงให้กด OK



รูปที่ ก.39 หน้าจอการลบบัญชีผู้ใช้ในเมนูผู้ดูแลระบบ

- UNLOCK ใช้สำหรับผู้ที่ถูกระงับบัญชีผู้ใช้ชั่วคราวในหัวข้อที่ ก.3 เมื่อกดปุ่มแล้วสถานะของผู้ใช้จะกลับสู่สภาวะปกติและปุ่ม UNLOCK จะหายไป



รูปที่ ก.40 หน้าจอแสดงปุ่ม UNLOCK สำหรับผู้ที่ถูกระงับบัญชีผู้ใช้ชั่วคราว

ภาคผนวก ข

วิธีติดตั้งซอฟต์แวร์บล็อกเวิร์ล บีต้า

ซอฟต์แวร์บล็อกเวิร์ล บีต้าทำงานบนอินเตอร์เน็ทในรูปแบบของเว็บ การติดตั้งซอฟต์แวร์อย่างถูกต้องมีความจำเป็นเพื่อให้ซอฟต์แวร์ทำงานได้อย่างเต็มประสิทธิภาพ

ข.1 ซอฟต์แวร์ที่จำเป็น

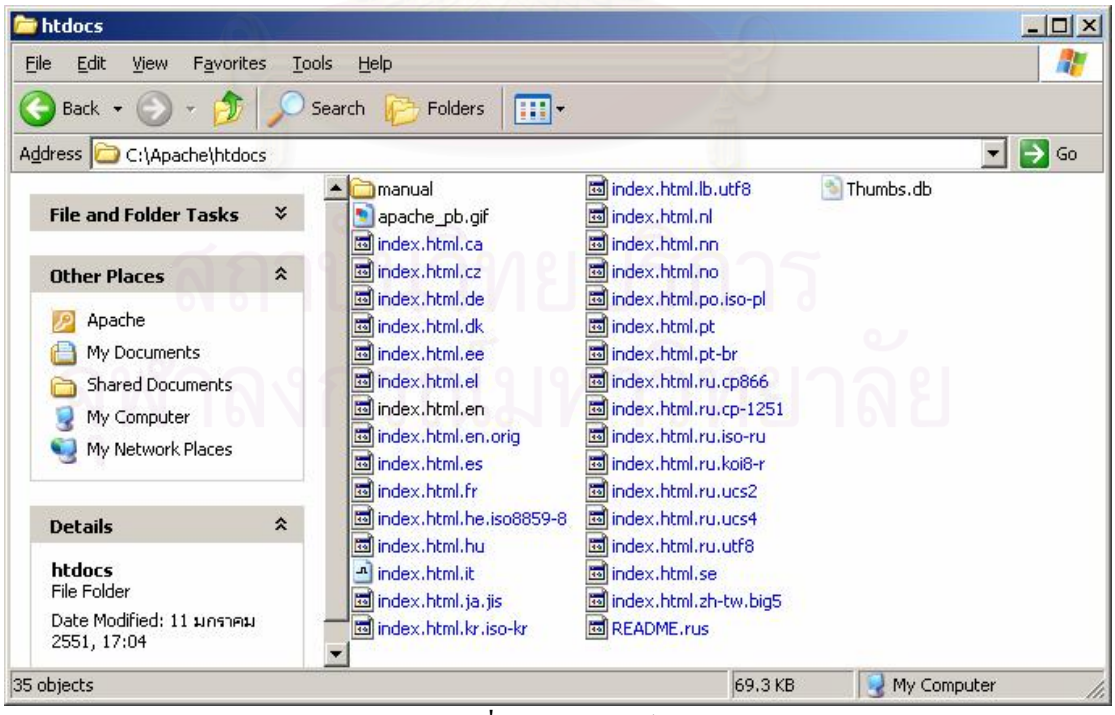
เนื่องจากซอฟต์แวร์บล็อกเวิร์ล บีต้าอยู่ในรูปแบบของเว็บ ก่อนทำการติดตั้งจึงต้องมีซอฟต์แวร์ที่จำเป็นเตรียมไว้ก่อนดังนี้

1. เว็บเซิร์ฟเวอร์ที่รองรับภาษาพีเอชพี (PHP) รุ่น 4.3.8 หรือสูงกว่าที่ติดตั้งเอสเอสแอล (SSL) แล้ว
2. ฐานข้อมูลมายเอสคิวแอล (MySQL) รุ่น 4.0.20a-nt หรือสูงกว่า

ข.2 การติดตั้งซอฟต์แวร์

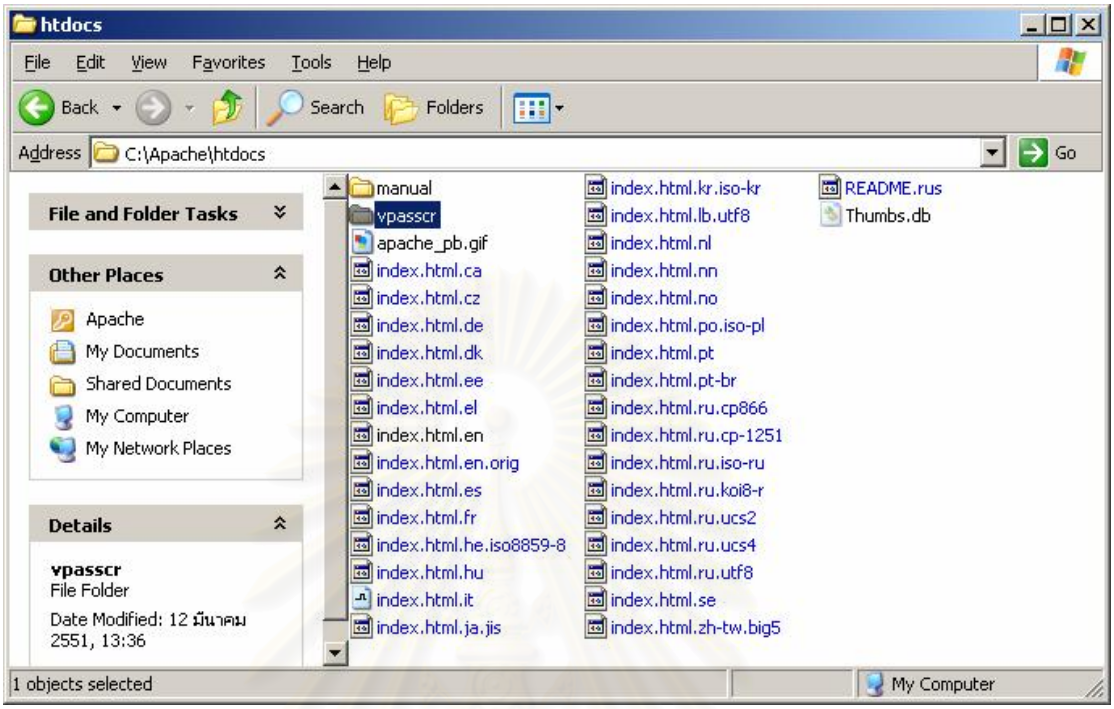
การติดตั้งซอฟต์แวร์แบ่งออกเป็น 3 ขั้นตอนดังนี้

1. การติดตั้งไฟล์เว็บ
   a. เปิดโฟลเดอร์ wwwroot



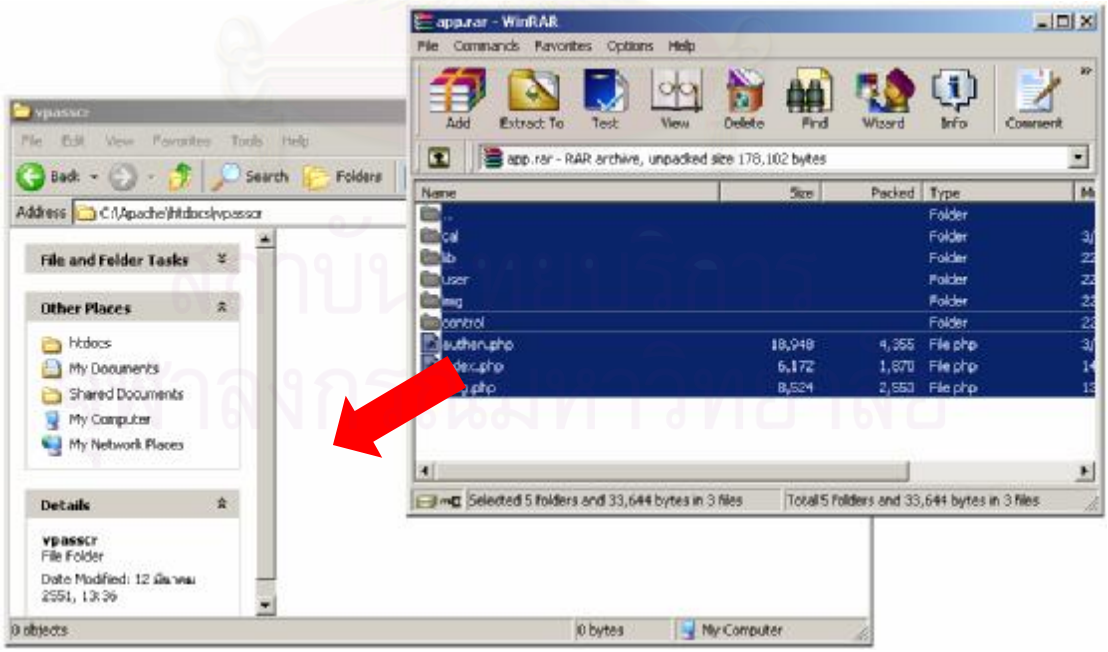
รูปที่ ข.1 โฟลเดอร์ wwwroot

b. สร้างโฟลเดอร์ vpasscr



รูปที่ ข.2 สร้างโฟลเดอร์ vpasscr

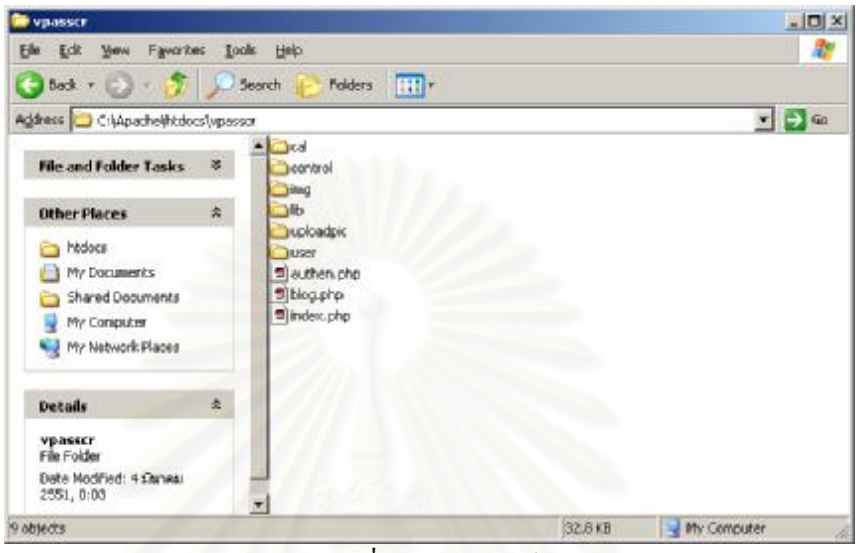
c. ลากไฟล์จาก app.rar ลงในโฟลเดอร์ wwwroot



รูปที่ ข.3 คัดลอกไฟล์จาก app.rar ลงในโฟลเดอร์ vpasscr

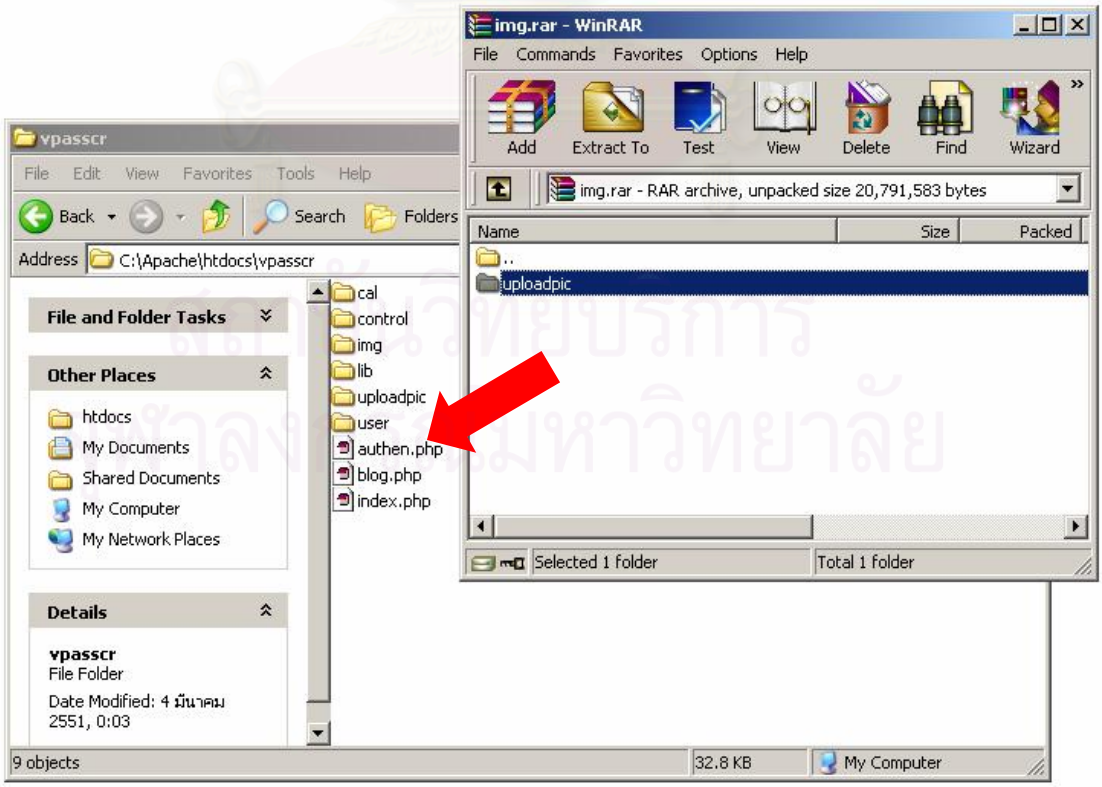
2. การติดตั้งไฟล์รูปภาพ

a. เปิดโฟลเดอร์ wwwroot\vpasscr



รูปที่ ข.4 โฟลเดอร์ vpasscr

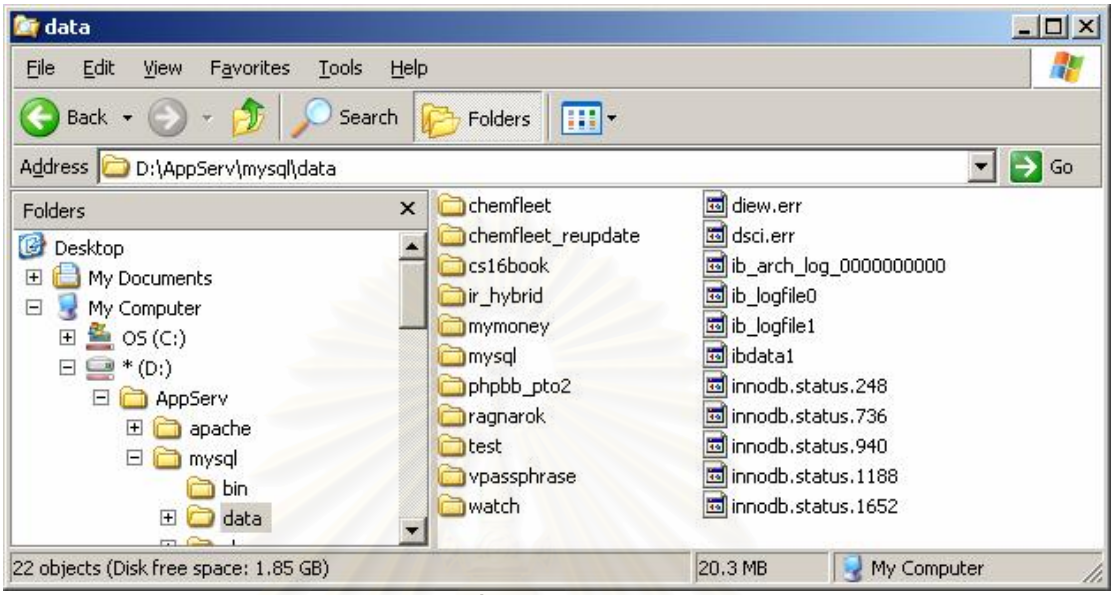
b. ลากไฟล์จาก img.rar ลงในโฟลเดอร์ wwwroot\vpasscr



รูปที่ ข.5 คัดลอกโฟลเดอร์จาก img.rar ลงในโฟลเดอร์ vpasscr

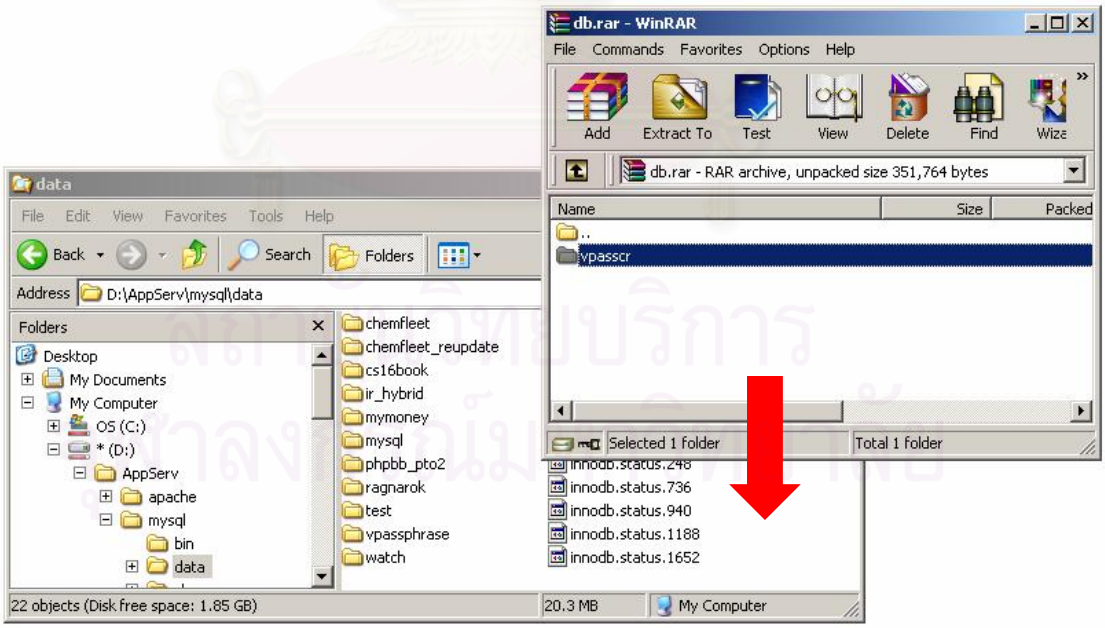
3. การติดตั้งฐานข้อมูล

   a. เปิดโฟลเดอร์ mysql\data



รูปที่ ข.6 โฟลเดอร์ mysql\data

   b. ลากไฟล์จาก db.rar ลงในโฟลเดอร์ mysql\data

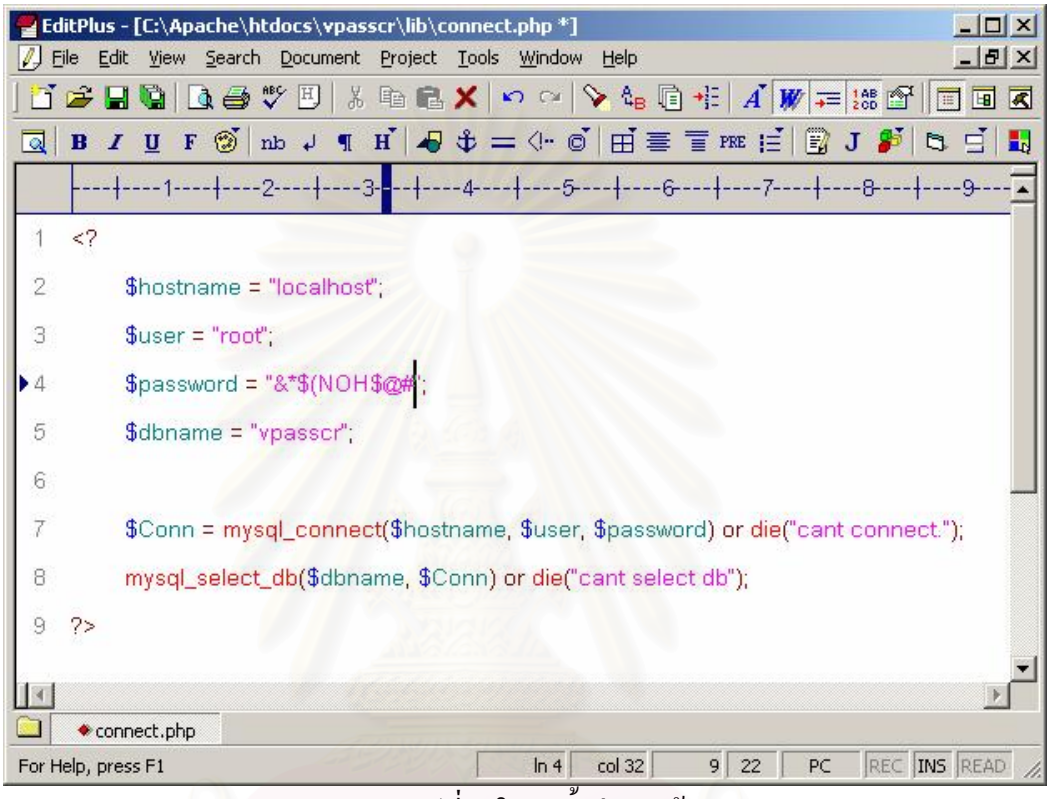


รูปที่ ข.7 คัดลอกโฟลเดอร์จาก db.rar ลงในโฟลเดอร์ mysql\data

ข.3 การตั้งค่าซอฟต์แวร์

หลังจากติดตั้งซอฟต์แวร์เรียบร้อยแล้ว ขั้นตอนต่อมาคือการตั้งค่าซอฟต์แวร์ตามเครื่องที่ใช้ โดยมี 2 ขั้นตอนดังนี้

1. การตั้งค่าฐานข้อมูล เปิดไฟล์ vpasscr\lib\connect.php ขึ้นมาดังรูปที่ ข.8



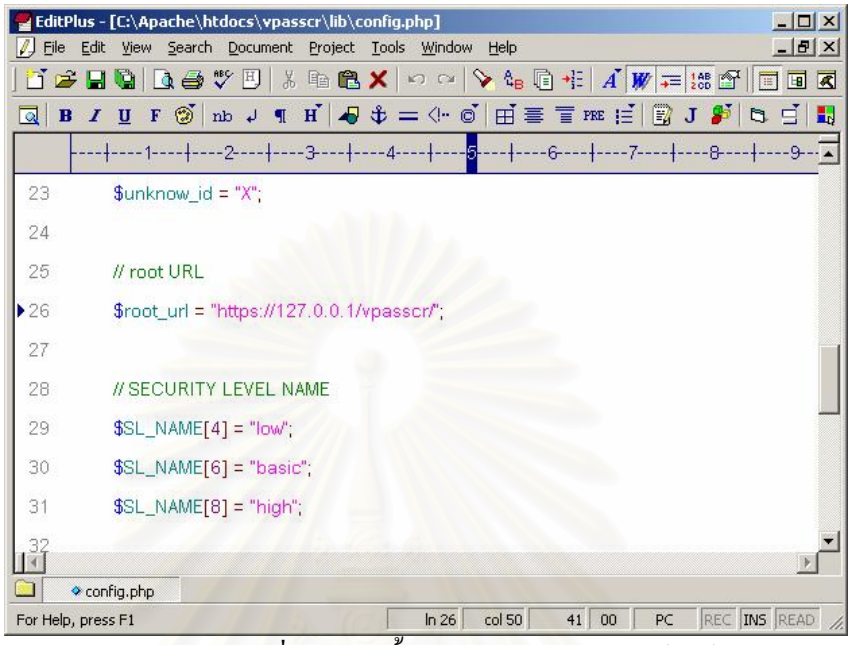
รูปที่ ข.8 การตั้งค่าฐานข้อมูล

ค่าที่ต้องทำการตั้งค่ามี 4 ค่าดังนี้

ตารางที่ ข.1 ตัวแปรในการตั้งค่าฐานข้อมูล

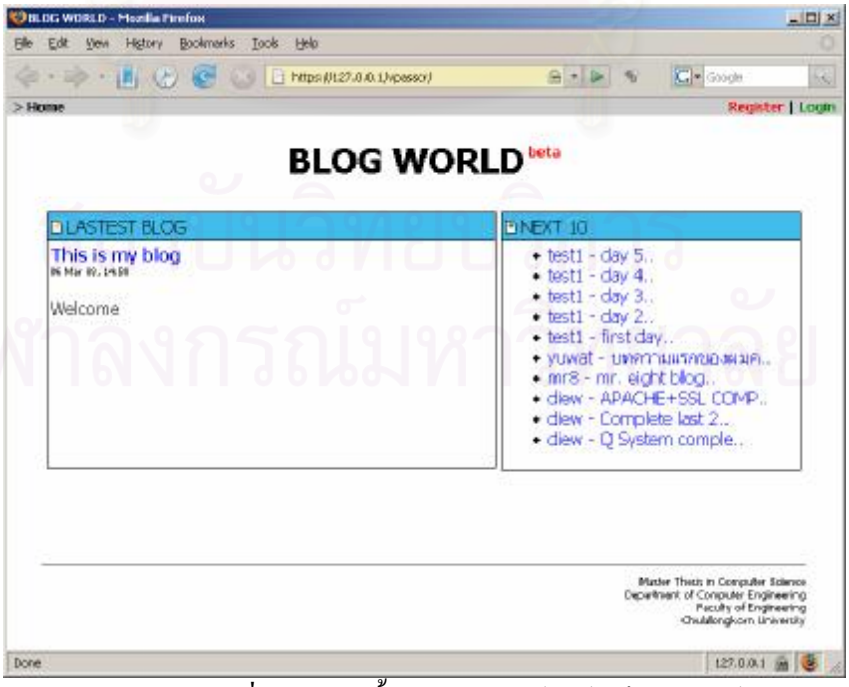
ชื่อตัวแปร	**คำอธิบาย**
$hostname	ชื่อของเครื่องที่ติดตั้งซอฟต์แวร์
$user	ชื่อผู้ใช้ของฐานข้อมูล mySQL
$password	รหัสผ่านผู้ใช้ของฐานข้อมูล mySQL
$dbname	ชื่อฐานข้อมูล

2. การตั้งค่าหน้าหลักของซอฟต์แวร์ เปิดไฟล์ vpasscr\lib\config.php ขึ้นมา ในบรรทัดที่ 26 ทำการตั้งค่าหน้าหลักของซอฟต์แวร์ให้ตรงกับเครื่อง ดังรูปที่ ข.9



รูปที่ ข.9 การตั้งค่าหน้าหลักของซอฟต์แวร์

3. ทดลองเปิดหน้าหลักของซอฟต์แวร์เพื่อตรวจสอบว่าการตั้งค่าของซอฟต์แวร์เสร็จสมบูรณ์ดังรูปที่ ข.10



รูปที่ ข.10 การตั้งค่าของซอฟต์แวร์เสร็จสมบูรณ์

ประวัติผู้เขียนวิทยานิพนธ์

นายยุวัฒน์ เชื้อสาธุชน เกิดเมื่อวันที่ 3 พฤษภาคม พ.ศ. 2526 ที่จังหวัดอุบลราชธานี สำเร็จการศึกษาระดับปริญญาบัณฑิต หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ จาก มหาวิทยาลัยขอนแก่น เมื่อ พ.ศ. 2548 และได้เข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ณ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปี พ.ศ. 2548