

รายงานฉบับสมบูรณ์

รหัสโครงการ 17P23W0039

ซอฟต์แวร์ป้องกันการปลอมตัวตนด้วยลายเซ็น

(Shoulder surfing protector with dynamic signature recognition)

โปรแกรมเพื่อการประยุกต์ใช้งาน

รายงานฉบับสมบูรณ์

เสนอต่อ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

กระทรวงวิทยาศาสตร์และเทคโนโลยี

ได้รับทุนอุดหนุน โครงการวิจัย พัฒนาและวิศวกรรม

โครงการแข่งขันพัฒนาโปรแกรมคอมพิวเตอร์แห่งประเทศไทย ครั้งที่ 17

ประจำปีงบประมาณ 2557

โดย

นายธนวรรณ ดีโป

นายปณัฏฐ์ บุญเอกอนันต์

นายพิชิต อุปพันธ์

ผศ.ดร.โชติรัตน์ รัตนมัทธนะ

โรงเรียนมหิดลวิทยานุสรณ์

กิตติกรรมประกาศ

ขอขอบคุณศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ(NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติที่ให้ทุนสนับสนุนภายใต้ชื่อโครงการ **Shoulder surfing protector with dynamic signature recognition** ในการแข่งขันพัฒนาโปรแกรมคอมพิวเตอร์แห่งประเทศไทย ครั้งที่ 17

ขอขอบพระคุณ อาจารย์พิชิตต์ อุปพันธ์ อาจารย์ที่ปรึกษา และผู้ช่วยศาสตราจารย์ ดร.โชติรัตน์ รัตนมัทธนะซึ่งกรุณาสละเวลาให้ความรู้และคำแนะนำตลอดการทำโครงการ

ขอขอบพระคุณ โรงเรียนมหิดลวิทยานุสรณ์ ที่เอื้อเฟื้อระบบอินเทอร์เน็ตไร้สายอันเป็นพันธมิตรสำคัญที่ทำให้โครงการนี้ขับเคลื่อนไปได้

ท้ายที่สุด ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ ผู้ให้กำลังใจและให้โอกาสการศึกษาอันมีค่ายิ่งขอบคุณ พี่ๆเพื่อนๆและน้องๆทุกคนที่ได้ให้ความช่วยเหลือในด้านต่างๆจนทำให้โครงการนี้สำเร็จเสร็จไปได้ด้วยดี

ผู้พัฒนา

31 ม.ค. 2558

บทคัดย่อ

ปัจจุบันข้อมูลของเราต้องมีการป้องกันเพื่อความปลอดภัยที่มากขึ้น ถ้าต้องการให้รหัสผ่านมีความซับซ้อนมากขึ้น เราสามารถเพิ่มอักขระพิเศษเช่น @, #, _ และ % เป็นต้น หรือ เพิ่มความยาวของรหัสผ่าน ไม่ว่าจะวิธีใดก็ตาม ต่างก็เพิ่มระยะเวลาที่ผู้ใช้ใช้ในการเข้าสู่ระบบ ในโครงการนี้การระบุตัวตนจะรวดเร็ว ปลอดภัย จากการ shoulder surfing โดยใช้เทคนิคการจดจำลายเส้นบนข้อมูล time series อัลกอริทึม dynamic time warping ใช้ในการวัดระยะห่างเพื่อนำไปวิเคราะห์และจดจำลายเส้นที่รับเข้ามาในรูปแบบพิกัด (x, y) เราสร้างส่วนติดต่อผู้ใช้แบบพิเศษขึ้นมาใหม่ซึ่งผู้ใช้งานสามารถเขียนลายเส้นและจะเก็บข้อมูลลายเส้นทุกๆ 10 ms ข้อมูลที่รับเข้ามาจะถูกวิเคราะห์ในกระบวนการระบุตัวตนเพื่อยืนยันตัวตนผู้ใช้งาน การทดลองของเราพิสูจน์ว่าโปรแกรม shoulder-surfing protector ที่เราสร้างขึ้นสามารถเพิ่มความปลอดภัยต่อบัญชีผู้ใช้ได้

คำสำคัญ: shoulder surfing, signature recognition, dynamic time warping, time series data

บทนำ

ในปัจจุบัน การพิสูจน์ตัวตนนั้น มีหลายรูปแบบ ซึ่งในแต่ละรูปแบบ มีทั้งข้อดีและข้อเสีย ผู้ที่ต้องการให้ข้อมูลของตนมีความเป็นส่วนตัว ก็ควรเพิ่มความยากในการเข้ารหัส เช่น เพิ่มความยาวของรหัส หรือ การใช้อักขระพิเศษเป็นต้น ซึ่งจะทำให้ใช้เวลานานในการพิสูจน์ตัวตน และในบางครั้งอาจมีผู้ไม่ประสงค์ดีสามารถรู้ข้อมูลของรหัสได้โดยวิธีการต่างๆ เช่น การแอบมองในขณะที่กรอกรหัส หรือ การใช้โปรแกรมบางอย่างในการบันทึกข้อมูลรหัสที่กรอก เป็นต้น ซึ่งจะก่อให้เกิดความเสียหายต่อเจ้าของรหัสได้ ข้าพเจ้าจึงสร้างโปรแกรมเพื่อแก้ปัญหาการพิสูจน์ตัวตนดังกล่าว

สารบัญ

หน้า

กิตติกรรมประกาศ.....	ก
บทคัดย่อ	ข
บทนำ	ค
สารบัญ.....	ง
วัตถุประสงค์และเป้าหมาย.....	1
สรุปปัญหา.....	1
สมมติฐาน/เป้าหมายโครงการ	1
รายละเอียดของการพัฒนา	2
เนื้อเรื่องย่อ	2
ทฤษฎีหลักการที่ใช้.....	3
หลักการที่ใช้.....	3
อัลกอริทึม.....	3
การวิเคราะห์พิกัด.....	4
เครื่องมือที่ใช้ในการพัฒนา.....	4
รายละเอียดเชิงเทคนิคของโปรแกรม	4
Input.....	5
Output.....	5
Functional Specification	5
ขอบเขตและข้อจำกัดของโปรแกรม	6
คุณลักษณะของอุปกรณ์ที่ใช้กับโปรแกรม.....	6
กลุ่มผู้ใช้โปรแกรม.....	7
ผลของการทดสอบโปรแกรม.....	8

ตารางสรุปผลการทดลอง	11
กราฟแสดงผลการทดลอง	12
การวิเคราะห์ข้อมูล	12
เปรียบเทียบความแม่นยำระหว่างอัลกอริทึม Dynamic Time Warping (DTW) กับอัลกอริทึม Off-line	12
เปรียบเทียบจำนวนครั้งที่เข้าสู่ระบบสำเร็จเมื่อใช้จังหวะในการวิเคราะห์ของผู้ใช้งานจริงกับผู้ปลอมแปลง	12
การสรุปผลข้อมูล.....	13
เปรียบเทียบความแม่นยำระหว่างอัลกอริทึม Dynamic Time Warping (DTW) กับอัลกอริทึม Off-line	13
เปรียบเทียบจำนวนครั้งที่เข้าสู่ระบบสำเร็จเมื่อใช้จังหวะในการวิเคราะห์ของผู้ใช้งานจริงกับผู้ปลอมแปลง	13
ปัญหาและอุปสรรค	14
แนวทางในการพัฒนาและประยุกต์ใช้.....	15
ข้อสรุปและข้อเสนอแนะ	16
ข้อสรุป	16
ข้อเสนอแนะ	16
เอกสารอ้างอิง	17
ผู้พัฒนาและอาจารย์ที่ปรึกษา	18
ภาคผนวก	20
คู่มือการติดตั้งโปรแกรม.....	20
คู่มือการใช้งานโปรแกรม.....	21

วัตถุประสงค์และเป้าหมาย

ในปัจจุบัน การพิสูจน์ตัวตนนั้น มีหลายรูปแบบ ซึ่งในแต่ละรูปแบบ มีทั้งข้อดีและข้อเสีย ผู้ที่ต้องการให้ข้อมูลของตนมีความเป็นส่วนตัว ก็ควรเพิ่มความยากในการเข้ารหัส เช่น เพิ่มความยาวของรหัส หรือ การใช้อักขระพิเศษเป็นต้น ซึ่งจะทำให้ใช้เวลานานในการพิสูจน์ตัวตน และในบางครั้งอาจมีผู้ไม่ประสงค์ดีสามารถรู้ข้อมูลของรหัสได้โดยวิธีการต่างๆ เช่น การแอบมองในขณะที่กรอกรหัส หรือ การใช้โปรแกรมบางอย่างในการบันทึกข้อมูลรหัสที่กรอก เป็นต้น และเมื่อรหัสของเราถูกขโมยไปด้วยผู้ไม่ประสงค์ดี จะทำให้เกิดความไม่ปลอดภัยของข้อมูลและเกิดความเสียหายต่อเจ้าของรหัสได้ ซึ่งสิ่งเดียวที่จะสามารถแก้ปัญหานี้ได้ก็คือการเปลี่ยนรหัสผ่านใหม่ซึ่งจะทำให้ผู้ใช้งานนั้นเสียเวลาในการสร้างรหัสผ่านใหม่ และยากต่อการจดจำรหัสผ่านใหม่อีก ข้าพเจ้าจึงสร้างโปรแกรมเพื่อแก้ปัญหการพิสูจน์ตัวตนดังกล่าว

สรุปปัญหา

1. เกิดจากการที่มีผู้ไม่ประสงค์ดีสามารถขโมยรหัสด้วยวิธีการแอบมอง
2. ความยากในการสร้าง จดจำ และกรอกรหัสผ่านของผู้ใช้

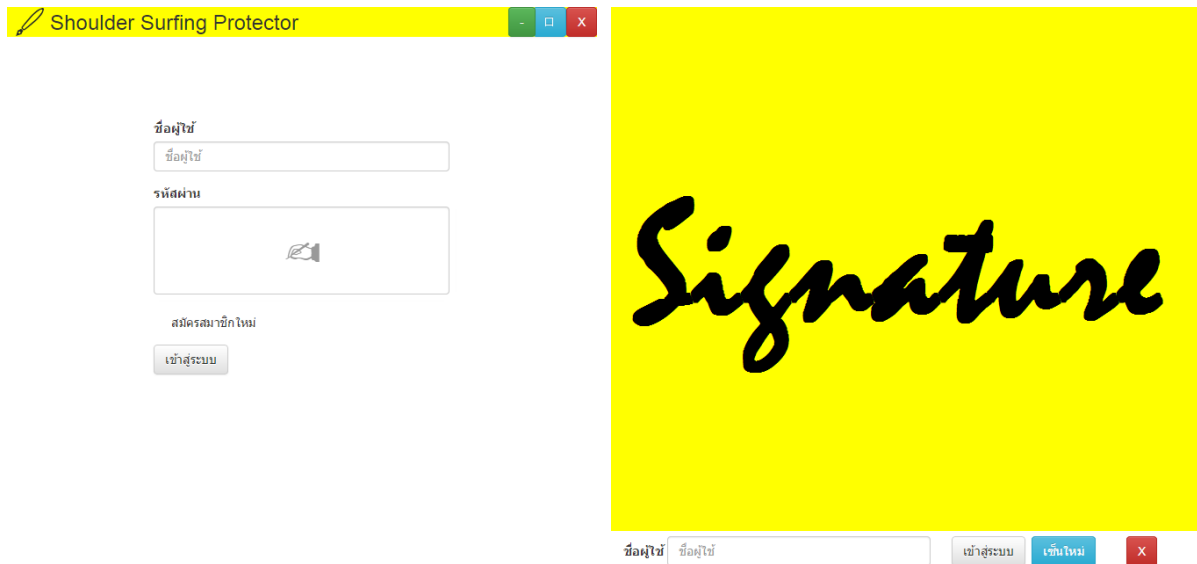
สมมติฐาน/เป้าหมายโครงการ

1. การเพิ่มจังหวะการเซ็นในอัลกอริทึมที่สอง ช่วยป้องกัน **shoulder surfing** ได้ดีกว่าอัลกอริทึมแรก
2. สร้างซอฟต์แวร์ในการยืนยันตัวตนที่สามารถป้องกัน **shoulder surfing** ได้อย่างมีประสิทธิภาพ

รายละเอียดของการพัฒนา

เนื้อเรื่องย่อ

แบบร่างของโปรแกรม Shoulder Surfing Protector



เมื่อคลิกที่ช่องรหัสผ่าน จะปรากฏพื้นที่ลงลายเซ็นแบบเต็มหน้าจอ



เมื่อเข้าสู่ระบบแล้วไม่ผ่าน ต้องเซ็นใหม่อีกครั้ง

เมื่อเซ็นเรียบร้อยแล้วกด X ช่องรหัสผ่านจะแสดงสีเขียว

ทฤษฎีหลักการที่ใช้

หลักการที่ใช้

Z-normalization

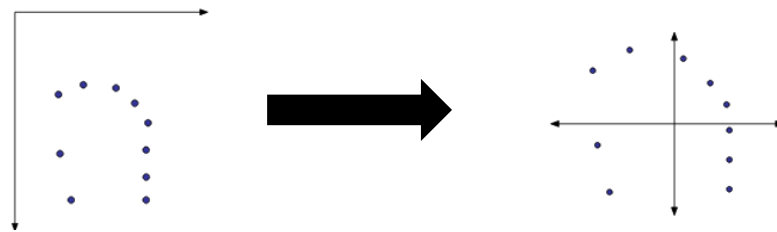
เป็นหลักการที่ใช้ในการปรับค่าของพิกัดก่อนจะนำไปวิเคราะห์ด้วยอัลกอริทึมต่างๆ

สมการ

$$X_{new} = \frac{x - \bar{x}}{S.D._x} \times size$$

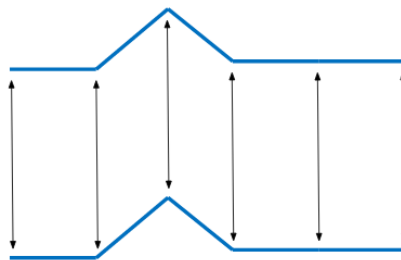
$$Y_{new} = \frac{y - \bar{y}}{S.D._y} \times size$$

ตำแหน่งของพิกัดหลังจากผ่านการ Z-normalization จะกระจายตำแหน่งโดยรอบจุดกำเนิด (0,0) เป็นระยะทางเฉลี่ยโดยรวมเท่ากับค่า size ที่เรากำหนดไว้



อัลกอริทึม

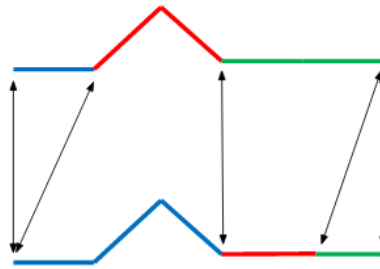
1. Off-line algorithm



กำหนดให้ลายเส้นล่างเป็นลายเส้นที่รับเข้ามาใหม่ และลายเส้นบนเป็นลายเส้นเทมเพลต

อัลกอริทึมนี้จะวิเคราะห์เฉพาะรูปร่าง รูปทรงของลายเส้นเท่านั้น โดยเมื่อผู้ใช้งานเซ็นสำเร็จ จะทำการสร้างพิกัดเพื่อแบ่งลายเส้นออกเป็นส่วนๆ ที่เท่ากันแล้วจึงทำการวิเคราะห์ค่าความแตกต่างของพิกัดพวกนี้กับเทมเพลต

2. Dynamic Time Warping algorithm (DTW)



กำหนดให้ลายเส้นล่างเป็นลายเส้นที่รับเข้ามาใหม่ ลายเส้นบนเป็นลายเส้นเทมเพลต และแต่ละสีคือจังหวะต่างๆกัน

อัลกอริทึมนี้จะรับค่าพิกัดขณะที่ผู้ใช้งานเขียนลายเส้น (แบบ on-line) โดยจะรับค่าพิกัดทุกๆ 10 ms แล้วนำไปวิเคราะห์ค่าความแตกต่างของพิกัดเหล่านี้กับเทมเพลต แม้ว่ารูปร่าง รูปทรงของลายเส้นจะเหมือนกัน แต่ถ้าจังหวะในการเขียนต่างกัน การยืนยันตัวตนด้วยอัลกอริทึมนี้ก็จะไม่สำเร็จ

การวิเคราะห์พิกัด

ในทุกๆพิกัดที่รับเข้ามา อัลกอริทึมก็จะนำพิกัดที่รับมาทุกพิกัดมาจับคู่กับพิกัดที่เหมาะสมในเทมเพลต โดยพิจารณาหาระยะห่างระหว่างคู่พิกัดที่น้อยที่สุด ถ้าลายเส้นที่รับเข้ามาใกล้เคียงกับลายเส้นในเทมเพลต ระยะทางระหว่างคู่พิกัดก็จะน้อย อัลกอริทึมจะพิจารณาระยะทางเหล่านี้ โดยเทียบกับช่วงระยะทางที่ยอมรับได้ว่าเป็นลายเส้นที่เหมือนกัน

เครื่องมือที่ใช้ในการพัฒนา

- พัฒนาด้วยภาษา C#
- พัฒนาด้วย Windows Presentation Foundation (WPF) applications
- พัฒนากับ Microsoft Windows 8
- Microsoft Visual Studio Express 2013 for Windows Desktop

รายละเอียดเชิงเทคนิคของโปรแกรม

ในโปรแกรมยืนยันตัวตนจะเปรียบเทียบ 2 อัลกอริทึม ดังนี้

1. อัลกอริทึมแรก เป็นการประมวลผลแบบ off-line โดยมองลายเส้นเป็นเสมือนภาพบนกระดาษ ซึ่งใช้การวิเคราะห์จากรูปร่าง (shape) เป็นหลัก การประมวลผลแบบ off-line จะกระทำเมื่อสิ้นสุดการลงลายเส้น

2. อัลกอริทึมที่สอง เป็นการประมวลผลแบบ on-line โดยเพิ่มตัวแปรเรื่องเวลาเข้ามาเกี่ยวข้อง เช่น ความสัมพันธ์ของพิกัดในแกน x กับเวลา: $x(t)$, จังหวะการเขียน, Dynamic time warping (DTW) การประมวลผลแบบ on-line จะกระทำระหว่างการลงลายเซ็น

Input

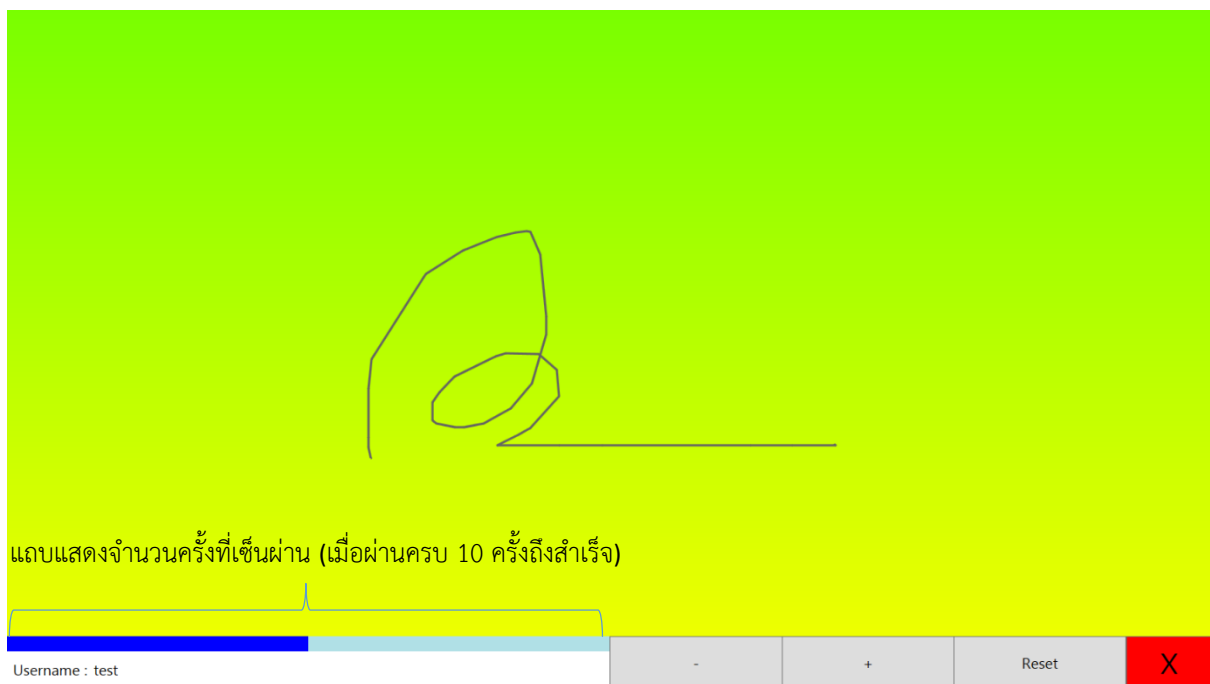
List ของพิกัด (x,y) ของลายเซ็นในทุกๆหนึ่งหน่วยเวลาคงที่ และเวลาในการยกปากกาแต่ละครั้ง

Output

ผลการยืนยันตัวตนด้วยอัลกอริทึมที่สอง คือ ผ่านและไม่ผ่าน

Functional Specification

1. ให้ลายมือหรือลายเซ็นเป็นรหัสผ่านในการยืนยันตัวตนเพื่อเข้าใช้บัญชี
2. บัญชีผู้ใช้ 1 บัญชี รองรับลายมือหรือลายเซ็น 1 อัน
3. สร้างบัญชีผู้ใช้ใหม่ด้วยการเซ็น 10 ลายเซ็น



4. รองรับการเซ็นหลายส่วนโดยการยกปากกา



5. มีการอัปเดตการเปลี่ยนแปลงของลายเซ็นทุกครั้งที่ยืนยันตัวตนผ่าน

ขอบเขตและข้อจำกัดของโปรแกรม

- ใช้กับระบบปฏิบัติการ Microsoft Windows 7 เป็นต้นไป
- ใช้กับเครื่องมือที่สามารถวาดพิกัดได้ เช่น touch screen, mouse pen, touchpad เป็นต้น

คุณลักษณะของอุปกรณ์ที่ใช้กับโปรแกรม

- touch screen
- mouse pen
- touchpad
- เครื่องมืออื่นๆ ที่สามารถวาดพิกัดได้

กลุ่มผู้ใช้โปรแกรม

ผู้ที่ต้องการให้ระบบการยืนยันตัวตนของตนเองมีประสิทธิภาพมากขึ้น

สามารถใช้ได้กับผู้ใช้งานทุกคนที่มีบัญชีผู้ใช้เป็นของตนเอง และสามารถเขียนได้ (ใช้ไม่ได้กับผู้พิการทางการเขียน)

ผลของการทดสอบโปรแกรม

ผู้ทดสอบ(คนที่)	ครั้งที่เซ็น	ทดลองเข้ารหัสด้วยลายเซ็น			
		ผู้ใช้จริง		ผู้ปลอมแปลง	
		Off-line	DTW	Off-line	DTW
1	1	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	2	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	3	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	4	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	5	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	6	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	7	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	8	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	9	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	10	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
2	1	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	2	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	3	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	4	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	5	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	6	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	7	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	8	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	9	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	10	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
3	1	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	2	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	3	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	4	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	5	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	6	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	7	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	8	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	9	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	10	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
4	1	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	2	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	3	ผ่าน	ไม่ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	4	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	5	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	6	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	7	ผ่าน	ไม่ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	8	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	9	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน

[illegible]

9	1	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	2	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	3	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	4	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	5	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	6	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	7	ผ่าน	ผ่าน	ผ่าน	ผ่าน
	8	ผ่าน	ไม่ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	9	ผ่าน	ไม่ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	10	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
10	1	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	2	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	3	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	4	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	5	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	6	ผ่าน	ไม่ผ่าน	ผ่าน	ไม่ผ่าน
	7	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	8	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน
	9	ผ่าน	ผ่าน	ไม่ผ่าน	ไม่ผ่าน
	10	ผ่าน	ผ่าน	ผ่าน	ไม่ผ่าน

ในการทดลองเราควบคุมตัวแปรโดย

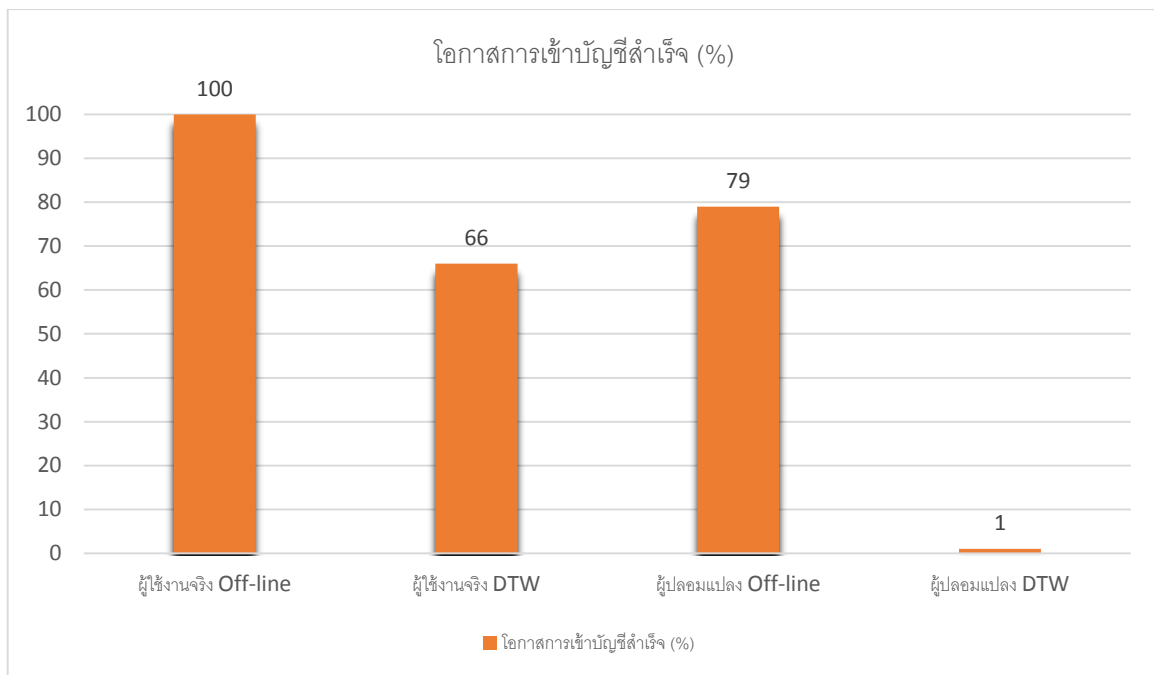
ผู้ใช้งานจริงเซ็นลายเซ็นลงในกระดาษแล้วนำไปให้ผู้ปลอมแปลงศึกษาลักษณะก่อน แล้วจึงเข้าสู่ระบบ

ได้ว่าผู้ปลอมแปลงรู้ถึงรูปร่างลักษณะของลายเซ็นแต่ไม่สามารถทราบถึงจังหวะที่ใช้ในการเซ็น

ตารางสรุปผลการทดลอง

ผู้ทดสอบ (คนที่)	ผู้ใช้งานจริง (จำนวนครั้งที่ผ่าน)		ผู้ปลอมแปลง (จำนวนครั้งที่ผ่าน)	
	Off-line	DTW	Off-line	DTW
1	10	7	8	0
2	10	6	8	0
3	10	8	10	0
4	10	6	8	0
5	10	7	8	0
6	10	5	9	0
7	10	8	8	0
8	10	6	6	0
9	10	6	6	1
10	10	7	8	0
รวม	100	66	79	1

กราฟแสดงผลการทดลอง



การวิเคราะห์ข้อมูล

กรณีที่อัลกอริทึมประมวลผลถูกต้องคือ

1. เข้าบัญชีสำเร็จเมื่อเป็นผู้ใช้งานจริง
2. เข้าบัญชีไม่สำเร็จเมื่อเป็นผู้ปลอมแปลง

เปรียบเทียบความแม่นยำระหว่างอัลกอริทึม Dynamic Time Warping (DTW) กับอัลกอริทึม Off-line

1. นับจำนวนครั้งที่อัลกอริทึมประมวลผลถูกต้องของแต่ละบัญชีผู้ใช้ ซึ่งก็คือผ่านเมื่อผู้เซ็นเป็นเจ้าของบัญชี และไม่ผ่านเมื่อผู้เซ็นไม่ใช่เจ้าของบัญชีผู้ใช้นั้น รวมทั้งหมด 20 ครั้งต่อหนึ่งบัญชีผู้ใช้ (จากผู้ใช้จริง 10 ครั้ง และ การถูกปลอมตัวตน 10 ครั้ง ตามข้อ)
2. กลุ่มแรก นำเลขจำนวนครั้งที่ถูกของอัลกอริทึม Dynamic Time Warping (DTW) 10 จำนวน (10 บัญชีผู้ใช้) มาเปรียบเทียบกับ กลุ่มที่สอง นำเลขจำนวนครั้งที่ถูกของอัลกอริทึม Off-line 10 จำนวน (10 บัญชีผู้ใช้) ว่าแตกต่างกันอย่างมีนัยสำคัญหรือไม่อย่างไร ด้วยวิธีการทางสถิติ T-test

เปรียบเทียบจำนวนครั้งที่เข้าสู่ระบบสำเร็จเมื่อใช้จังหวะในการวิเคราะห์ของผู้ใช้งานจริงกับผู้ปลอมแปลง

1. นับจำนวนครั้งที่ลดลงเมื่อเปลี่ยนการเข้าสู่ระบบด้วย อัลกอริทึม Off-line (ไม่พิจารณาจังหวะ) เป็นการเข้าสู่ระบบด้วย อัลกอริทึม Dynamic Time Warping (พิจารณาจังหวะ)

2. กลุ่มแรกของ ผู้ใช้งานจริง กลุ่มที่สองของผู้ปลอมแปลง นำมาเปรียบเทียบกับว่าแตกต่างกันอย่างมีนัยสำคัญหรือไม่อย่างไร ด้วยวิธีการทางสถิติ T-test

การสรุปผลข้อมูล

เปรียบเทียบความแม่นยำระหว่างอัลกอริทึม Dynamic Time Warping (DTW) กับอัลกอริทึม Off-line

- อัลกอริทึม DTW

ผู้ใช้งานจริงเข้าระบบได้ 66 ครั้งจาก 100 ครั้งเพราะฉะนั้นประมวลผลถูกต้องเท่ากับ 66 ครั้งจาก 100 ครั้ง

ผู้ปลอมแปลงเข้าระบบได้ 1 ครั้งจาก 100 ครั้งเพราะฉะนั้นประมวลผลถูกต้องเท่ากับ 99 ครั้งจาก 100 ครั้ง

รวมอัลกอริทึมประมวลผลถูกต้อง 165 ครั้งจาก 200 ครั้ง คิดเป็น 82.5 %

- อัลกอริทึม Off-line

ผู้ใช้งานจริงเข้าระบบได้ 100 ครั้งจาก 100 ครั้งเพราะฉะนั้นประมวลผลถูกต้องเท่ากับ 100 ครั้งจาก 100 ครั้ง

ผู้ใช้งานจริงเข้าระบบได้ 79 ครั้งจาก 100 ครั้งเพราะฉะนั้นประมวลผลถูกต้องเท่ากับ 21 ครั้งจาก 100 ครั้ง

รวมอัลกอริทึมประมวลผลถูกต้อง 121 ครั้งจาก 200 ครั้ง คิดเป็น 60.5 %

เมื่อนำข้อมูลการประมวลผลถูกต้องของแต่ละบัญชีผู้เข้ามาเปรียบเทียบกับได้ว่าแตกต่างกันอย่างมีนัยสำคัญ

จากเปอร์เซ็นต์ที่อัลกอริทึมประมวลผลถูกต้อง ได้ว่าอัลกอริทึม Dynamic Time Warping (DTW) มีความแม่นยำมากกว่า อัลกอริทึม Off-line คิดเป็น 12%

เปรียบเทียบจำนวนครั้งที่เข้าสู่ระบบสำเร็จเมื่อใช้จังหวะในการวิเคราะห์ของผู้ใช้งานจริงกับผู้ปลอมแปลง จำนวนครั้งที่ผู้ใช้งานจริงเข้าสู่ระบบด้วย อัลกอริทึม Off-line เท่ากับ 100 ครั้ง อัลกอริทึม Dynamic Time Warping (DTW) เท่ากับ 66 ครั้ง ลดลงเท่ากับ 34 ครั้ง

จำนวนครั้งที่ผู้ปลอมแปลงเข้าสู่ระบบด้วย อัลกอริทึม Off-line เท่ากับ 79 ครั้ง อัลกอริทึม Dynamic Time Warping (DTW) เท่ากับ 1 ครั้ง ลดลงเท่ากับ 78 ครั้ง

เมื่อพิจารณาจำนวนครั้งที่ลดลงได้ว่า การพิจารณาจังหวะในการเซ็นสามารถลดจำนวนการเข้าของผู้ปลอมแปลงได้มากกว่าผู้ใช้งานจริง

สรุปได้ว่าการนำจังหวะมาพิจารณาสามารถแก้ปัญหา Shoulder Surfing ได้

ปัญหาและอุปสรรค

1. ในการใช้งานจริง การเซ็นแต่ละครั้ง จะมีขนาดที่ไม่เท่ากันแต่รูปทรงจะเหมือนกัน จึงใช้เทคนิค **Z normalization** ลงไปเพื่อปรับพิกัดลายเซ็นให้มีขนาดเท่ากัน
2. ในบางลายเซ็นผู้ใช้อาจมีการยกปากกา จึงทำการรับข้อมูลที่ยกปากกเพิ่มขึ้นก่อนที่จะนำข้อมูลมาพิจารณาด้วยอัลกอริทึม
3. เมื่อเวลาผ่านไปลายเซ็นของผู้ใช้อาจมีการเปลี่ยนแปลงจึงทำการอัปเดตฐานข้อมูลลายเซ็นในทุกๆครั้งที่มีการยืนยันตัวตนผ่าน
4. ในการใช้งานจริงของกลุ่มผู้ทดลอง ในบางคนไม่มีเมาส์ปากกาจึงจำเป็นต้องมาให้ทดลองในเครื่องของผู้พัฒนา (สำหรับผู้ที่สามารถทดลองในเครื่องตนเองได้)

แนวทางในการพัฒนาและประยุกต์ใช้

1. เชื่อมต่อโปรแกรมเข้ากับโปรแกรมอื่น ที่บัญชี หรือ ฐานข้อมูลต้องการความปลอดภัย และความเป็นส่วนตัวเพื่อยืนยันตัวตนในการเข้าสู่ระบบ แทนการเข้าสู่ระบบรูปแบบอื่นๆ
2. สามารถนำไปพัฒนาโดยการวิเคราะห์ลายเซ็นเพื่อเป็นการแสดงตัวตน ซึ่งหลังจากเซ็นลายเซ็น โปรแกรมก็จําแนข้อมูลลายเซ็นมาวิเคราะห์เพื่อสามารถหาเจ้าของลายเซ็นได้ (ใช้แทน username)

ข้อสรุปและข้อเสนอแนะ

ข้อสรุป

1. โปรแกรมสามารถยืนยันตัวตนของผู้ใช้งานได้
2. โอกาสที่ผู้ใช้งานสามารถผ่านการยืนยันตัวตน 66 เปอร์เซ็นต์
3. โอกาสที่การปลอมตัวตนสำเร็จ 1 เปอร์เซ็นต์

ข้อเสนอแนะ

1. เนื่องจากในการสร้างบัญชีผู้ใช้นั้นมีการวิเคราะห์ลายเซ็นทุกครั้งที่น่าเข้ามา ในกลุ่มผู้ทดลองการสร้างบัญชีนั้นค่อนข้างยากจึงอาจทำให้ต้องเซ็นใหม่หลายครั้ง ทำให้ใช้เวลานานในการสร้างบัญชี ในกลุ่มผู้ทดลองเสนอแนะว่า “ควรลดจำนวนครั้งที่ใช้ในการสร้างบัญชี”

เอกสารอ้างอิง

1. Donald O. Tanguay, Jr. Hidden Markov Models for Gesture Recognition. Cambridge:Massachusetts Institute of Technology, 1995
2. Ying-Jun Weng. Time series clustering based on shape dynamic time warping using cloud models. IEEE, 2003
3. Rabiner, L. An introduction to hidden Markov models. IEEE, 2003
4. Yhat, Recognizing Handwritten Digits in Python. <http://blog.yhathq.com/posts/digit-recognition-with-node-and-python.html>, 2013
5. Dr. Faundez-Zanuy, On-line signature recognition based on VQ-DTW. Elsevier, 2007

ผู้พัฒนาและอาจารย์ที่ปรึกษา

ผู้พัฒนาคนที่ 1

ชื่อ-นามสกุล นายธนวรรธน์ ดีโป

โทรศัพท์ 028497000 มือถือ 087-6657779

E-mail d.tanawat@hotmail.com

ผู้พัฒนาคนที่ 2

ชื่อ-นามสกุล นายปณณธร บุญเอกอนันต์

โทรศัพท์ 028497000 มือถือ 080-2880111

โทรสาร 028497201 E-mail pok11pok@hotmail.com

อาจารย์ที่ปรึกษาหลัก

ชื่อ-นามสกุล นายพิชญุตม์ อุปพันธ์ ตำแหน่งครูวิชาการ

สังกัด โรงเรียนมหิดลวิทยานุสรณ์

สถานที่ติดต่อ 364 หมู่ 5 ตำบลศาลายา อำเภอพุทธมณฑล จังหวัดนครปฐม 73170

โทรศัพท์ 028497204 มือถือ 083-0846725

โทรสาร 028497201 E-mail pichayoot@mwit.ac.th

การศึกษา B.S. in Computer Science, University of illinois at Urbana-Champagn

M.S. in Computer Science, University of California San Diego

ขอบเขตงานที่เชี่ยวชาญ Computer Vision

อาจารย์ที่ปรึกษา

ชื่อ-นามสกุล ผศ.ดร.โชติรัตน์ รัตนมัทธนะ ตำแหน่งผู้ช่วยศาสตราจารย์ A-4

สังกัด ภาควิชาวิศวกรรมคอมพิวเตอร์

สถานที่ติดต่อ ชั้น 17 อาคาร 100 ปี คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย 254 ถนนพญาไท
แขวงวังใหม่ เขตปทุมวัน กทม. 10330

โทรศัพท์ 022153555

มือถือ 0894999400

E-mail chotirat@gmail.com

การศึกษา B.S. in Computer Science, Carnegie Mellon University, Pennsylvania, U.S.A.

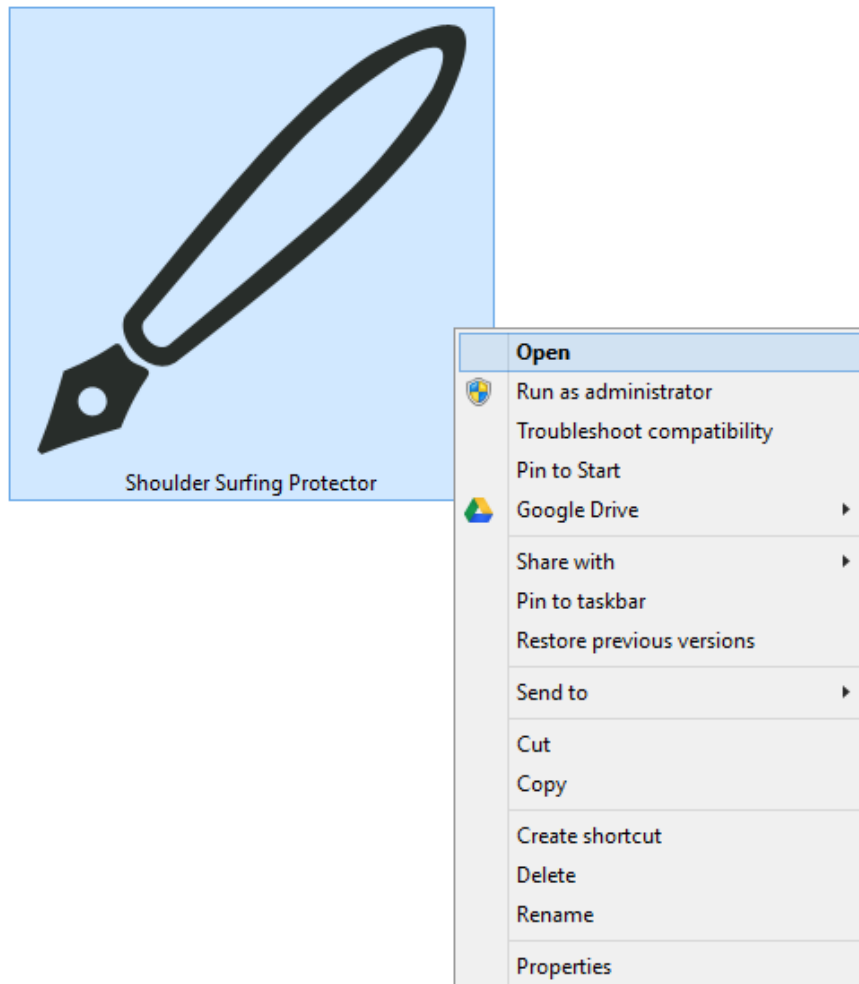
Ph.D. in Computer Science, University of California, Riverside, California, U.S.A.

ขอบเขตงานที่เชี่ยวชาญ Time Series Data

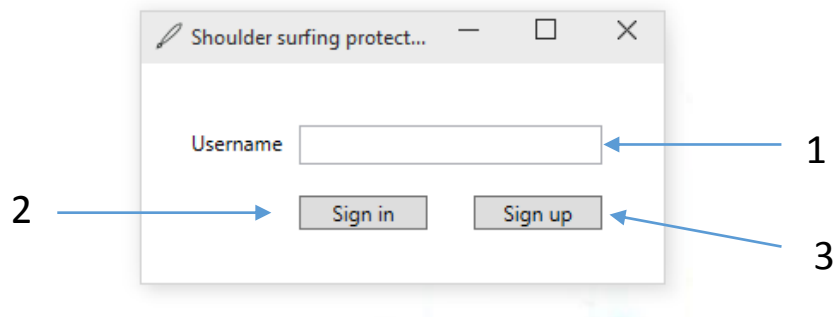
ภาคผนวก

คู่มือการติดตั้งโปรแกรม

สามารถเรียกใช้งานจากตัวโปรแกรมได้ทันที

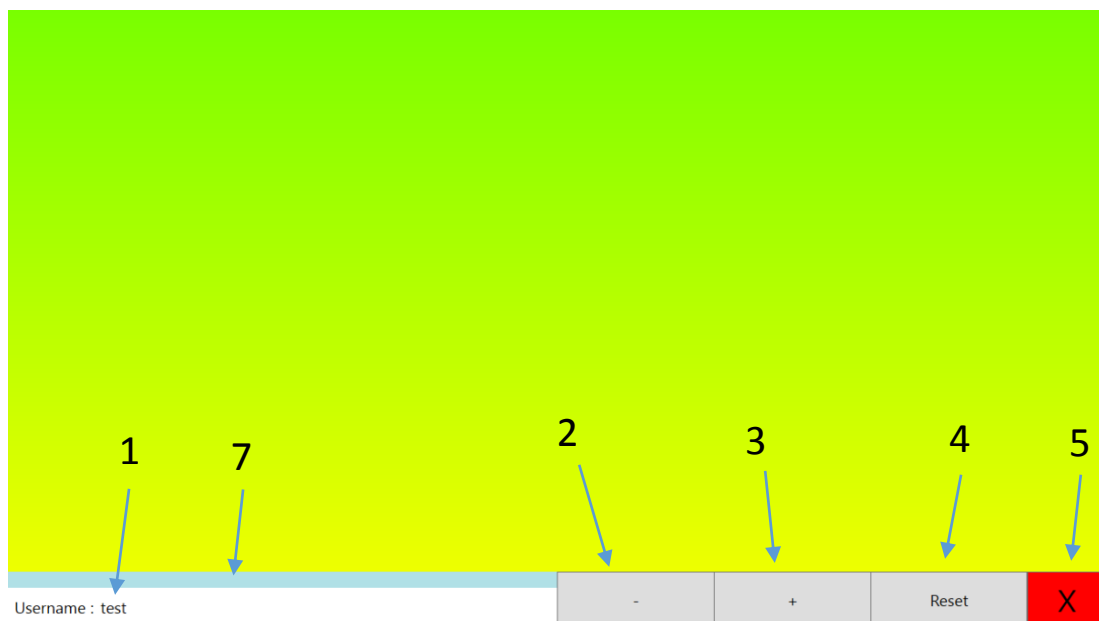


คู่มือการใช้งานโปรแกรม



โปรแกรม Shoulder Surfing Protector

1. กรอกรหัสความลับสำหรับกรอกบัญชีผู้ใช้
2. ปุ่มกดเพื่อเซ็นลายเซ็นเพื่อเข้าสู่บัญชี
3. ปุ่มกดเพื่อสร้างบัญชีผู้ใช้งานใหม่

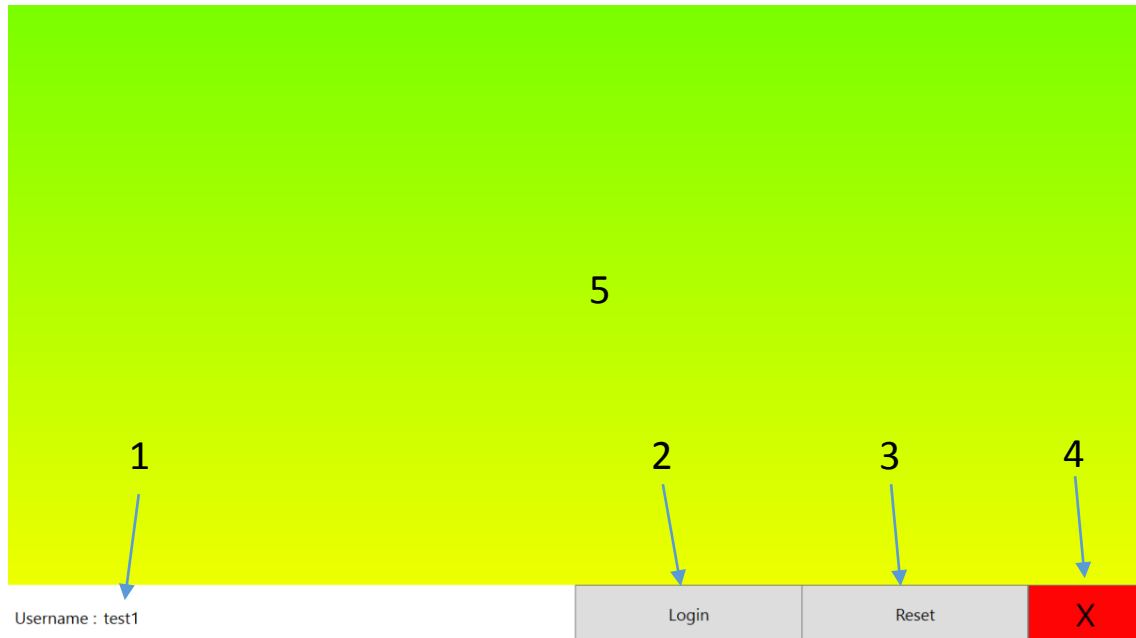


หน้าต่าง sign up

1. ชื่อบัญชีผู้ใช้
2. ปุ่มลบข้อมูลลายเซ็นก่อนหน้า
3. ปุ่มเก็บข้อมูลลายเซ็น
4. ปุ่มลบข้อมูลลายเซ็นที่เซ็นอยู่เพื่อเซ็นใหม่
5. ปุ่มปิดหน้าต่าง

6.พื้นที่สำหรับเซ็น

7.แถบบอกจำนวนลายเซ็นที่เก็บในเทมเพลต



หน้าต่างสำหรับเซ็นลายเซ็นเพื่อเข้าบัญชีผู้ใช้

- 1.ชื่อบัญชีผู้ใช้
- 2.ปุ่มเข้าสู่ระบบ
- 3.ปุ่มลบลายเซ็นเพื่อเซ็นใหม่
- 4.ปุ่มปิดหน้าต่าง
- 5.พื้นที่สำหรับเซ็น