การพิสูจน์ตนด้วยชีวมาตร

BIOMETRIC AUTHENTICATION

นายอาทิตย์ สามารถ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2548

การพิสูจน์ตนด้วยชีวมาตร

BIOMETRIC AUTHENTICATION

โดย

นายอาทิตย์ สามารถ

อาจารย์ที่ปรึกษา

อาจารย์อัครเดช วัชระภูพงษ์

ผศ.ธนา หงษ์สุวรรณ

อาจารย์ธนัญชัย ตรีภาค

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2548

ปริญญานิพนธ์ปีการศึกษา 2548

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การพิสูจน์ตนด้วยชีวมาตร

BIOMETRIC AUTHENTICATION

ผู้จัดทำ

นายอาทิตย์ สามารถ รหัสนักศึกษา 45010964

_____ อาจารย์ที่ปรึกษา

(อาจารย์ อัครเดช วัชระภูพงษ์)

_____ อาจารย์ที่ปรึกษา

(ผศ. ธนา หงษ์สุวรรณ)

_____ อาจารย์ที่ปรึกษา

(อาจารย์ ธนัญชัย ตรีภาค)

การพิสูจน์ตนด้วยชีวมาตร

นายอาทิตย์ สามารถ 45010964
อาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ผศ. ธนา หงษ์สุวรรณ อาจารย์ที่ปรึกษาร่วม
อาจารย์ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษาร่วม
ปีการศึกษา 2548

บทคัดย่อ

หากกล่าวถึงระบบรักษาความปลอดภัยแล้ว จะมีหลายลักษณะ หลายวิธีการแตกต่างกันไป ไม่ว่าจะมองในระดับไหน รูปแบบหนึ่งซึ่งนับได้ว่าเกี่ยวข้อง คือ การพิสูจน์ตน ซึ่งในปัจจุบัน การพิสูจน์ตนก็เป็นวิธีการ เป็นกระบวนการหนึ่งที่มีการนำไปใช้กันอย่างกว้างขวางในทุกวงการ ทั้งองค์กรขนาดเล็ก หรือขนาดใหญ่ แต่หากจะกล่าวแล้วรูปแบบที่น่าจะเป็นที่คุ้นเคยกันมากรูปแบบหนึ่งคือ การพิสูจน์ตนเมื่อมีการเข้าใช้งานคอมพิวเตอร์ โดยเฉพาะระบบปฏิบัติการลินุกซ์ ซึ่งก่อนจะเข้าใช้งานระบบได้นั้นจำเป็นต้องมีการใส่ชื่อบัญชีผู้ใช้ เพื่อแสดงความจำนงเข้าใช้งาน และโดยปกติแล้ว จะมีการถามรหัสผ่านสำหรับการเข้าใช้งานในชื่อบัญชีผู้ใช้ดังกล่าว นอกจากวิธีการพิสูจน์ตนโดยใช้ชื่อบัญชีผู้ใช้ และรหัสผ่านแล้ว ก็ยังมีวิธีการในลักษณะอื่นอีก ซึ่งมีความน่าเชื่อถือ และรูปแบบการใช้งานที่ต่างกันออกไป หนึ่งในหลายรูปแบบของการพิสูจน์ตนคือ การพิสูจน์ตนด้วยชีวมาตร ซึ่งมีการใช้ลักษณะเฉพาะของแต่ละบุคคลเป็นสิ่งยืนยันแทนการใช้รหัสผ่านดังได้กล่าวมา

ระบบที่พัฒนา มุ่งเน้นในส่วนของการนำเอาระบบรักษาความปลอดภัยโดยการใช้ใบหน้าในการตรวจสอบยืนยันผู้เข้าใช้งานในระบบปฏิบัติการลินุกซ์ แทนการใช้รหัสผ่าน ซึ่งจะกล่าวถึงวิธีการในการใช้งานเมื่อผู้ใช้ต้องการ ล็อกอินเข้าใช้งาน โดยชื่อบัญชีผู้ใช้ของตนเอง นอกจากนั้นจะกล่าวถึงในส่วนของผู้ดูแลระบบซึ่งสามารถเพิ่มหรือ ลบผู้ใช้งานได้ด้วย รวมไปถึงทฤษฎีบทที่เกี่ยวข้อง กับงานวิจัยครั้งนี้

BIOMETRIC AUTHENTICATION

Arthit Samart	45010964
Akkaradach Watcharapupong	Advisor
Asst.Prof. Thana Hongsuwan	Co-Advisor
Tananchai Treepak	Co-Advisor
Academic Year 2005	

ABSTRACT

According to the security, there are several mechanisms which are different from each other. Authentication is one of those which has been used widely and the authentication we are used to is when we are logging in the system especially on Linux OS where we need to enter username first to check for authority whether we can access computer and we also need to enter the password for that account. In addition there are plenty of mechanisms for authentication which is different from each other and reliable, one of them is Biometric Authentication which based on individual physical characteristic and need no password as mention before

This project focuses on applying the security using face to authenticate user on Linux instead of using password .The project mentions to process when user login using his username and administration section also theories which concern to this project

กิตติกรรมประกาศ

โครงงาน การพิสูจน์ตนด้วยชีวมาตรนี้ ได้ผ่านการศึกษา และจัดทำจนประสบผลสำเร็จได้ในที่สุดซึ่งเป็นผลเนื่องมาจาก การให้ความรู้ การให้คำปรึกษา และคำแนะนำหลาย ๆ อย่าง จาก อาจารย์อัครเดช วัชระภูพงษ์ ผศ.ธนา หงส์สุวรรณ และอาจารย์ธนัญชัย ตรีภาค อาจารย์ที่ปรึกษาโครงงานตลอดระยะเวลาในการทำโครงงาน ผู้ดำเนินโครงงาน จักขอขอบพระคุณท่านอาจารย์ทั้งสามท่านเป็นอย่างสูง

ขอขอบคุณพี่ ๆ เพื่อน ๆ และน้อง ๆ ในห้องวิจัยและพัฒนาการรักษาความปลอดภัยข้อมูล (ISAG) ที่คอยช่วยเหลือตลอดมา ขอบคุณห้องวิจัย ที่เอื้อเฟื้อทรัพยากร สถานที่และอุปกรณ์ อำนวยความสะดวก ตลอดระยะเวลาในการดำเนินโครงงาน

ขอบคุณพี่ ๆ เพื่อน ๆ และน้อง ๆ นอกห้องวิจัยและพัฒนาการรักษาความปลอดภัยข้อมูล (ISAG) ทั้งต่างคณะ ต่างสถาบันที่เป็นที่ปรึกษา ให้กำลังใจ และรับฟังปัญหาตลอดมา

บุคคลสำคัญที่ต้องขอบคุณเป็นพิเศษ คือ บิดา มารดา ที่คอยให้กำลังใจ และช่วยเหลือเสมอมาจนทำให้มีวันนี้ ท้ายที่สุดแล้วต้องขอบคุณผู้ดำเนินโครงงานเองที่มีความมานะ อุตส่าห์ จนทำให้โครงงานสำเร็จลุล่วงด้วยดี

อาทิตย์ สามารถ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

ปัจจุบันการใช้งานระบบปฏิบัติการลินุกซ์ได้รับความนิยมเพิ่มมากขึ้นอย่างกว้างขวาง ทั้งในระดับผู้ใช้งานทั่วไป หรือองค์กร และสำหรับการใช้ในงานระบบปฏิบัติการลินุกซ์นั้น โดยปกติแล้วก่อนจะสามารถเข้าใช้งานในระบบได้ จำเป็นต้องมีการตรวจสอบและยืนยันผู้เข้าใช้งานก่อน ทั้งนี้ก็เพื่อความปลอดภัยของระบบ วิธีการในการตรวจสอบและยืนยันผู้ใช้โดยปกติแล้วจะใช้ ชื่อบัญชีผู้ใช้ และรหัสผ่านเป็นสำคัญ แต่เนื่องจากความปลอดภัยของระบบถือเป็นเรื่องสำคัญมาก ฉะนั้นการใช้วิธีการป้อนข้อมูลเพียง ชื่อบัญชีผู้ใช้ และรหัสผ่าน อาจไม่เพียงพอต่อความปลอดภัยของระบบ เพราะผู้ใช้อาจลืมรหัสผ่าน ทำรหัสผ่านหาย หรืออาจมีผู้อื่นล่วงรู้รหัสผ่านนั้น และนำมาแอบอ้างเข้าใช้งานโดยที่ระบบไม่สามารถล่วงรู้ได้ ฉะนั้นวิธีการที่นำเอาระบบรักษาความปลอดภัยด้วยการใช้ใบหน้าในการตรวจสอบ และยืนยันผู้เข้าใช้งานในระบบปฏิบัติการลินุกซ์แทนการใช้รหัสผ่าน จึงเป็นอีกวิธีการที่มีความปลอดภัยมากกว่า เนื่องมาจากวิธีการดังกล่าวเป็นวิธีการที่เรียกว่า เทคโนโลยีชีวมาตร ซึ่งใช้หลักการวิธีการพิจารณาองค์ประกอบทางกายภาพของบุคคลซึ่งจะมีความเป็นเอกลักษณ์แตกต่างกันไป ดังนั้นการตรวจสอบโดยใช้ใบหน้าจะถือว่า ตำแหน่งขององค์ประกอบบนใบหน้าแต่ละคนก็มีลักษณะที่เป็นเอกลักษณ์เฉพาะตัวที่แตกต่างกันออกไป อีกทั้งยังเป็นการยากต่อการลอกเลียนแบบ และไม่สามารถทำหายได้ นอกจากนั้นแล้วก็ไม่สามารถมีผู้ใดขโมยใบหน้าไปได้ หากมองถึงงานวิจัยและเทคโนโลยีที่เกี่ยวข้องในการตรวจสอบใบหน้าของบุคคลนั้น ก็ได้รับการพัฒนาจนสามารถนำมาประยุกต์ใช้ในการทำโครงงานได้

ด้วยเหตุผลดังกล่าว จึงได้มีการนำเอาระบบรักษาความปลอดภัยด้วยใบหน้ามาใช้ในการตรวจสอบและยืนยันผู้เข้าใช้งานในระบบปฏิบัติการลินุกซ์แทนการใช้รหัสผ่าน โดยเมื่อผู้ใช้ต้องการ ล็อกอินเข้าในบัญชีผู้ใช้ของตนก็สามารถทำได้โดยการสแกนใบหน้า ถ้าการตรวจสอบถูกต้องผู้ใช้คนนี้ก็จะสามารถเข้าใช้งานระบบในบัญชีผู้ใช้ของตนได้ตามปกติ แต่ถ้ามีความผิดพลาดเกิดขึ้นก็จะไม่สามารถใช้งานได้ จะต้องทำการล็อกอินใหม่อีกครั้ง ทั้งนี้ระบบยังสามารถทำการเพิ่มผู้ใช้งาน และลบผู้ใช้งานได้อีกด้วย ในส่วนของการตรวจสอบนั้นจะทำงานร่วมกับไลบรารี PAM (Pluggable Authentication Modules) ซึ่งเป็นโมดูลในการตรวจสอบผู้ใช้งานของระบบปฏิบัติการลินุกซ์และโดยปกติแล้ว ระบบปฏิบัติการลินุกซ์จะใช้มอดูล pam_unix.so ในการดำเนินการในส่วนการพิสูจน์ตน สำหรับโครงงานนี้ได้พัฒนามอดูล pam_anubis.so เพื่อให้ระบบสามารถเรียกใช้งานเมื่อต้องการทำการพิสูจน์ตนด้วยการใช้ใบหน้าได้

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อเน้นเรื่องความปลอดภัยในการล็อกอินเข้าสู่ระบบปฏิบัติการลินุกซ์

1.2.2 เพื่ออำนวยความสะดวกแก่ผู้ใช้งานระบบปฏิบัติการลินุกซ์

1.2.3 เพื่อพัฒนาวิธีการพิสูจน์ตนทางชีวมาตร ให้ใช้งานร่วมกับระบบปฏิบัติการลินุกซ์

1.2.4 เพื่อพัฒนาเทคโนโลยีระบบรักษาความปลอดภัยในส่วนการพิสูจน์ตน

1.2.5 เพื่อเพิ่มทางเลือกในการพิสูจน์ตน รวมถึงการล็อกอินเข้าระบบปฏิบัติการลินุกซ์

1.3 ขอบเขตของโครงงาน

1.3.1 ผู้ใช้งานระบบสามารถล็อกอินเข้าสู่ระบบได้ ด้วยการป้อนชื่อบัญชีผู้ใช้ และแสดงใบหน้าแทนการป้อนรหัสผ่าน

1.3.2 ผู้ดูแลระบบสามารถเพิ่มชื่อบัญชีผู้ใช้ และลบชื่อบัญชีผู้ใช้ได้

1.3.3 กระบวนการพิสูจน์ตนใช้กระบวนการของเฟรมเวิร์ค PAM ซึ่งเป็นเฟรมเวิร์คที่ใช้ในการพิสูจน์ตนของระบบปฏิบัติการลินุกซ์

1.3.4 ระบบปฏิบัติการ Linux (Debian 3.1) / Kernel 2.6

1.3.5 ในการพัฒนาโปรแกรมพิสูจน์ตนด้วยใบหน้า ใช้ไลบรารี่ OpenCV (Opensource Computer Vision) ช่วยในการพัฒนา

1.3.6 การพิสูจน์ตนใช้ อุปกรณ์ คือ กล้องเว็บแคม Logitech QuickZoom

1.4 วิธีการดำเนินงาน

1.4.1 ศึกษาข้อมูลของ PAM (Plugable Authentication Module) ลักษณะวิธีการทำงาน การเขียนโปรแกรมที่สามารถใช้งานร่วมกับ PAM ได้

1.4.2 ศึกษาข้อมูลของการตรวจจับใบหน้าบุคคล การจำแนกใบหน้าบุคคล การเขียนโปรแกรมในการตรวจจับใบหน้าบุคคล จำแนก หรือพิสูจน์ตนได้

1.4.3 กำหนดแนวทางที่เป็นไปได้ในการทำโครงงาน ขอบเขต และรูปแบบของโครงงาน

1.4.4 ดำเนินงานตามแนวทางที่วางไว้ เขียนโปรแกรมและทดลองการทำงาน

1.4.5 สรุปผลการทดลอง และวิจารณ์

1.4.6 จัดทำปริญญานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้รับความรู้ ความเข้าใจเกี่ยวกับกระบวนการทำงานของ PAM มอดูล

1.5.2 ได้รับความรู้ ความเข้าใจเกี่ยวกับกระบวนการจดจำลักษณะใบหน้า

1.5.3 สามารถเขียนมอดูลในการพิสูจน์ตนเพื่อใช้งานร่วมกับ PAM

1.5.4 สามารถประยุกต์การพิสูจน์ตนให้มีรูปแบบแตกต่างขึ้น

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความสำคัญและที่มาของโครงงาน วัตถุประสงค์ของโครงงาน ขอบเขตของโครงงาน วิธีการดำเนินการ ประโยชน์ที่คาดว่าจะได้รับ และส่วนประกอบของปริญญานิพนธ์

บทที่ 2 กล่าวถึงทฤษฎีพื้นฐานที่ใช้ในโครงงาน ซึ่งประกอบด้วยทฤษฎีในการพิสูจน์ตน เทคโนโลยีชีวมาตร PAM(Plugable Authentication Module) ทฤษฎีในการรู้จำใบหน้า วิธีการตรวจสอบ

บทที่ 3 กล่าวถึงการออกแบบซอฟต์แวร์ที่ได้ทำขึ้น โครงสร้างซอฟต์แวร์ อุปกรณ์ที่ใช้ในการดำเนินงาน

บทที่ 4 กล่าวถึงการทดลองและผลการทดลอง

บทที่ 5 เป็นบทวิจารณ์และสรุป ซึ่งกล่าวถึงบทสรุปของโครงงาน วิจารณ์สิ่งที่ได้รับจากโครงงาน และข้อเสนอแนะสำหรับเป็นแนวทางในการพัฒนาต่อ

บทที่ 2
ทฤษฎีพื้นฐานที่ใช้ในโครงงาน

ในบทนี้จะกล่าวถึงทฤษฎีพื้นฐานต่างๆ ที่เกี่ยวข้องในการวิจัยซึ่งประกอบไปด้วยทฤษฎีพื้นฐานของระบบพิสูจน์ตน การพิสูจน์ตนบุคคล เทคโนโลยีชีวมาตร หลักการพื้นฐานของ PAM ซึ่งเป็นกระบวนการในการพิสูจน์ตนในลินุกซ์ การปรับแต่งค่าต่าง ๆ และรายเอียดในส่วนอื่นที่เกี่ยวข้อง

2.1 ระบบพิสูจน์ตน

ในปัจจุบันนี้ กระบวนการพิสูจน์ตน ถือได้ว่ามีความสำคัญ ต่อความปลอดภัยของระบบมาก กล่าวคือ หากระบบใด ๆ ที่ไม่มีการตรวจสอบการเข้าใช้งาน ของผู้ใช้งานระบบแล้ว ย่อมมีความเสี่ยงต่อความเสียหายที่อาจเกิดขึ้นกับระบบ เนื่องจากอาจมีการแอบอ้าง เป็นบุคคลอื่นเพื่อให้ได้มาซึ่งสิทธิ์ในการเข้าถึงระบบ ไม่ว่าจะด้วยจุดประสงค์อันใดก็ตาม ด้วยเหตุดังกล่าว การนำวิธีการพิสูจน์ตน ที่เหมาะสม ปลอดภัยมาประยุกต์ใช้จึงเป็นสิ่งที่ควรให้ความสำคัญ

2.1.1 ระบบรักษาความปลอดภัยบนคอมพิวเตอร์

ระบบรักษาความปลอดภัยบนคอมพิวเตอร์ คือ สิ่งที่คอยปกป้องคุ้มครองคอมพิวเตอร์และสิ่งที่เกี่ยวข้องให้พ้นอันตรายและการสูญหาย ทุกสิ่งที่เกี่ยวข้องกับคอมพิวเตอร์จะได้รับการคุ้มครองจากระบบรักษาความปลอดภัย ตามทฤษฎีระบบรักษาความปลอดภัยมีสิ่งที่ต้องคำนึงถึงดังต่อไปนี้

1. ความมั่นคงและถูกต้อง (Integrity & Accuracy) ข้อมูลที่อยู่บนคอมพิวเตอร์ต้องปลอดภัย ไม่สูญหาย ไม่เสียหาย ไม่ถูกเปลี่ยนแปลง โดยอุบัติเหตุหรือเจตนาจากผู้ที่ไม่ได้รับอนุญาต ในการส่งผ่านข้อมูลต้องมีการรับรองอย่างถูกต้อง มีบันทึกเกี่ยวกับการรับส่ง

2. ความมั่นใจ (Confidentiality) คอมพิวเตอร์ต้องเก็บรักษาความลับได้ จำแนกได้ว่าใครเป็นผู้มีสิทธิ์ และใครคือผู้ไม่มีสิทธิ์ จัดการข้อมูล

3. ความสามารถเข้าถึงข้อมูลได้(Availability) ข้อมูลที่ควรเข้าถึงได้ ต้องเข้าถึงได้ง่ายสะดวกต่อการนำมาใช้ อยู่ในที่ ที่สามารถนำมาใช้ได้ตลอดเวลา หาเกิดอุบัติเหตุขึ้นต้องสามารถกู้คืนได้

2.1.2 ส่วนประกอบของระบบความปลอดภัย

ส่วนที่ประกอบขึ้นมาเป็นระบบรักษาความปลอดภัยมีด้วยกัน 3 ข้อ

1. การออกแบบระบบ การออกแบบระบบที่ดีทำให้สามารถรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ การใช้สถาปัตยกรรมเข้ามาจัดการระบบเป็นตัวอย่างหนึ่งของการออกแบบระบบที่ดี ทำให้สามารถจัดแบ่งหน่วยความจำ และแยกอภิสิทธิ์ออกจากสิทธิ์ทั่วไปได้

2. การควบคุมการจัดข้อมูล การควบคุมข้อมูลหมายถึง การกำหนดว่าให้ใครสามารถจัดการข้อมูลได้บ้าง และต้องกำหนดด้วยว่าจัดการข้อมูลไปเพื่อจุดประสงค์ใด

3. การควบคุมการจัดการในระบบ การควบคุมการจัดการในระบบทำให้สามารถกำหนดได้ว่าใครมีสิทธิ์ใช้ข้อมูลได้ถึงระดับไหน นอกจากนี้ยังทำให้แน่ใจด้วยผู้ที่ไม่ได้รับอนุญาต จะไม่มีสิทธิ์จัดการข้อมูล

2.1.3 การควบคุมการจัดการ

เป้าหมายหลักของการรักษาความปลอดภัยอยู่ที่ต้องสามารถจำกัดได้ว่าให้ใครเข้าถึงข้อมูลได้มากขนาดไหนซึ่งเรียกว่าการควบคุมการจัดการ (access control) เหตุผลที่ต้องควบคุมจัดการคือ

1. เพื่อสนับสนุนให้การเข้าถึงข้อมูลของผู้ที่ได้รับอนุญาตเป็นไปอย่างถูกต้องและง่ายดาย
2. เพื่อส่งเสริมให้เกิดความมั่นคงของข้อมูล
3. เพื่อปกป้องความเป็นส่วนตัวในข้อมูลส่วนบุคคล

นอกจากนี้แล้ว การควบคุมการจัดการยังมีขอบเขตไปถึงการจำกัดการใช้โปรแกรมต่าง ๆ เพื่อลบ เขียนทับ และทำสำเนาด้วย ในการควบคุมการจัดการเราต้องคำนึงถึงสิ่งต่อไปนี้

1. ใครที่สามารถใช้ได้บ้าง (Authentication)
2. ผู้ที่ได้รับอนุญาต มีสิทธิ์ใช้ส่วนใดและระดับใดได้บ้าง (Authorization)
3. ต้องบันทึกการกระทำต่าง ๆ ของผู้ที่ได้รับอนุญาต (Accounting)

เมื่อผู้ใช้ต้องการใช้บริการจากระบบ ผู้ใช้ต้องระบบว่าเป็นใคร และระบบจะตรวจสอบว่าผู้ใช้เป็นคนนั้นจริงหรือไม่ ทั้งสองขั้นตอนนี้เรียกว่าการแสดงตน (Identification) และการพิสูจน์ตน (Authentication)

2.1.4 การพิสูจน์ตนบุคคล

การพิสูจน์ตนบุคคล คือ การที่ระบบตรวจสอบว่าผู้ใช้เป็นคนเดียวกับบุคคลที่อ้างหรือไม่ และสำหรับการพิสูจน์ตนบุคคลนั้นค่อนข้างจะแตกต่างกันในด้านวิธีการทั้งนี้ขึ้นกับความสามารถของสิ่งที่ทำการพิสูจน์ตน ความสามารถที่สำคัญ 2 สิ่ง คือ ความสามารถในการเก็บกุญแจรหัส

ลับคุณภาพสูง และ ความสามารถในการดำเนินการกับรหัสลับ สำหรับคอมพิวเตอร์จะมีความสามารถทั้ง 2 อย่างที่กล่าวมา ในขณะที่มนุษย์ไม่มี มนุษย์ไม่มีความสามารถในการเก็บกุญแจรหัสลับคุณภาพสูงไว้อย่างปลอดภัย อีกทั้งความรวดเร็วและความแม่นยำเมื่อดำเนินการกับรหัสลับ ก็ไม่เป็นที่ยอมรับในความสามารถ

ลักษณะในการตรวจสอบมี 3 ลักษณะ

2.1.4.1 สิ่งที่คุณรู้ (what you know)

จะใช้วิธีการในการพิสูจน์ โดยผู้ใช้ต้องรู้ในสิ่งระบบต้องการรู้เพื่อใช้ตรวจสอบโดยปกติแล้วคือ รหัสผ่าน ซึ่งหมายความว่าหากผู้ใช้ทราบรหัสผ่านแล้วก็ถือว่าเป็นผู้ใช้ตัวจริง ซึ่งรหัสผ่านนั้น เช่น ตัวเลข หรือข้อความ วิธีนี้ถือว่าเป็นวิธีที่ค่อนข้างมีการใช้งานกันอย่างแพร่หลาย เนื่องจากสามารถใช้งานง่าย แต่กระนั้นวิธีนี้ก็ยังเป็นวิธีการที่มีความปลอดภัยไม่สูงมาก เนื่องจากหากมีการขโมยรหัสผ่าน หรือมีผู้อื่นล่วงรู้รหัสผ่าน ซึ่งสามารถทำได้ไม่ยาก ก็สามารถเข้าใช้งานระบบได้

แนวคิดของวิธีการนี้ คือ เมื่อมีความต้องการพิสูจน์ว่านาย ก เป็นนาย ก จริงโดยไม่สามารถพิจารณาได้จากรูปลักษณ์ที่เห็น สามารถตกลงกันไว้ก่อนได้ โดยหากใครสามารถบอกคำดังกล่าวได้ ก็หมายความว่าผู้นั้นคือ นาย ก รูปแบบรหัสผ่านนี้ใช้กันในวงการทหาร กล่าวคือ ทุกคนในกลุ่มจะได้รับรหัสผ่านในแต่ละวัน หากกลับมาถึงหลังจากดวงอาทิตย์ตกแล้วจะต้องบอกรหัสผ่านเพื่อพิสูจน์ว่าไม่ใช่ศัตรู หรือในระบบคอมพิวเตอร์เมื่อพิมพ์ชื่อบัญชีผู้ใช้แล้วก็จะ ต้องใส่รหัสผ่านเพื่อพิสูจน์ว่าเป็นผู้ใช้คนนั้นจริง เป็นต้น

อย่างไรก็ดีโดยส่วนใหญ่แล้ว ผู้ใช้ส่วนใหญ่ที่ล็อกอินเข้าระบบโดยพิมพ์ชื่อบัญชีผู้ใช้และรหัสผ่านอยู่บ่อยครั้งนั้น อาจไม่ได้คิดถึงปัญหาของการใช้รหัสผ่านสำหรับการพิสูจน์ดนซึ่งมีมาก

- อาจมีผู้อื่นเห็นรหัสผ่านขณะที่ทำการพิมพ์เพื่อล็อกอิน
- อาจมีการอ่านข้อมูลจากไฟล์ซึ่งคอมพิวเตอร์ใช้เก็บข้อมูลของรหัสผ่าน
- รหัสผ่านที่ใช้อาจง่ายต่อการเดา
- มีการบังคับให้ใช้รหัสผ่านที่เดายาก จนอาจทำให้ให้ระบบไม่สะดวกหรืออาจใช้งานไม่ได้ หรืออาจมีการเขียนรหัสผ่านไว้

2.1.4.2 สิ่งที่คุณมี (what you have)

ใช้วิธีการในการพิสูจน์ โดยผู้ใช้ต้องมีในสิ่งที่ระบบต้องการให้แสดงเพื่อการตรวจสอบ เช่น บัตรสมาร์ทการ์ด บัตรที่มีแถบแม่เหล็ก หรือกุญแจ ซึ่งแม้ว่าจะเป็นวิธีการที่ใช้เทคโนโลยีสูงกว่าแบบแรก แต่ก็มีปัญหาได้ หากสิ่งดังกล่าวถูกขโมย หรือแม้กระทั่งมีการทำการคัดลอกซึ่งอาจจะยากกว่าแบบรหัสผ่าน จำเป็นต้องใช้เทคโนโลยีบางแขนงเข้ามาช่วยแต่ก็สามารถทำได้

วิธีการนี้เป็นวิธีการที่ใช้อุปกรณ์ซึ่งผู้ใช้สามารถถือ หรือพกพาได้และใช้ในการพิสูจน์ตน โดยทั่วไปแล้ววิธีการนี้มีทั้งข้อได้เปรียบและข้อเสียเปรียบ นอกจากนั้นแล้วยังต้องใช้ร่วมกับวิธีการอื่น หนึ่งในสองวิธีที่เหลือเพื่อให้มีความปลอดภัยเพิ่มมากยิ่งขึ้น

วิธีการนี้มีหลายรูปแบบที่ใช้กันอยู่ในปัจจุบัน และที่นิยมใช้กันมากที่สุดคือ กุญแจ ซึ่งใช้ในการปลดล็อค ประตูบ้าน หรือ ประตูรถยนต์ สำหรับรูปแบบอื่นนั้นเช่น บัตรเครดิต ซึ่งหากบัตรเครดิตดังกล่าว มีรูปและลายเซ็นด้วยแล้ว ก็ถือเป็นการรวมวิธีการทางชีวมาตรแบบปฐมภูมิ ซึ่งสามารถเปรียบเทียบลายเซ็น หรือตรวจสอบได้ว่าเหมือนกับรูปบนบัตรหรือไม่

ปัจจุบันนี้บัตรเครดิตจะมีแถบแม่เหล็กซึ่งเก็บข้อมูล ข้อได้เปรียบที่ได้จากแถบแม่เหล็กนอกเหนือจาก รูปแบบที่เป็นรหัสผ่านธรรมดา นั่นคือ ไม่สามารถผลิตซ้ำได้และยังสามารถเก็บข้อมูลลับซึ่งมีปริมาณเยอะกว่าที่คนธรรมดาทั่วไปจะสามารถจดจำได้ แต่ใช่ว่าจะมีข้อดีเพียงอย่างเดียว วิธีการนี้ยังมีข้อเสีย เช่น

- ต้องการอุปกรณ์ที่สนับสนุน เช่น ช่องเสียบกุญแจ หรือตัวอ่านบัตร ที่จะต้องมีอุปกรณ์ดังกล่าวอยู่ทุกที่ ที่จะให้บริการ ซึ่งนั่นก็หมายความว่า ค่าใช้จ่ายที่สูงขึ้นและมาตรฐานที่จำเป็นต้องเป็นไปในแนวทางเดียวกันหรือว่ามีมาตรฐานเดียวกัน
- วิธีนี้เสี่ยงต่อการสูญหาย หรือถูกขโมย สำหรับเหตุผลทางด้านความปลอดภัยแล้วยังต้องมีการเสริมด้วย พิน หรือ รหัสผ่าน

อย่างไรก็ตาม อุปกรณ์เหล่านี้ก็ไม่สามารถป้องกันการขโมยข้อมูลในการสื่อสารมากนัก เมื่อไหร่ที่ข้อมูลถูกส่งออกไป ก็สามารถที่จะถูกดักจับ และนำไปใช้ภายหลังได้ ซึ่งหากมีการขโมยข้อมูลเกิดขึ้นแล้ว ผู้ขโมยสามารถติดต่อกับเครือข่ายผ่านทางช่องทางที่ไม่ใช่ช่องทางปกติทั่วไป แล้วนำข้อมูลที่ขโมยได้กลับมาใช้งานอีกครั้งโดยไม่จำเป็นต้องสร้างบัตรขึ้นใหม่

แต่เทคโนโลยีที่พัฒนาขึ้นก็ช่วยพัฒนาให้มีรูปแบบที่ดีขึ้น นั่นคือ บัตรสมาร์ทการ์ด อุปกรณ์รูปแบบนี้ก็มีขนาดเช่นเดียวกับบัตรเครดิต แต่จะมีการฝังหน่วยประมวลผลและหน่วยความจำลงไป เมื่อสอดบัตรเข้าไปในตัวอ่านบัตร ก็จะมีการสื่อสารกันระหว่างบัตรกับตัวอ่าน ซึ่งจะตรงข้ามกับแบบแถบแม่เหล็ก ที่จะเก็บข้อมูลโดยตรง

รูปแบบของบัตรสมาร์ทการ์ด

1. PIN protected memory card

บัตรประเภทนี้ มีข้อมูลเก็บในหน่วยความจำของบัตรซึ่งจะถูกอ่านได้หลังจากใส่พินไปแล้ว และโดยปกติแล้วเมื่อใส่พินผิดพลาดเป็นจำนวนครั้งที่กำหนด บัตรจะล็อกตัวเองและจะไม่ให้ข้อมูลกับใครเลย ข้อมูลที่เก็บบนบัตรสมาร์ทการ์ดจะปลอดภัยมากกว่าเก็บบนแถบแม่เหล็ก เนื่องจากบัตรสมาร์ทการ์ดที่ถูกขโมยไปโดยไม่มีพินก็จะใช้ประโยชน์อะไรไม่ได้ นอกจากนี้แล้วบัตรประเภทนี้ยังคัดลอก ปลอมแปลงยากกว่าแบบแถบแม่เหล็กแต่ก็ยังทำได้หากมีพิน

2. Cryptographic challenge/response cards

บัตรประเภทนี้จะมีกุญแจลับในหน่วยความจำ และจะมีการเข้ารหัสและถอดรหัสโดยใช้กุญแจ แต่จะไม่เปิดเผยกุญแจแม้หลังจากการใส่พินแล้วก็ตาม บัตรประเภทนี้ได้รับการออกแบบมาให้ยากต่อการคัดลอก จนเกือบจะทำการคัดลอกไม่ได้เลย หรือแม้กระทั่งดึงค่ากุญแจออกมา

3. Cryptographic calculator

มีลักษณะคล้ายกับบัตรสมาร์ทการ์ดตรงที่มีการคำนวณการเข้ารหัสด้วยการใช้กุญแจ ซึ่งจะไม่มีการเปิดเผย แต่ก็ไม่เหมือนกับบัตรสมาร์ทการ์ดที่ ไม่ต้องการการเชื่อมต่อใดๆ ทางอิเล็กทรอนิกส์ กับเทอร์มินอล ข้อได้เปรียบที่เด่นชัดที่สุดของบัตรประเภทนี้คือสามารถใช้งานได้จากเทอร์มินอลปกติทั่วไปโดยไม่มีอุปกรณ์พิเศษเพิ่มเติมใด ๆ ซึ่งได้รับความนิยมภายในกลุ่มบริษัทที่ต้องการให้พนักงานล็อกอินจากบ้านโดยใช้ แลบท็อป และโมเด็ม

2.1.4.3 สิ่งที่คุณเป็น (what you are)

ใช้วิธีการในการพิสูจน์ โดยผู้ใช้ต้องแสดงในสิ่งซึ่งเป็นลักษณะทางกายภายของผู้ใช้ ซึ่งนั่นคือวิธีการทางชีวมาตร (Biometrics)

2.1.5 การพิสูจน์ตนด้วยชีวมาตร

เทคโนโลยีชีวมาตรกำลังกลายเป็นพื้นฐานของการระบุตัวตนและแนวทางการยืนยันบุคคล เนื่องด้วยระดับของความปลอดภัยได้แตกแยกออกมากมาย และการขโมยธุรกรรมต่าง ๆ ก็เพิ่มขึ้นจึงทำให้เกิดความต้องการในเทคโนโลยีการระบุตัวตนและการยืนยันตัวบุคคล แนวทางชีวมาตรสามารถสร้างความมั่นใจในการทำธุรกรรมด้านการเงินรวมถึงข้อมูลส่วนบุคคลได้

เนื่องด้วยการใช้ รหัสผ่าน หรือพิน ขยายตัวเพิ่มปริมาณการใช้อย่างรวดเร็ว ตามการพัฒนาของระบบข้อมูลสารสนเทศ ซึ่งนับว่าการจำกัดสิทธิในการเข้าถึงข้อมูลที่สำคัญ หรือข้อมูลที่เป็นส่วนตัวเป็นสิ่งสำคัญ ดังนั้นการใช้งานพิน และ รหัสผ่านนั้นอาจถูกแทนที่ด้วยวิธีการอื่นได้ ซึ่งวิธีการทางชีวมาตรนั้นมีการใช้งานที่สะดวกมากกว่าสำหรับผู้ใช้งาน สามารถที่จะป้องกันการเข้าถึงส่วนที่ไม่มีสิทธิ์ หรือการใช้งานที่ผิดวัตถุประสงค์ดังตัวอย่างของเอทีเอ็ม รวมทั้ง โทรศัพท์ระบบเซลลูล่า สมาร์ทการ์ด คอมพิวเตอร์ส่วนบุคคล เครือข่ายคอมพิวเตอร์

เทคโนโลยีชีวมาตร เป็นวิธีการในการจดจำบุคคล โดยดูจากลักษณะทางกายภาพหรือลักษณะ พฤติกรรมโดยวัดจาก ใบหน้า ลายนิ้วมือ รูปทรงของมือ ลายมือ ม่านตา ฉากรับภาพหลังม่านตา เส้นโลหิตดำ และเสียง รวมไปถึงลายเซ็น

วิธีการของการบ่งชี้ ระบุตัวบุคคลหรือพิสูจน์ตนด้วยชีวมาตรนั้นได้รับความนิยมมากกว่าวิธีการโดยปกติทั่วไปซึ่งรวมถึง รหัสผ่าน และการใช้หมายเลขพินด้วย เนื่องด้วยเหตุผลที่ว่าการ

บ่งชี้ ระบุใครนั้นบุคคลนั้นจำเป็นที่จะต้องมีเพียงแค่ส่วนของร่างกาย เพื่อแสดงจุดที่จะทำการระบุหรือพิสูจน์ตน และเหตุผลอีกประการนั่นคือ วิธีการระบุตัวบุคคลด้วยชีวมาตรหรือวิธีการพิสูจน์ตนด้วยชีวมาตร นั้น สามารถหลีกเลี่ยงความจำเป็นที่จะต้องทำการจำรหัสผ่าน หรือพกพาสัญลักษณ์ เช่น สมาร์ทการ์ด

เทคโนโลยีชีวมาตรได้รับการนำไปใช้งานในหลายส่วน ทั้งองค์กรรัฐบาล ทหาร หรือทางด้านพาณิชย์ ดังปรากฏในงานด้านต่าง ๆ ทั้งโครงสร้างพื้นฐานความปลอดภัยด้านเครือข่าย บัตรประจำตัวทางราชการ ระบบธนาคารแบบอิเล็กทรอนิกส์ ธุรกรรมด้านการเงินการลงทุน ธุรกิจค้าปลีก การบังคับใช้ทางกฎหมาย บริการสุขภาพและสังคม ล้วนได้รับประโยชน์จากเทคโนโลยีชีวมาตรทั้งสิ้น

แอพลิเคชันที่มีระบบพิสูจน์ตนแบบชีวมาตร รวมทั้ง คอมพิวเตอร์ประสิทธิภาพสูง เครือข่าย การล็อกอินแอพลิเคชัน การป้องกันข้อมูล การเข้าถึงระยะไกล ความปลอดภัยของธุรกรรม และความปลอดภัยของเว็บ ความน่าเชื่อถือของ ธุรกรรมอิเล็กทรอนิกส์เป็นสิ่งจำเป็นต่อการเติบโตของเศรษฐกิจโลก การนำวิธีการทางชีวมาตรมาใช้เพียงลำพัง หรือประยุกต์รวมกับเทคโนโลยีรูปแบบอื่น เช่น บัตรสมาร์ทการ์ด กุญแจเข้ารหัส และลายเซ็นดิจิตอล นั้นก็ได้รับการนำไปใช้อย่างแพร่หลายเกือบทุกด้านในทางเศรษฐกิจ และชีวิตประจำวัน การนำชีวมาตรไปใช้ในการพิสูจน์ตน กำลังกลายเป็นสิ่งที่มีความสะดวกอีกทั้งยังมีความถูกต้องแม่นยำมากกว่าวิธีการในปัจจุบัน (ตัวอย่างเช่น รหัสผ่าน หรือพิน) เนื่องจากชีวมาตรเชื่อมหลักฐานกับตัวบุคคลเข้าด้วยกัน (ในกรณีที่เป็นรหัสผ่าน หรือสิ่งที่ถือครองไว้ อาจมีการนำไปใช้งานโดยบุคคลอื่นที่ไม่มีสิทธิ์) หากมองในมุมของความสะดวกแล้วชีวมาตรไม่จำเป็นต้องพกพาหรือจดจำ หรือแม้ในส่วนของความแม่นยำแล้ว ชีวมาตรก็นับได้ว่ามีความถูกต้องอยู่ในเกณฑ์บวก

2.1.6 รูปแบบของวิธีการทางชีวมาตร

โดยทั่วไปแล้วระบบชีวมาตร เป็นระบบรู้จำรูปแบบซึ่งทำให้เกิดลักษณะที่แตกต่างกันสำหรับแต่ละบุคคล โดยดูจากลักษณะเฉพาะทางกายภาพ หรือลักษณะพฤติกรรมที่เกิดจากบุคคล แต่ปัจจัยสำคัญในการออกแบบระบบที่สามารถนำไปใช้งานได้จริง คือทำอย่างไรให้ลักษณะแต่ละบุคคลถูกระบุได้ บ่งชี้ได้ พิสูจน์ได้ ทั้งนี้ทั้งนั้นขึ้นกับสภาวะแวดล้อม กล่าวคือ ระบบชีวมาตรจะเป็นระบบพิสูจน์ตนหรือไม่ก็เป็นระบบแสดงตน

ตัวอย่างของวิธีการทางชีวมาตร

ลายนิ้วมือ ใช้วิธีตรวจสอบลายเส้นของนิ้วมือ โดยลายนิ้วมือจะประกอบด้วยเส้นลายนิ้วมือ และช่องระหว่างเส้นลายนิ้วมือ ซึ่งแต่ละคนจะมีลักษณะรูปแบบของลายนิ้วมือที่แตกต่างกัน วิธีนี้มีการนำไปใช้งานกันมาเป็นเวลานานมาก ระดับความผิดพลาดอยู่ในระดับต่ำเนื่องจากมีความแม่นยำ ค่อนข้างสูง และค่าใช้จ่ายเมื่อเทียบกับรูปแบบอื่น ๆ แล้วยังถือว่าไม่สูง

ใบหน้า เป็นวิธีการซึ่งพิจารณารูปลักษณ์ใบหน้าของบุคคล วิธีนี้คอมพิวเตอร์สามารถวัดขนาดของใบหน้า และยังมีความสามารถในการจดจำใบหน้าบุคคลได้เป็นอย่างดี

จอตา เป็นวิธีที่มีการตรวจสอบเส้นเลือดบริเวณด้านหลังของดวงตา โดยมีการใช้แสงที่มีความเข้มต่ำ ในการตรวจจับลักษณะของจอตา ซึ่งลักษณะที่ได้มานั้นจะมีความเป็นเอกภาพสำหรับแต่ละบุคคลเช่นเดียวกับลายนิ้วมือ และการใช้วิธีนี้มีความแม่นยำสูง โดยผู้ใช้ไม่จำเป็นต้องมอง หรือจ้องไปที่จุดที่กำหนด แต่โดยปกติผู้ใช้จะต้องถอดแว่นตาออกเท่านั้น ระดับความผิดพลาดอยู่ในระดับต่ำมาก แต่วิธีการนี้จำเป็นต้องใช้อุปกรณ์ซึ่งมีราคาแพง

ม่านตา เป็นวิธีการซึ่งคล้ายกับการใช้ จอตาจะทำการตรวจสอบลักษณะของม่านตาบริเวณวงแหวนสีซึ่งล้อมรอบรูม่านตา ซึ่งจำเป็นต้องใช้กล้องที่มีคุณภาพ วิธีนี้จะมีส่วนติดต่อผู้ใช้ที่นับได้ว่าเป็นจุดเด่น คืออุปกรณ์สแกนม่านตาสามารถทำการสแกนม่านตาได้แม้ระยะห่างระหว่างดวงตากับกล้องจะห่างกันพอสมควร แต่ผู้ใช้ก้อจำเป็นต้องถอดแว่นตาออกด้วย วิธีนี้มีระดับความผิดพลาดต่ำมากเช่นกัน แต่ค่าใช้จ่ายก็อยู่ในระดับสูงด้วย

ลายมือ เป็นวิธีที่มีการใช้งานกันอย่างกว้างขวางมากกว่าวิธีการตรวจสอบลายนิ้วมือเพียงอย่างเดียวเนื่องจากวิธีนี้จะวัดขนาดของมือ ความยาวนิ้ว ความกว้าง วิธีนี้อาจเหมาะกับที่ซึ่งมีจำนวนผู้ใช้มาก ๆ หรือผู้ใช้มีการใช้งานไม่บ่อย นอกจากนั้น ระดับของความถูกต้องก็อยู่ในระดับสูงหากต้องการ ทั้งยังยืดหยุ่นในการปรับแต่งประสิทธิภาพและเหมาะกับหลาย ๆ แอพลิเคชันหากจะนำไปใช้งานร่วม ทั้งยังมีราคาถูกกว่าอุปกรณ์ของการตรวจสอบลายนิ้วมืออีกด้วย

เสียง เป็นวิธีที่จะใช้การพิจารณาลักษณะของสเปคตรัมความถี่ของเสียงของคน จังหวะในการพูด ระดับเสียง วิธีนี้จำเป็นต้องใช้ ไมโครโฟน และแม้ว่าประสิทธิภาพจะเพิ่มขึ้นตามคุณภาพของอุปกรณ์รับเสียง และ ราคาของอุปกรณ์ก็ไม่สูง แต่วิธีนี้อาจมีปัญหาได้เช่นกัน กล่าวคือหากในการพิสูจน์ตนผู้ที่ทำการพิสูจน์ตนเป็นหวัดก็ส่งผลต่อเสียงได้หรือแม้กระทั่งการเลียนเสียง ซึ่งโดย ทั่วไปแล้วมักนิยมใช้ประกอบกับวิธีการอื่น ๆ เช่น วิธีการตรวจสอบลายมือ นอกจากนั้นแล้ววิธีนี้ยังมี ระดับความผิดพลาดสูงจึงไม่นิยมใช้ในการระบุตัวบุคคลเช่นกัน

จังหวะการพิมพ์ เป็นวิธีที่ใช้จังหวะการพิมพ์ของแต่ละบุคคลซึ่งมีลักษะที่แตกต่างกันอย่างชัดเจน เช่น ระยะเวลาที่ใช้ระหว่างการกดตัวอักขระ รูปแบบของความถี่ในการปุ่มอักขระเป็นต้น

ลายเซ็น เป็นวิธีการที่ใช้ตรวจสอบจากการเซ็นของบุคคลซึ่งยากที่จะลอกเลียนแบบให้มีระยะเวลา จังหวะการเคลื่อนไหว แรงกดที่เหมือนกันได้ ในบางระบบได้นำวิธีการนี้ไปใช้โดยให้ผู้ใช้งานทำการเซ็นชื่อบนอุปกรณ์อิเล็คทรอนิคส์ วิธีนี้โดยปกติแล้วจะใช้ในการยืนยันตัวบุคคล ไม่ใช้สำหรับการระบุตัวบุคคลเนื่องจากระดับความผิดพลาดค่อนข้างสูง

Identification and Verification

ในบางครั้ง Identification และ Verification ถูกใช้ในความหมายที่ไม่ต่างกัน แต่ในความเป็นจริงแล้วทั้ง สองคำนี้กลับมีความหมายที่ต่างกัน

Identifation หมายความถึง การระบุตัวบุคคลด้วยการแสดงลักษณะทางชีวมาตร ของบุคคลนั้น ซึ่งวิธีการนี้จะมีการค้นหารูปแบบตัวอย่างจากฐานข้อมูลและจับคู่กับตัวอย่างชีวมาตรจนกระทั่งได้รูปแบบที่มีความคล้ายคลึงกันมากที่สุด ซึ่งวิธีการนี้รู้จักในลักษณะของ "1:N" หรือ "one-to-many"

Verification หมายความถึง การตรวจสอบว่า ผู้ใช้งานเป็นผู้ใช้งานคนเดียวกับที่ตัวเขาอ้างถึงหรือไม่ โดยลักษณะชีวมาตรที่ผู้ใช้งานแสดงนั้น จะถูกนำมาตรวจสอบกับลักษณะชีวมาตรที่ถูกเก็บไว้เป็นข้อมูลอ้างอิงไม่ว่าจะเป็นบนบัตรสมาร์ทการ์ดหรือในฐานข้อมูล

เห็นได้ว่า Verification เป็นวิธีการที่ตรงข้ามกับ Identification กล่าวคือ วิธีการ verification นั้นมีเพียงลักษณะของชีวมาตรเพียงลักษณะเดียวที่ถูกนำมาเปรียบเทียบในขณะที่ identification นั้นจะใช้การเปรียบเทียบกับหลาย ๆ รูปแบบในลักษณะ one-to-many ดังที่ได้กล่าวมาแล้ว

2.2 Pluggable Authentication Modules (PAM)

เป็นเฟรมเวิร์คซึ่งได้รับการออกแบบมาในลักษณะที่เรียกว่า ปลั๊กอิน เพื่อให้แอพลิเคชั่นอื่น ๆ เช่น login ftp หรือ telnet สามารถเรียกใช้งานได้ โดยไม่ต้องเปลี่ยนแปลงคำสั่ง หรือแก้ไข ส่วนโค้ดของโปรแกรม PAM ให้บริการแอพลิเคชั่นในระบบด้วยกระบวนการพิสูจน์ตนและบริการด้านความปลอดภัยอื่นที่เกี่ยวข้อง เช่น DCE หรือ Kerboros นอกจากกระบวนการ หรือกลไกในส่วนของการพิสูจน์ตนแล้ว กลไกในการจัดการบัญชีรายชื่อ การจัดการเซสชัน และการจัดการรหัสผ่านก็มีในเฟรมเวิร์คนี้ด้วย

PAM เฟรมเวิร์ค ช่วยให้ผู้ดูแลระบบเองสามารถเลือกวิธีการ กระบวนการหรือ กลไกต่างๆ เพื่อใช้ในการพิสูจน์ตนซึ่งการใช้ PAM มีข้อดีคือ

การปรับแต่งค่าที่ยืดหยุ่น

- การพิสูจน์ตนสำหรับแต่ละแอพลิเคชั่น
  สามารถเลือกกลไกพื้นฐานสำหรับการพิสูจน์ตนที่ไม่ได้ระบุเจาะจงไว้
  รหัสผ่านหลายรหัสสำหรับระบบที่มีความปลอดภัยสูง
- ง่ายสำหรับผู้ใช้ทั่วไป
  ไม่ต้องพิมพ์รหัสผ่านหลายครั้งหากเหมือนกัน
  ใช้รหัสผ่านเดียว แม้ว่ารหัสผ่านนั้นจะใช้ในกลไกการพิสูจน์ตนที่แตกต่างกันโดยผ่านการเปรียบเทียบรหัสผ่าน

PAM แบ่งออกได้เป็น 4 รูปแบบการใช้งานที่แตกต่างกันคือ การพิสูจน์ตน การจัดการบัญชีผู้ใช้ การจัดการเซสชัน การจัดการรหัสผ่าน

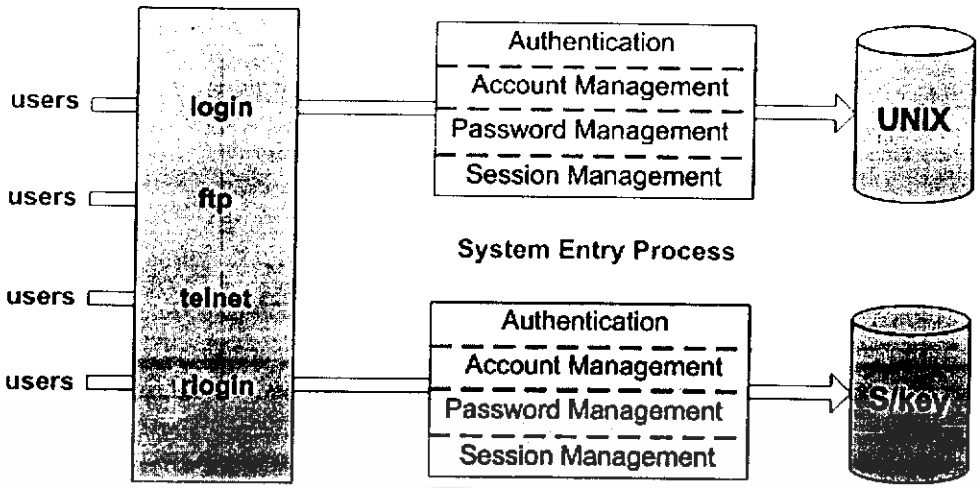
ซึ่งมอดูลในการพิสูจน์ตนนั้นจะทำการพิสูจน์ตนผู้ใช้และมีการรับรองการใช้งานของผู้ใช้ตั้งแต่การเริ่มการรับรองหรือสิ้นสุดการรับรอง

มอดูลสำหรับบัญชีผู้ใช้ จะตรวจสอบอายุของรหัสผ่าน การหมดอายุการใช้งานของบัญชีและการกำหนดช่วงเวลา เมื่อผู้ใช้ทำการแสดงตนด้วยการใช้งานมอดูลพิสูจน์ตนแล้ว มอดูลบัญชีผู้ใช้จะทำการตัดสินใจว่าจะอนุญาตให้ผู้ใช้ได้รับสิทธิ์เข้ามาใช้งานหรือไม่

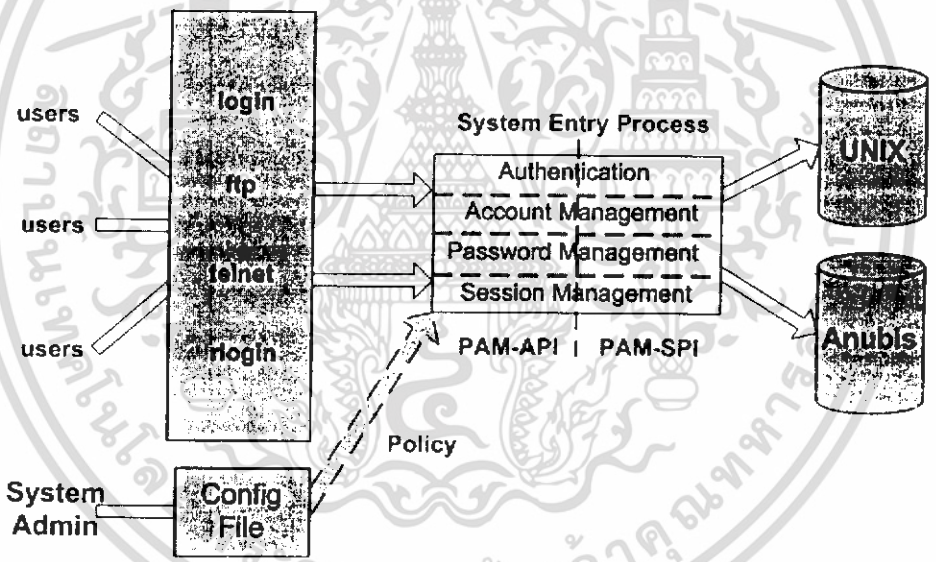
มอดูลเซสชัน จะจัดการในส่วนของการเปิดเซสชัน และปิดเซสชันเป็นหลัก

มอดูลรหัสผ่าน จะมีการอนุญาตให้มีการเปลี่ยนรหัสผ่านและค่าต่างๆ ที่เกี่ยวข้อง

แอพลิเคชันต่าง ๆ ทั้ง ftp telnet หรือ login จะใช้ PAM ไลบรารี่ เพื่อใช้งานมอดูลที่เกี่ยวข้องโดยเมื่อมีการเรียกใช้ PAM ไลบรารี่ แล้ว PAM ไลบรารี่ จะดูค่าการปรับแต่งซึ่งมีการระบุไว้ที่ /etc/pam.conf หรือในไดเร็กทอรี่ /etc/pam.d/ ซึ่งไฟล์ดังกล่าวนี้จะทำหน้าที่บอกว่ามอดูลใดจะถูกใช้งานโดย แอพลิเคชั่นหนึ่ง ๆ และมอดูลจะตอบสนองต่อการเรียกใช้งานของแอพลิเคชั่นผ่าน PAM ไลบรารี่



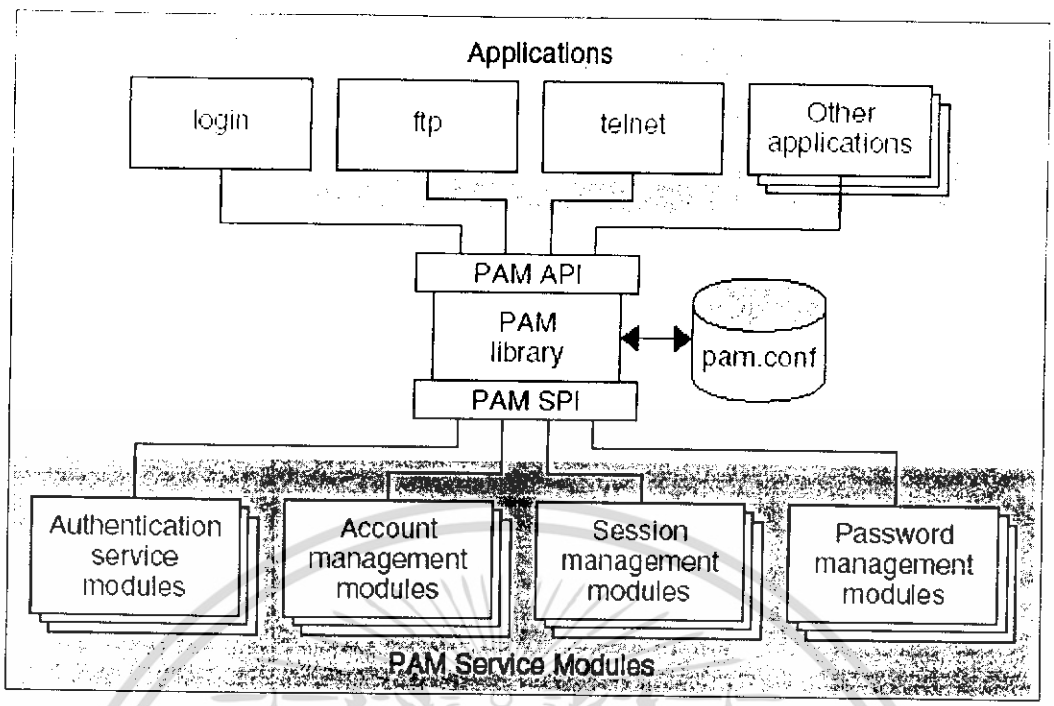
รูปที่ 2.1 การพิสูจน์ตนรูปแบบเดิม



รูปที่ 2.2 การพิสูจน์ตนแบบใช้ PAM

2.2.1 PAM เฟรมเวิร์ค

PAM เฟรมเวิร์คเป็นเสมือนแบบแผน หรือแนวทางสำหรับกระบวนการที่เกี่ยวการพิสูจน์ตน แนวทางดังกล่าวส่งผลให้ ผู้พัฒนาแอพลิเคชั่นสามารถใช้บริการ PAM ได้โดยไม่จำเป็นต้องทราบถึงแนวทางหรือ วิธีการหรือกฎเกณฑ์



รูปที่ 2.3 แสดงความสัมพันธ์ ของ PAM เฟรมเวิร์ค

ภาพที่ 2.3 แสดงความสัมพันธ์ของการทำงานของ PAM แอพลิเคชั่นที่มีการเรียกใช้และรวมถึงไลบรารี่ที่เกี่ยวข้อง กล่าวคือ แอพลิเคชั่นติดต่อกับ PAM ไลบรารี่ ผ่าน PAM แอพลิเคชั่นโปรแกรมมิ่งอินเทอร์เฟส (application programming interface - API) ในขณะที่ PAM มอดูล ติดต่อกับ PAM ไลบรารี่ ผ่าน PAM เซอร์วิสโพรไวเดอร์อินเทอร์เฟส (service provider interface - SPI) แสดงให้เห็นว่า PAM ไลบรารี่ อนุญาตให้แอพลิเคชั่น และมอดูลสามารถติดต่อซึ่งกันและกันได้

แนวทางในการพิสูจน์ตนนั้นสามารถดัดแปลงแก้ไขได้อย่างเป็นอิสระจาก แอพลิเคชั่น และด้วยการทำงานของ PAM ส่งผลให้ผู้ดูแลระบบสามารถเพิ่มส่วนของการพิสูจน์ตนที่ต้องการกับระบบโดยไม่ต้องเปลี่ยนแปลงแอพลิเคชั่นใด ๆ การปรับเปลี่ยนสามารถทำได้โดยแก้ไขไฟล์ปรับแต่งค่า

PAM เฟรมเวิร์คประกอบด้วย 4 ส่วน คือ

- PAM แอพลิเคชั่น (PAM application)
- PAM ไลบรารี่ (PAM library)
- PAM เซอร์วิสมอดูล (PAM sevice modules)
- PAM คอนฟิกกูเรชันไฟล์ (PAM configuration file)

2.2.2 PAM แอพลิเคชั่น (PAM application)

แอพลิเคชั่นซึ่งใช้ PAM ต้องมีการอ้างถึงไลบรารี่ libpam และก่อนที่แอพลิเคชั่นใด ๆ จะใช้บริการซึ่งมีให้โดยโมดูลแล้ว จำเป็นต้องเรียกฟังก์ชั่น pam_start() เพื่อสร้างตัวถือครอง (handle) ในการส่งผ่าน การเรียกใช้ PAM ทุกกรณี และเมื่อแอพลิเคชั่นเสร็จสิ้นแล้วต้องเรียกฟังก์ชั่น pam_end() เพื่อทำการลบข้อมูลต่าง ๆ ที่มีการเรียกใช้โดย PAM ไลบรารี่

2.2.3 PAM ไลบรารี่ (PAM library)

PAM ไลบรารี่ เก็บอยู่ใน /usr/lib/libpam ถือเป็นศูนย์กลางในโครงสร้างของ PAM ให้มอดูลต่างสามารถเชื่อมต่อได้

libpam มี API ทำให้แอพลิเคชั่นสามารถเรียก API ดังกล่าวสำหรับการพิสูจน์ตน (authentication) การจัดการแอคเคาท์ (account management) การออกใบรับรอง (credential establishment) การจัดการเซสชัน (session management) และการเปลี่ยนรหัสผ่าน (password changes)

libpam นำไฟล์หลักในการปรับแต่งค่า (pam.conf) มาใช้ในการระบุเจาะจงว่า PAM มอดูลใดที่จะถูกเรียกใช้สำหรับแต่ละบริการ ซึ่งผู้ดูแลระบบจะเป็นผู้จัดการไฟล์ปรับแต่งค่าของ PAM

libpam นำ pam_sm SPI มาใช้ซึ่งถูกใช้ใน service มอดูล

2.2.4 PAM เซอร์วิสมอดูล (PAM sevice modules)

แต่ละมอดูลจะมีการกำหนดกระบวนการ และวิธีการเฉพาะ ในบางมอดูลอาจมีการกำหนดให้สามารถให้บริการได้เพียงแค่ รูปแบบเดียว ในขณะที่บางมอดูลอาจจะมีการกำหนดให้สามารถทำงานได้หลายรูปแบบ ทั้งนี้ทั้งนั้นถือเป็นสิ่งจำเป็นที่ในแต่ละมอดูล จะต้องมีการกำหนดให้สามารถให้บริการได้ 1 รูปแบบ ตัวอย่างเช่น /usr/lib/security/pam_unix.so สนับสนุนทั้ง 4 รูปแบบของบริการ คือ การพิสูจน์ตน (Authentication) , การจัดการบัญชีผู้ใช้ (Account Management) ,การจัดการ เซสชัน (Session Management) และ การจัดการรหัสผ่าน (Password Management)

จะเห็นได้ว่า PAM จะมีการแบ่งงานเป็น 4 ส่วน ซึ่งจะเป็นอิสระต่อกัน และแต่ละส่วนก็จะทำงานแตกต่างกันออกไป คือ

2.2.4.1 การจัดการการพิสูจน์ตน (Authentication management) ส่วนนี้จะดูแลในเรื่องการพิสูจน์สิทธิ์โดยตรงซึ่งตามปกติแล้ว การพิสูจน์สิทธิ์นั้น จะกระทำโดยมีการตรวจสอบ ชื่อบัญชีผู้ใช้และรหัสผ่าน ถ้าการตรวจสอบผ่าน ก็สามารถเข้าใช้บริการได้แต่ในบางครั้งการพิสูจน์

สิทธิ์ อาจทำโดยรูปแบบอื่น เช่น ผ่านทาง สมาร์ท การ์ด ลายนิ้วมือ หรือใบหน้า ดังนั้นจึงเป็นสิ่งจำเป็นที่ผู้ดูแลระบบ จะต้องเลือกใช้ มอดูลให้ตรงกับกระบวนการในการพิสูจน์ตน

2.2.4.2 การจัดการบัญชีผู้ใช้ (Account management) ส่วนนี้จะดูแลในลักษณะการจัดการการใช้บริการ หรืออนุญาตให้ใช้บริการนั้นได้ เช่น บัญชีผู้ใช้ นี้มีสิทธิ์ที่จะเข้าใช้บริการหรือไม่

2.2.4.3 การจัดการรหัสผ่าน (Password management) ส่วนนี้ถูกใช้ในการกำหนดรหัสผ่านของบัญชีผู้ใช้ หรือทำการกำหนดรหัสผ่านใหม่เมื่อมีการเปลี่ยนแปลงเกิดขึ้น

2.2.4.4 การจัดการเซสชัน (Session management) ส่วนนี้ จะระบุว่าจะมีการทำอะไรบ้างในช่วงที่ ผู้ใช้บริการเริ่มใช้ และช่วงหลังจากที่ใช้บริการเสร็จแล้ว เช่น ช่วงเริ่มใช้บริการอาจมีการบันทึกข้อมูลลงล็อกไฟล์ และหลังจากที่ ใช้บริการเสร็จแล้วอาจมีการส่งข้อความไปแจ้งให้ระบบได้รับรู้

2.2.5 PAM คอนฟิกูเรชันไฟล์ (PAM configuration file)

ไฟล์สำหรับการปรับแต่งค่าของ PAM เป็นส่วนที่จะทำการระบุว่าแต่ละแอพลิเคชันจะเรียกใช้มอดูลใดบ้าง กี่มอดูล ซึ่งไฟล์สำหรับปรับแต่งค่าเองจะมีสองรูปแบบคือ

- แบบไฟล์เดียว (/etc/pam.conf) วิธีการพิสูจน์สิทธิ์ ของทุก ๆ บริการจะถูกเก็บไว้ภายในไฟล์นี้เท่านั้น
- แบบแยกเป็นแต่ละเซอร์วิสที่ให้บริการ ซึ่งจะไฟล์คอนฟิกสำหรับแต่ละเซอร์วิส จะถูกเก็บไว้ที่ตำแหน่ง /etc/pam.d เรียกรูปแบบการปรับแต่งค่าในลักษณะนี้ว่า ไดเร็กทอรี่เบสคอนฟิก (Directory based config)

ทั้งสองรูปแบบจะมีโครงสร้างที่ไม่ต่างกันมาก และจะมีตัวแปรที่กำหนดค่าต่าง ๆ กัน ค่าตัวแปรตัวหนึ่งที่สำคัญ คือค่า แฟล็กควบคุม (control flag) เป็นตัวแปรซึ่งถือได้ว่าเป็นตัวกำหนดความสำคัญของมอดูลที่เรียกถูกเรียกใช้ และยังส่งผลต่อผลลัพธ์ที่แอพลิเคชันจะได้รับกลับไปด้วย

ค่า control flag มีดังนี้

2.2.5.1 *required* ทุกไลบรารี่ที่อยู่ในกลุ่ม module-type เดียวกันที่มีแฟล็กควบคุมเป็น required จะต้องคืนค่าเป็น success ทั้งหมด และการคืนค่ากลับเป็น success นั้นจะเกิดขึ้นเมื่อไม่มีมอดูลที่เป็น binding หรือมอดูลที่เป็น required คืนค่า unsuccess

2.2.5.2 *requisite* หากไลบรารี่ ใดที่มีแฟล็กควบคุม เป็น requisite เมื่อมีการดำเนินการแล้วคืนค่า ออกมาเป็น unsuccess การพิสูจน์ตนจะถูกยกเลิก และคืนการทำงานไปยัง แอพลิ

เคชั่นที่เรียกใช้ PAM แต่จะมีการคืนค่ากลับเป็น success เมื่อทุก ๆ มอดูลที่เป็น requisite คืนค่ากลับเป็น success ทั้งหมด

2.2.5.3 *sufficient* ถ้าไลบรารี่ใดมีค่าแฟล็กควบคุมเป็น sufficient เมื่อมีการดำเนินการแล้วคืนค่า มาเป็น success ระบบจะไม่สนใจการทำงานของไลบรารี่อื่น ๆ ที่อยู่ในกลุ่ม module-type เดียวกัน และจะส่งค่า success คืนกลับไปให้แอพลิเคชั่นหากไม่มีมอดูลที่เป็น required ก่อนหน้ามีการคืนค่าเป็น unsuccess

2.2.5.4 *optional* ไม่ว่าค่าที่คืนกลับมาจะเป็น success หรือ unsuccess ก็จะไม่มีผลต่อการพิสูจน์ตนของระบบโดยรวม แต่จะมีผลเมื่อไฟล์ ปรับแต่งค่ามีการกำหนดค่าแฟล็กควบคุมของ เซอร์วิสชนิดนั้นเป็น optional เพียงอย่างเดียว

2.2.6 รูปแบบของไฟล์ปรับแต่งค่า

2.2.6.1 *แบบไฟล์เดียว* (/etc/pam.conf) ไฟล์นี้จะเก็บค่าที่ระบุว่า แอพลิเคชั่น ใดในระบบจะเรียกใช้วิธีการ หรือกระบวนการในการพิสูจน์ตนใด โดยการระบุค่าในไฟล์มีลักษณะดังนี้

service_name	*module_type*	*control_flag*	*module_path*	*module_options*

service_Name ระบุชื่อของบริการ เช่น ftpd , login

module_type ระบุประเภทของมอดูล

auth	authentication
account	account
password	password
session	session

control_flag ระบุค่าแฟล็กควบคุม

module_path ระบุตำแหน่งของไลบรารี่มอดูล

module_options ระบุค่าออพชั่น ที่สามารถส่งไปยังมอดูล

ทั้ง 5 ส่วนที่กล่าวมานั้น มีเพียงส่วน module_options เท่านั้นที่สามารถละเว้นได้ นอกจากนั้นแล้วทั้ง 4 ส่วนแรก เป็นส่วนที่จำเป็นซึ่งต้องระบุลงไป

ตัวอย่างไฟล์ pam.conf ซึ่งมีการระบุการใช้งานทุก ๆ บริการในไฟล์เพียงไฟล์เดียว

```
# PAM configuration
# Authentication management
login       auth        required        /usr/lib/security/pam_unix.so.1
login       auth        required        /usr/lib/security/pam_dial_auth.so.1
rlogin      auth        sufficient      /usr/lib/security/pam_rhost_auth.so.1
rlogin      auth        required        /usr/lib/security/pam_unix.so.1
dtlogin     auth        required        /usr/lib/security/pam_unix.so.1
telnet      auth        required        /usr/lib/security/pam_unix.so.1
su          auth        required        /usr/lib/security/pam_unix.so.1
ftp         auth        required        /usr/lib/security/pam_unix.so.1
uucp        auth        required        /usr/lib/security/pam_unix.so.1
rsh         auth        required        /usr/lib/security/pam_rhost_auth.so.1
OTHER       auth        required        /usr/lib/security/pam_unix.so.1
#
# Account management
login       account     required        /usr/lib/security/pam_unix.so.1
rlogin      account     required        /usr/lib/security/pam_unix.so.1
dtlogin     account     required        /usr/lib/security/pam_unix.so.1
telnet      account     required        /usr/lib/security/pam_unix.so.1
ftp         account     required        /usr/lib/security/pam_unix.so.1
#
# Session management
#
login       session     required        /usr/lib/security/pam_unix.so.1
rlogin      session     required        /usr/lib/security/pam_unix.so.1
dtlogin     session     required        /usr/lib/security/pam_unix.so.1
telnet      session     required        /usr/lib/security/pam_unix.so.1
uucp        session     required        /usr/lib/security/pam_unix.so.1
OTHER       session     required        /usr/lib/security/pam_unix.so.1
#
# Password management
passwd      password    required        /usr/lib/security/pam_unix.so.1
OTHER       password    required        /usr/lib/security/pam_unix.so.1
```

รูปที่ 2.4 แสดงความตัวอย่างของไฟล์ปรับแต่งค่าแบบไฟล์เดียว (/etc/pam.conf)

แอพลิเคชันใดอื่น ๆ เมื่อต้องการพิสูจน์ตน จัดการบัญชีผู้ใช้ จัดการเซสชัน หรือ จัดการรหัสผ่าน ก็จะใช้ค่ามาตรฐานซึ่งก็คือค่าที่ส่วนของ service_name มีค่าเป็น "OTHER"

```
# PAM configuration
# Authentication management
#
login           auth        required        /usr/lib/security/pam_unix.so.1
login           auth        required        /usr/lib/security/pam_dial_auth.so.1
rlogin          auth        sufficient      /usr/lib/security/pam_unix.so.1
rlogin          auth        required        /usr/lib/security/pam_rhost_auth.so.1
rsh             auth        required        /usr/lib/security/pam_rhost_auth.so.1
OTHER           auth        required        /usr/lib/security/pam_unix.so.1
#
# Account management
OTHER           account     Required        /usr/lib/security/pam_unix.so.1
#
# Session management
OTHER           session     required        /usr/lib/security/pam_unix.so.1
#
# Password management
OTHER           Password    required        /usr/lib/security/pam_unix.so.1
```

รูปที่ 2.5 แสดงไฟล์ปรับแต่งค่าที่มีค่า OTHER

2.2.6.2 *แบบไฟล์ แยก* สำหรับแต่ละบริการ ซึ่งจะคล้าย ๆ กับการใช้ไฟล์ปรับแต่งค่าเพียงไฟล์เดียว หากแต่จะต่างกันที่แบบหลังนี้จะใช้ ชื่อไฟล์เป็นชื่อของบริการนั้น ๆ เลย จึงทำให้ภายในไฟล์ไม่การกำหนดชื่อเซอร์วิส และตำแหน่งของไฟล์ดังกล่าวจะอยู่ภายใต้ไดเร็กทอรี่ /etc/pam.d/ ทำให้การระบุค่าภายในไฟล์เป็นดังนี้

```
module_type     control_flag     module_path     arguments
```

ตัวอย่างไฟล์ /etc/pam.d/su

auth	sufficient	/lib/security/pam_rootok.so	
auth	required	/lib/security/pam_stack.so	service=system-auth
account	required	/lib/security/pam_stack.so	service=system-auth
password	required	/lib/security/pam_stack.so	service=system-auth
session	required	/lib/security/pam_stack.so	service=system-auth
session	required	/lib/security/pam_xauth.so	

รูปที่ 2.6 แสดงไฟล์ปรับแต่งค่าของแอพลิเคชั่น su

2.2.7 กระบวนการในการพิสูจน์ตน

วิธีการซึ่งแอพลิเคชั่นเรียกใช้ PAM ไลบรารี่สำหรับการพิสูจน์ตน พิจารณาได้จากตัวอย่างในการพิสูจน์ตนของผู้ใช้โดยโปรแกรม login

2.2.7.1 แอพลิเคชั่น เริ่มการเรียกใช้งาน PAM โดยเรียกฟังก์ชั่น pam_start() และระบุว่าเป็น บริการ login

2.2.7.2 แอพลิเคชั่นเรียกฟังก์ชั่น pam_authenticate() ซึ่งเป็นส่วนหนึ่งของ PAM API ที่ได้รับจาก PAM ไลบรารี่

2.2.7.3 ไลบรารี่จะค้นหาส่วนที่ได้มีการระบุค่า login ว่ามีอยู่ใน pam.conf หรือไม่

2.2.7.4 แต่ละมอดูล ใน pam.conf ซึ่งได้มีการปรับแต่งค่าสำหรับบริการ login PAM ไลบรารี่จะเรียกใช้ฟังก์ชั่น pam_sm_authenticate() ซึ่ง pam_sm_authenticate() ก็เป็นส่วนหนึ่งของ PAM SPI

2.2.8 การทำงานในลักษณะสแต็ก

เมื่อแอพลิเคชั่นเรียกใช้ฟังก์ชั่นใดก็ตามต่อไปนี้ libpam จะอ่านค่าจาก ไฟล์ปรับแต่งค่า เพื่อใช้ในการพิจารณาว่ามอดูลไหนจะถูกเรียกใช้งานสำหรับบริการ หรือแอพลิเคชั่น

- pam_authenticate()
- pam_acct_mgmt()
- pam_setcred()
- pam_open_session()
- pam_close_session()
- pam_chauthok()

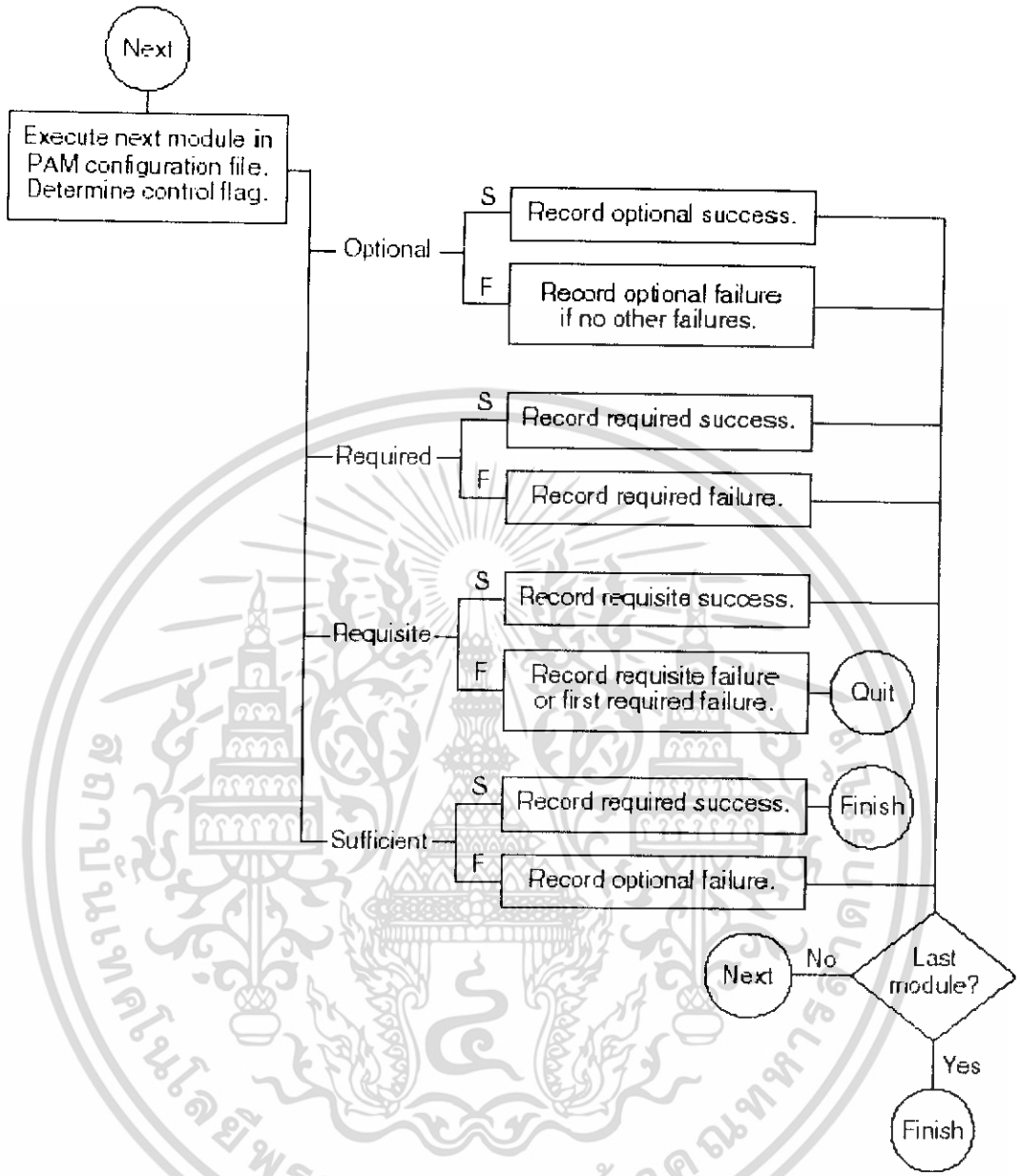
ภายในไฟล์ปรับแต่งค่าของ PAM นั้นจะมีค่าเพียง 1 มอดูล สำหรับการดำเนินงานแต่ละส่วน ของมอดูลนั้น เช่น authentication หรือ account management ผลที่ได้จากมอดูลดังกล่าวจะมีผลต่อการดำเนินงานที่อยู่ถัดไป สำหรับตัวอย่าง เห็นได้ว่ากระบวนการพิสูจน์ตน (auth) สำหรับแอพลิเคชั่น passwd จะมีเพียง 1 มอดูล คือ pam_passwd_auth.so.1

passwd	auth	required	pam_passwd_auth.so.1

ในทางกลับกันนั้น สามารถทำการกำหนดให้มีการเรียกใช้งานได้หลาย ๆ มอดูลซึ่งลักษณะนี้เรียกว่าเป็น สแต็ก ซึ่ง PAM สนับสนุนการทำงานแบบสแต็กด้วย

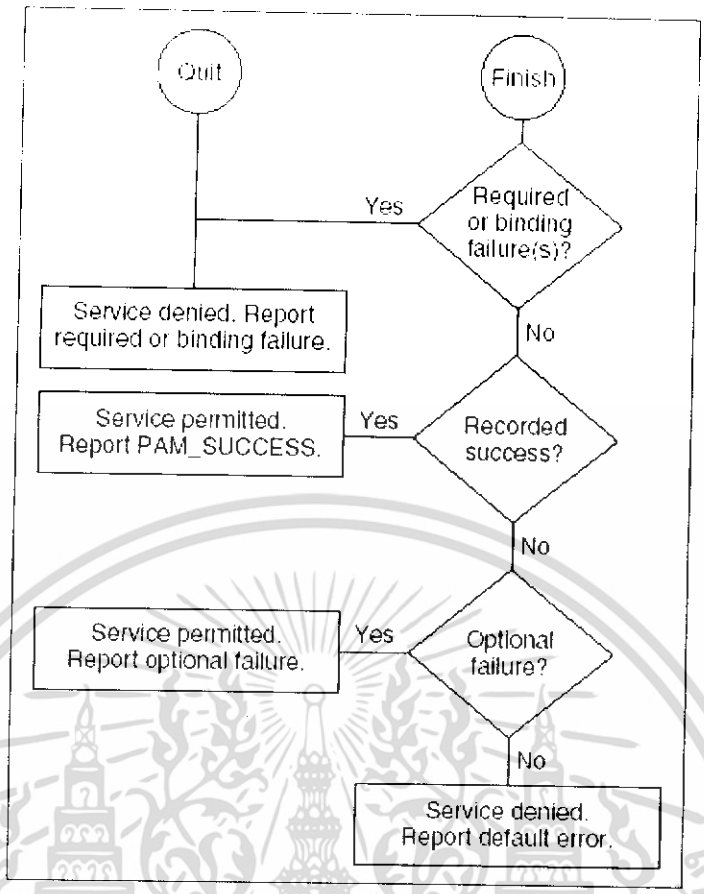
login	auth	requisite	pam_authtok_get.so.1
login	auth	required	pam_dhkeys.so.1
login	auth	required	pam_unix_cred.so.1
login	auth	required	pam_unix_auth.so.1
login	auth	required	pam_dial_auth.so.1

จากตัวอย่างแสดงให้เห็นสแต็กของการพิสูจน์ตน ของบริการ login อย่างง่าย ซึ่งในการพิจารณาผลที่ได้จากสแต็กดังกล่าว โค้ดผลลัพธ์ของแต่ละมอดูล จำเป็นต้องใช้ กระบวนการรวม ซึ่งในกระบวนการรวมนั้น มอดูลจะถูกดำเนินการ ตามลำดับที่ได้มีการระบุไว้ในไฟล์ปรับแต่งค่า โค้ดผลลัพธ์ที่ได้ทั้งสำเร็จและไม่สำเร็จจะถูกนำไปรวมไว้ในผลลัพธ์รวมซึ่งก็จะขึ้นกับ แฟล็กควบคุมของมอดูล ค่าแฟล็กควบคุมสามารถทำให้เกิดการสิ้นสุดของสแต็กได้ หลังจากการประมวลผลสแต็กเสร็จสิ้น ผลลัพธ์ที่ได้แต่ละค่าจะถูกนำมารวมกันเป็นค่าเดียว และค่าผลลัพธ์ ที่ได้นี้จะถูกส่งให้แอพลิเคชั่น



รูปที่ 2.7 ผลที่เกิดจากค่าแฟล็กควบคุม (Control Flags)

แสดงการบันทึกค่า success หรือ failure ของแต่ละชนิดของแฟล็กควบคุม โดยจะมีการตรวจสอบด้วยว่าเป็นมอดูลสุดท้ายหรือไม่ หากไม่ใช่ก็จะไปทำงานในมอดูลถัดไป และจะเก็บค่าผลลัพท์ที่ได้ไว้ จนกว่าจะถึงมอดูลสุดท้าย แล้วจะนำค่าที่เก็บไว้ไปประมวลผลอีกขั้นหนึ่ง



รูปที่ 2.8 การรวมค่าผลลัพธ์

แสดงการรวมค่าผลลัพธ์ที่เก็บไว้ ว่ามีแนวทางในการพิจารณาผลลัพธ์สุดท้ายอย่างไร

2.2.9 การตั้งค่าระบบ PAM

2.2.9.1 การวางแผนสำหรับ PAM

- พิจารณาความต้องการของระบบ เพื่อการเลือกใช้มอดูลได้อย่างถูกต้อง
- ระบุเซอร์วิสที่มีความต้องการใช้งานเป็นพิเศษ และเลือกใช้ OTHER ในกรณีที่เหมาะสม
- พิจารณาคำสั่งที่ทำให้มอดูลทำงาน
- เลือกแฟล็กควบคุมสำหรับมอดูลให้เหมาะสม
- เลือกตัวเลือกที่จำเป็นสำหรับมอดูล

การเปลี่ยนแปลงไฟล์ปรับแต่งค่าควรปฏิบัติดังนี้

- ใช้ OTHER สำหรับแต่ละรูปแบบมอดูลเพื่อที่แต่ละแอพลิเคชั่นไม่ต้องถูกรวมเข้าไปด้วย

- ทำให้แน่ใจว่ามีการพิจารณาความปลอดภัยของแฟล็กควบคุม sufficient และ optional
- ทบทวน man pages ที่เกี่ยวข้องกับมอดูลเพื่อทำความเข้าใจว่ามีหน้าที่และตัวเลือกอย่างไรบ้าง
- ทบทวน man pages เพื่อศึกษาการตอบสนองระหว่างมอดูลสแต็กต่าง ๆ

2.2.9.2 การเพิ่มมอดูล

- ศึกษาเอกสารที่เกี่ยวกับมอดูล และพิจารณาว่าควรใช้แฟล็กควบคุม และตัวเลือกอื่นๆ อย่างไร
- คัดลอกมอดูลใหม่ไปยัง /usr/lib/security
- ตั้งค่าสิทธิในการเข้าใช้งานระบบโดยไฟล์มอดูลจะเป็นสิทธิของ root และมีสิทธิ์เป็น 555
- แก้ไขไฟล์ PAM คอนฟิกกูเรชัน และเพิ่มมอดูลนี้ไปยังเซอร์วิสที่เหมาะสม
- ทดสอบการเปลี่ยนแปลง

หากเซอร์วิส มีการเรียกใช้งานเพียงครั้งเดียวเมื่อระบบเริ่มทำงานจำเป็นต้องทำการปิดและเปิดเครื่องใหม่อีกครั้งก่อนการทดสอบ นับเป็นสิ่งสำคัญมากที่จะต้องทดสอบระบบก่อนทำการปิดและเปิดเครื่องใหม่อีกครั้ง เพื่อป้องกันกรณีที่มีการตั้งค่าระบบที่ผิดพลาดเกิดขึ้น อย่างน้อยที่สุดพยายามทดสอบ rlogin su และ telnet ก่อน

2.2.9.3 การสร้างรายงานความผิดพลาด

เพิ่มรายการใน /etc/syslog.conf โดยต้องรีสตาร์ท หรือ SIGHUP ซิสล็อกเดม่อน (Syslog daemon) เพื่อแจ้งให้รู้ว่ามีการเปลี่ยนแปลงใด ๆ เกิดขึ้น การเลือกสามารถเพิ่มไปในไฟล์เพื่อรวมข้อมูลเกี่ยวกับ PAM ดังนี้

auth.alert ข้อมูลเกี่ยวกับสภาวะที่ควรได้รับการแก้ไขทันที

auth.crit ข้อมูลที่อยู่ในระดับอันตราย

auth.err ข้อมูลที่ผิดพลาด

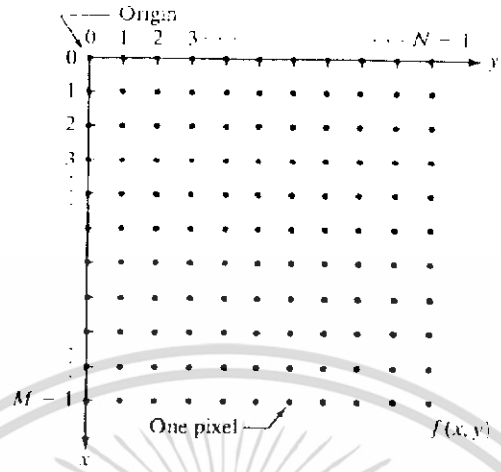
auth.info ข้อมูลที่บอกรายละเอียด

auth.debug ข้อมูลการดีบัก

แต่ละบรรทัดในล็อกประกอบด้วย Timestamp ชื่อของระบบที่สร้างมันขึ้นมา และข้อมูลอื่น โดยไฟล์ pamlog สามารถเก็บรายละเอียดข้อมูลได้จำนวนมาก

2.3 หลักการเบื้องต้นในการประมวลผลรูปภาพ

2.3.1 พิกเซล (Pixels)

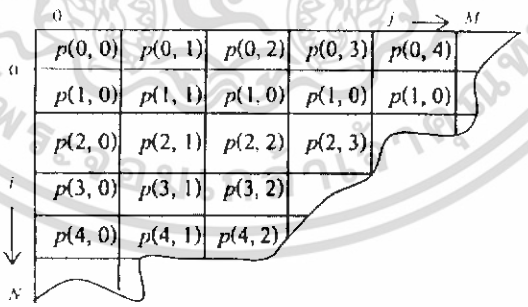


รูปที่ 2.9 พิกเซลแสดงลักษณะของจุดภาพและตำแหน่งของพิกเซล

N คือ จำนวนพิกเซลที่มากที่สุดในหลักหนึ่ง ๆ

M คือ จำนวนพิกเซลที่มากที่สุดในแถวหนึ่ง ๆ

ในภาพหนึ่ง ๆ เราสามารถอธิบายได้เป็นเมตริกซ์ของจุดพิกเซลขนาด MxN โดยใช้คู่ลำดับ p(i,j) แทนค่าของจุดแต่ละจุด โดย i และ j เป็นจำนวนบวกสเกลาร์ p(i,j) จะเป็นตัวชี้บอกความเข้มแสงที่จุดพิกเซลนั้น ๆ ของภาพ

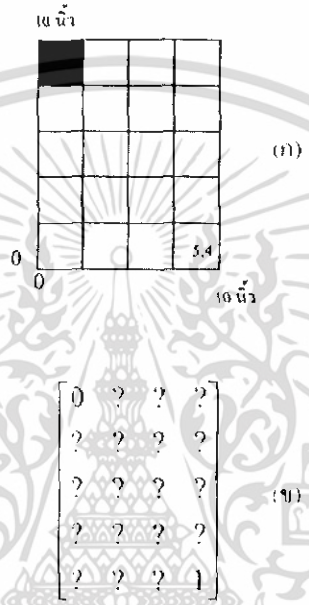


รูปที่ 2.10 ดัชนีแสดงพิกเซลในเมตริกซ์ภาพ

ค่าที่กำกับแต่ละพิกเซลจะแสดงถึงค่าเฉลี่ยของความเข้มแสงในภาพที่จุดพิกเซลนั้นแทนอยู่โดยค่าของพิกเซลดังกล่าวจะเขียนแทนด้วย p(i,j) มีค่าตั้งแต่ 0-1

2.3.2 ตำแหน่งของพิกเซล

ดังที่ได้กล่าวมาแล้วข้างต้น ในภาพหนึ่ง ๆ จะถูกแทนที่ด้วยอาร์เรย์ MxN และค่าในแต่ละจุดพิเซลจะหมายถึงค่าเฉลี่ยของความเข้มแสงที่ตกกระทบถึงภาพ ณ จุดพิกเซลนั้น ๆ พิจารณากรณีตัวอย่างเช่น ภาพขนาด 10x10 นิ้ว หากไม่มีแสงตกกระทบบริเวณด้านบนของภาพ แต่มีแสงที่สว่างมากมาตกกระทบบริเวณส่วนล่างเท่านั้น ดังแสดงในภาพที่ 2.11 เราจะใช้ระบบเลขฐานสองแทนค่าความเข้มของการส่องสว่าง โดยบริเวณที่ไม่ถูกแสงจะแทนด้วย "0" และบริเวณที่ถูกแสงจะแสดงด้วย "1"



รูปที่ 2.11 (ก) ลักษณะที่ตกกระจายไม่เท่ากันบนพื้นผิว
(ข) ค่าของพิกเซลของภาพพื้นผิว

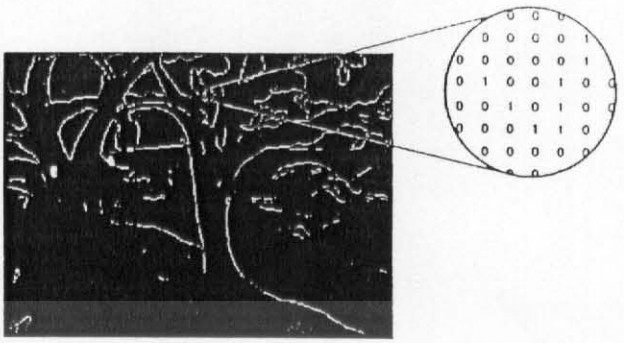
จะเห็นได้ว่าขณะนี้ ภาพจะถูกเขียนแทนด้วยเมตริกซ์ขนาด 5x4 (5 แถว 4 หลัก) แต่ละส่วนย่อยของภาพ (ขนาด 2.5x2.0 นิ้ว) จะมีค่าที่ขึ้นอยู่กับแสงที่ตกกระทบเฉลี่ย

บริเวณขนาด 2.5 x 2.0 นิ้ว ตรงส่วนมุมบนซ้ายของภาพจะถูกแทนด้วยตำแหน่ง (1, 1) ในเมตริกซ์ 5x4 มีค่าเท่ากับ 0 ซึ่งหมายถึงไม่มีแสงมาตกกระทบ

บริเวณขนาด 2.5 x 2.0 นิ้ว ตรงส่วนมุมขวาล่างของภาพถูกแสดงด้วยตำแหน่ง (5, 4) มีค่าเท่ากับ 1 ซึ่งหมายถึงมีความเข้มของการส่องสว่างสูงสุด

ทั้งนี้หมายเหตุไว้ว่า หากใช้ระบบ 16 ระดับสีเทา (16 Gray level systems) แทนระบบเลขไบนารี่ จุดพิกเซลที่ (1, 1) จะมีค่าเท่ากับ 0 และจุด (5, 4) จะมีค่าเท่ากับ 15

อีกประการหนึ่ง ผู้ออกแบบระบบจะต้องกำหนดค่าเธรโชล (Threshold value) ของความเข้มของการส่องสว่าง ที่จะใช้เป็นเกณฑ์ในการเปลี่ยนระดับจาก 0 เป็น 1



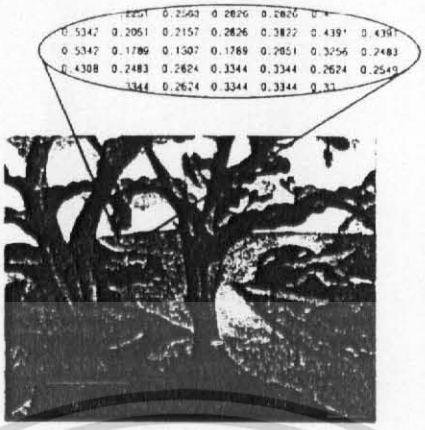
รูปที่ 2.12 ค่าของพิกเซลของภาพพื้นผิวภาพขาวดำ (Binary Image)

2.3.3 ระดับสีเทา (Gray level)

หากเราต้องการค่าข้อมูลที่ละเอียดมากขึ้น ก็จำเป็นที่จะต้องเพิ่มจำนวนบิตในการแสดงค่าของแต่ละพิกเซล ยกตัวอย่างเช่น หากแบ่งความเข้มของการส่องสว่างให้มี 4 ระดับ ก็ต้องใช้เลขฐานสอง จำนวน 2 บิต และ 4 บิต สำหรับ 16 ระดับ และ 8 บิต สำหรับ 256 ระดับ ซึ่งจำนวนระดับที่ใช้ในระดับสีเทานี้ มักเป็นเลขยกกำลังของ 2 ค่าที่ต่ำที่สุด คือ 0 กำหนดให้เป็นสีดำ และ 1 หรือ ตัวเลขที่น้อยกว่าค่าสูงสุดของระดับสีเทาอยู่ 1 (เช่น 15 สำหรับระดับสีเทา 16) แทนสีขาว ค่าที่กำหนดให้ในแต่ละพิกเซลมักเป็นจำนวนเต็ม

ในยุคแรก ๆ ของระบบการมองเห็นภาพจะใช้ระบบเลขฐานสอง แต่ในปัจจุบันเทคโนโลยีไมโครโปรเซสเซอร์เข้ามามีบทบาทมากขึ้น การแบ่งระดับเป็น 16, 64 หรือ 256 เป็นเรื่องที่ทำได้ง่าย แต่ทั้งนี้ในการมองเห็นของมนุษย์ จะสามารถแยกแยะความแตกต่างได้เพียง 10 – 15 ระดับเท่านั้น การแบ่งโดยละเอียดเป็น 64 ระดับ หรือ 256 ระดับ อาจจะนำไปประยุกต์ใช้กับงานการประมวลผลภาพแบบอื่นๆ

จะเห็นว่าจำนวนระดับสีเทาจะเป็นตัวจำกัดรายละเอียดของภาพ โดยทั่วไปแล้ว ยิ่งแบ่งระดับสีเทาเป็นหลาย ๆ ระดับ ก็เป็นการเพิ่มคุณภาพของภาพด้วย และการเพิ่มจำนวนพิกเซล เช่น จาก 30x35 เป็น 250x256 ก็จะเป็นการเพิ่มความละเอียด (Resolution) และรายละเอียด (Detail) ของภาพเช่นกัน จะเห็นว่าจะแตกต่างกับการขยาย (Zoom) ภาพคือ การเพิ่มขนาดของแต่ละพิกเซลให้ใหญ่ขึ้น ไม่ได้เป็นการเพิ่มจำนวนความละเอียด



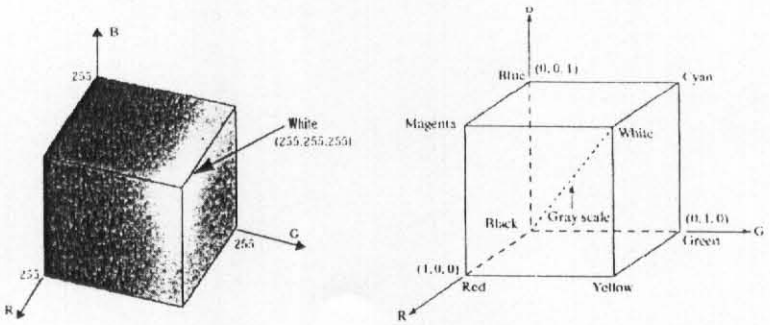
รูปที่ 2.13 ค่าของพิกเซลของพื้นผิวภาพระดับสีเทา (Gray scale image)

2.3.4 พื้นฐานและระบบโครงสร้างสีที่ใช้

2.3.4.1 ระบบโครงสร้างสีอาร์จีบี (RGB color model)

ในโครงสร้างสีนี้ สีแต่ละสีจะปรากฏ ในรูปของแม่สี (แดง เขียว น้ำเงิน) โครงสร้างสีนี้มีโครงสร้างเป็นลักษณะแกนคาร์ทีเซียนโคออดิเนต (Cartesian coordinate) โดยมีลักษณะเป็นทรงลูกบาศก์ดังแสดงในรูป 2.14 (ก) ค่าของสีแดง เขียวและน้ำเงิน จะอยู่ที่มุมทั้งสาม และค่าสีคราม ม่วง และเหลือง จะอยู่ที่มุมทั้งสามที่เหลือ สีดำจะอยู่ที่จุดกำเนิด สีขาวจะอยู่ไกลสุดในลักษณะทแยงมุมกับจุดกำเนิด ค่าของระดับสีเทา (Gray scale) จะอยู่บนเส้นที่เชื่อมระหว่างสีดำกับสีขาวในลักษณะทแยงมุมกับจุดกำเนิด ค่าของสี คือ จุดที่อยู่บนผิวหรือในลูกบาศก์ถูกกำหนดค่าโดยเวกเตอร์ที่ชี้ออกจากจุดกำเนิด ซึ่งช่องว่างแต่ละที่ในลูกบาศก์เรียกว่า ความลึกของพิกเซล (Pixel depth) โดยแม่สีแต่ละสีมีค่า 8 บิต แต่ละแม่สีจะมี 2^8 = 256 สี เพราะฉะนั้นแม่สีทั้งสามระนาบจะมีความลึกของพิกเซล 24 บิต โดยรวมสีทั้งหมดของความลึกของพิกเซลในลูกบาศก์ (24 บิตอาร์จีบี) จะได้ทั้งหมด $(2^8)^3$ = 16,777,216 สี เพื่อความสะดวกเราจะสมมุติให้ค่าสีถูกนอร์มอลไลซ์ ทั้งสามสีให้มีค่าอยู่ในช่วง 0 ถึง 1 ลูกบาศก์ที่แสดงในรูปที่ 2-14(ข) นี้จึงได้เป็นลูกบาศก์หนึ่งหน่วย

ภาพในโครงสร้างสีอาร์จีบี ประกอบด้วยภาพสามระนาบที่เป็นอิสระจากกัน สำหรับแต่ละแม่สี เมื่อป้อนเข้าไปในมอร์นิเตอร์ที่เป็นแบบอาร์จีบี ภาพทั้งสามสีจะรวมกันที่จอภาพกลายเป็นภาพสีผสม ดังนั้น การใช้โครงสร้างสีอาร์จีบี ในการประมวลผลภาพนั้นจะมีความเหมาะสมอย่างยิ่ง เมื่อภาพถูกแยกสีออกโดยธรรมชาติ ให้อยู่ในเทอมของทั้งสามแม่สี กล้องถ่ายรูปดิจิตอลส่วนใหญ่ที่ให้ภาพดิจิตอลจะอยู่ในรูปแบบของโครงสร้างสีอาร์จีบีดังนั้น โครงสร้างสีนี้จึงเป็นโครงสร้างที่สำคัญมาก ในการประมวลผลภาพ



รูปที่ 2.14 (ก) แสดงโครงสร้างสีอาร์จีบี (ข) แสดงโครงสร้างสีอาร์จีบี เป็นลูกบาศก์หนึ่งหน่วย

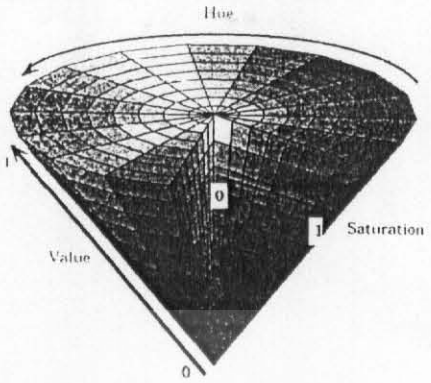
2.3.4.2 ระบบโครงสร้างสีวายซีบีซีอาร์ (YCbCr Color Model)

ในโครงสร้างสีนี้จะใช้เป็นที่แพร่หลายสำหรับดิจิตอลวิดีโอ ในรูปแบบของโครงสร้างสีนี้ ค่าปริมาณของแสงในการส่องสว่างจะเก็บข้อมูลนี้ไว้ในส่วนของ (Y) และในส่วนความแตกต่างของสีนั้นจะแบ่งได้เป็น 2 สี คือ Cb และ Cr โดย Cb จะแสดงให้เห็นถึงความแตกต่างของส่วนประกอบสีฟ้า และอ้างถึงค่าในหมวดสีฟ้านั้น ส่วน Cr จะแสดงให้เห็นถึงความแตกต่างของสีแดง และอ้างถึงค่าในหมวดสีแดง โดยโครงสร้างสีวายซีบีซีอาร์ มีความเที่ยงตรงและแม่นยำมากขึ้น ในส่วนของการส่องสว่าง และหมวดสี ซึ่งเป็นโครงสร้างสีที่ใช้กันในการเข้ารหัสแบบเอ็มพีอีจี (MPEG & JPEG)

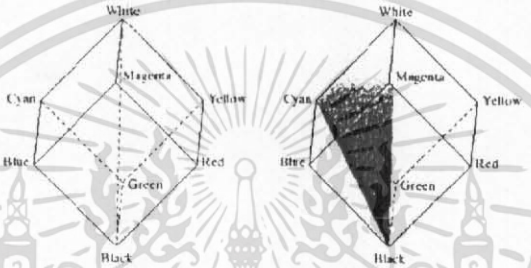
2.3.4.3 ระบบโครงสร้างสีเอชเอสวี (HSV)

ในส่วนโครงสร้างสีเอชเอสวี (H:hue คือ การจัดระดับของสี S:saturation คือ ความอิ่มตัวของสี V:values คือ ค่าความสว่างของสีนั้น ๆ) ซึ่งบ่อยครั้งที่ถูกใช้ในการเลือกสีจากแผ่นเลือกสี เพราะว่ามันมีลักษณะการแบ่งเฉดสีได้ดีกว่าอาร์จีบี

ค่าในการจัดระดับของสี (Hue) จะแปรค่าจาก 0 ไปถึง 1 ระดับของสีจะแปรจากสีแดง ไปยังสีเหลือง เขียว ฟ้าคราม น้ำเงิน ม่วง จนกลับไปเป็นสีแดง ส่วนค่าความอิ่มตัวของสี (saturation) จะแปรค่าจาก 0 ไปยัง 1 เช่นเดียวกัน โดยแกนสีเดียวกันในระดับของสีนั้นจะแปรค่าจากค่าที่ยังไม่มีความอิ่มตัวของสี (ระดับสีเทา) ไปยังที่อิ่มตัวของสีนั้นเต็มที่ ส่วนค่าความสว่างของสี (values) ก็แปรค่าจาก 0 ไปยัง 1 เช่นกัน โดยจะเห็นได้ว่าสีนั้นจะมีความสว่างเพิ่มขึ้น



(ก)

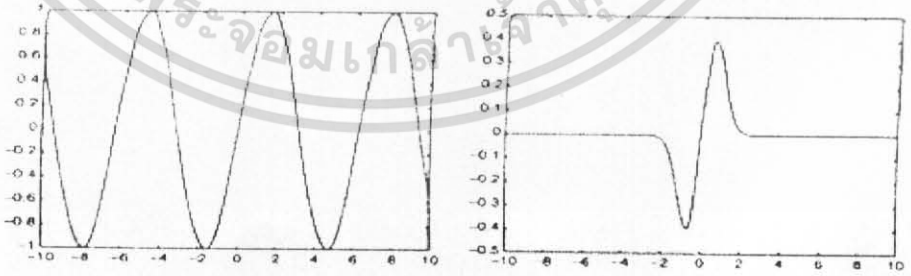


(ข)

ภาพที่ 2.15 (ก) แสดงโครงสร้างสีเอชเอสวี
(ข) แสดงความสัมพันธ์ระหว่างโครงสร้างสีเอชเอสวีและอาร์จีบี

2.3.5 เวฟเล็ท (Wavelet)

แนวคิดของการใช้เวฟเลท เพื่อที่จะรักษารูปแบบของคลื่นไว้ แต่ลดในส่วนที่เป็นคาบ (periodicity) ทั้งนี้อาจพิจารณาเวฟเลทเป็นส่วนเล็ก ๆ ส่วนหนึ่ง ที่ไม่ใช่ ศูนย์ของคลื่นสัญญาณภาพในช่วงพื้นที่เล็ก ๆ ก็ได้ ดังรูปที่ 2.16 แสดงให้เห็น wave และ wavelet ในช่วงเดียวกัน



(ก) (ข)

รูปที่ 2.16 (ก) เวฟ (wave) (ข) เวฟเลท (wavelet)

หาก f = w(x) เป็นฟังก์ชันที่อธิบายเวฟเลทเราสามารถ

ขยายขนาดได้โดยใส่สเกลลิ่งแฟคเตอร์ (scaling factor) ให้กับ x เช่น x:f(2x) จะบีบอัดเวฟเลทและ f(x/2) จะขยายเวฟเลท

- เปลี่ยนตำแหน่งโดยเพิ่มตัวลบ เช่น x : f(x-2) จะเลื่อนเวฟเลทไป 2 หน่วย ด้านขวา หรือ f(x+3) จะเลื่อนไปทางซ้าย 3 หน่วย

- เปลี่ยนแปลงความสูงโดยการคูณฟังก์ชัน กับค่าคงที่ นอกจากนี้แล้วเราสามารถ กระทำทั้ง 3 ลักษณะลงไปพร้อมๆ กันได้ด้วย เช่น

$$4f(x/2 - 5) \quad , \quad 8f(4x + 2) \, , \ldots \tag{2.1}$$

ดังนั้นเราสามารถอธิบายเวฟเลทได้ในรูปของสมการ

$$aw(bx + c) \tag{2.2}$$

หากกล่าวถึง 2 มิติ เราสามารถที่จะประยุกต์ใช้เวฟเลทกับภาพในรูปแบบเดียวกันกับที่เราประยุกต์ไซน์ (sine) และโคไซน์ (cosines) กับการแปลงรูปฟูเรีย (Fourier Transform)

การใช้เวฟเลททำให้ได้ กระบวนการประมวลผลที่มีประสิทธิภาพสูงมาก เพราะเวฟเลทสามารถใช้ในการลดสัญญาณรบกวน (noise reduction) ตรวจจับขอบ (edge detection) และการบีบอัดภาพ

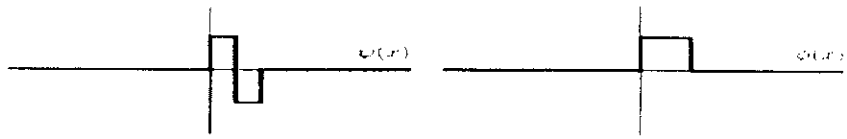
2.3.6 ฮาร์เวฟเลท (The Haar Wavelet)

เป็นเวฟเลทที่ใช้กันอยู่โดยทั่วไปมาเป็นเวลานานแล้ว และถูกนำใช้กับภาพในชื่อ การแปลงรูปของฮาร์ (The Haar Transform) เมื่อไม่นานมานี้เองที่มีการมองการแปลงรูปของฮาร์เป็นเพียงการแปลงรูปเวฟเลทอย่างง่าย

ฮาร์เวฟเลท อธิบายได้ด้วยฟังก์ชัน

$$\psi(x) = \begin{cases} 1 \ if \ \ 0 < x < 1/2 \\ -1 \ if \ \ 1/2 \le x < 1 \\ 0 \ if \ \ otherwise \end{cases} \tag{2.3}$$

ดังที่ได้แสดงในสมการ (2.3) ได้กล่าวถึงฟังก์ชั่นเวฟเลท w(x) เราสามารถบีบอัดและขยาย เวฟเลทนี้ได้ทั้งโดยความสูงหรือความกว้าง รวมไปถึง สามารถเลื่อนตำแหน่งได้



รูปที่ 2.17 ฟังก์ชั่นเวฟเลท w(x)

2.3.6.1 ประยุกต์ใช้ ฮาร์เวฟเลท (Applying the Haar Wavelet)

การแปลงรูปเวฟเลท คือ ผลรวมของ ค่าที่ได้จากฟังก์ชัน คูณกับ ค่า wavelet หรือหากมองในส่วนของ DFT จะเป็น ผลคูณของค่าที่ได้จาก ฟังก์ชัน กับเอกซ์โพแนนเชียลเชิงซ้อน หรือในส่วนของ DCT จะเป็น ผลคูณของค่าที่ได้จาก ฟังก์ชันกับโคไซน์

การแปลงรูปดีสครีตเวฟเลท (DWT) สามารถเขียนเป็นสมการได้ดังนี้

$$W_\phi(j_0,k) = \frac{1}{\sqrt{M}} \sum_x f(x)\phi_{j_0,k}x \tag{2.4}$$

$$W_\psi(j,k) = \frac{1}{\sqrt{M}} \sum_x f(x)\psi_{j,k}x \tag{2.5}$$

ซึ่ง $\phi(x)$ และ $\psi(x)$ หมายถึง การดีเลท (dilate) และการเลื่อนตำแหน่ง ของฟังก์ชันหลัก หรือสามารถเขียนในรูป f(x) โดย

$$f(x) = \frac{1}{\sqrt{M}} \sum_k W_\phi(j_0,k)\phi_{j_0,k}x + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{\infty} W_\psi(j,k)\psi_{j,k}(x) \tag{2.6}$$

สมการเหล่านี้ แสดงให้เห็นว่า DWT มีพื้นฐานเดียวกับที่ปรากฏใน DFT และ DCT ซึ่งในแต่ละกรณีที่มีการจัดรูปแบบของผลบวก ของค่าอินพุตคูณกับค่าที่ได้จากฟังก์ชันที่กำหนด

จากรูปแบบของสมการข้างต้น แสดงให้เห็นว่าการแปลงรูปดีสครีตเวฟเลทสามารถเขียนในรูป ของ ผลคูณเมทริกซ์ (matrix multiplication)

สังเกตว่าฮาร์เวฟเลทสามารถเขียนในรูปของ พัลส์ ฟังก์ชันได้

$$\phi(x) = \begin{cases} 1 & if \quad 0 \le x < 1 \\ 0 & if \quad otherwise \end{cases} \tag{2.7}$$

ใช้ความสัมพันธ์

$$\psi(x) = \phi(2) - \phi(2x-1) \tag{2.8}$$

จะเห็นว่าไม่มีค่าที่ทำให้ $\phi(2x)$ เท่ากับ 1 สำหรับค่า x ในช่วง $0 \le x \le 1/2$ และเช่นเดียวกัน สำหรับ $\phi(2x-1)$ หาก x อยู่ในช่วง $1/2 \le x < 1$

พัลส์ฟังก์ชันสามารถแทนได้ด้วยสมการ

$$\phi\left(\frac{x}{2}\right) = \phi(x) - \phi(x-1) \tag{2.9}$$

ตามทฤษฎีของเวฟเลทในกรณีนี้ หมายถึง ฟังก์ชัน $\psi(x)$ จะเรียกว่า mother wavelet และ corresponding function $\phi(x)$ เรียกว่า scaling function (บางครั้งเรียกว่า father wavelet)

สามารถเขียนสมการการสเกลตามสมการ (2.9) ได้เป็น

$$\phi(x) = \phi(2x) + \phi(2x-1) \tag{2.10}$$

ซึ่งสมการ (2.9) และ (2.10) นี้จะบอกว่าเวฟเลทจะถูกสเกล อย่างไร ที่รีโซลูชั่นต่างกัน ออกไปสมการที่ (2.10) ถือได้ว่าเป็นสมการที่สำคัญมาก ถูกเรียกว่าสมการดีเลชั่นเนื่องจากเกี่ยวข้องในส่วนของฟังก์ชั่นสเกลลิ่งที่เพิ่มขนาด ตัวเอง

จากสมการดีเลชั่นและและเวฟเลทจะมีส่วนทางขวาที่เหมือนกัน ยกเว้นเครื่องหมาย สามารถเขียนใหม่ได้เป็น

$$\phi(x) = \ldots + h_{-2}\phi(2x+2) + h_{-1}\phi(2x+1) + h_0\phi(2x) + h_1\phi(2x-1) + h_2\phi(2x-2) + \ldots \tag{2.11}$$

$$\psi(x) = \ldots - h_{-2}\phi(2x-3) + h_{-1}\phi(2x-2) - h_0\phi(2x-1) + h_1\phi(2x) - h_2\phi(2x+1) + \ldots \tag{2.12}$$

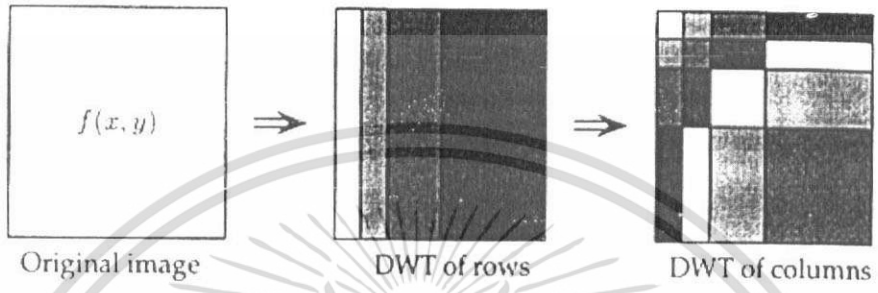
ค่า h_i เรียกว่า filter coefficients หรือ แท็บของเวฟเลท

เวฟเลทจะถูกระบุ เจาะจงด้วยแท็บของมันเอง

การแปลงรูปเวฟเทลจำนวนไม่น้อยที่สามารถ คำนวณได้อย่างรวดเร็วโดยอัลกอริทึมที่ดี ซึ่งก็จะคล้ายกับในรูปแบบของค่าเฉลี่ยหรือความต่างกระบวนการเหล่านี้ จะถูกเรียกว่า กระบวนการยกขึ้น (lifting methods)

2.3.6.2 เวฟเลท 2 มิติ (2-Dimensional Wavelets)

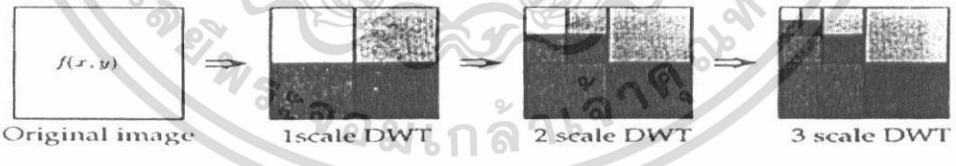
การแปลงรูปเวฟเลท 2 มิติเป็นส่วนที่มีการแยกจากกัน ซึ่งหมายความว่า สามารถใช้การแปลงรูปเวฟเทล 1 มิติเดียวกับภาพได้ในทางเดียวกันกับ DFT คือ ใช้ DWT 1 มิติ กับทุกหลักและต่อด้วย DWT 1 มิติ กับทุกแถวของผลลัพธ์ ที่ได้ วิธีการนี้เรียก การดีคอมโพซิชั่นมาตรฐาน (standard decomposition)



รูปที่ 2.18 การดีคอมโพซิชั่นมาตรฐานของ DWT 2 มิติ

เราสามารถใช้การแปลงรูปเวฟเลทในแบบที่ต่างออกไปได้ สมมติว่าใช้การแปลงรูปเวฟเลทกับภาพโดยหลัก และต่อด้วย แถว แต่ก็เป็นการแปลงรูปเพียงสเกลเดียวเท่านั้น วิธีการนี้จะทำให้ผลลัพธ์ที่ได้อยู่ในรูป 4 ควอเตอร์มุมบนซ้ายจะเป็นขนาดครึ่งหนึ่งของภาพ และควอเตอร์อื่น ๆ จะเป็นไฮพาสฟิลเตอร์ (high-pass filtered)

ควอเตอร์เหล่านี้ จะเก็บขอบแนวนอน แนวตั้งและแนวทแยงของภาพ จากนั้นเราจะใช้ DWT สเกลเดียว กับควอเตอร์บนซ้าย แล้วสร้างภาพที่เล็กลง ไปเรื่อย ๆ วิธีการแบบนี้เรียกการดีคอมโพซิชั่นแบบไม่มาตรฐาน



รูปที่ 2.19 การดีคอมโพซิชั่นที่ไม่มาตรฐานของ DWT 2 มิติ

2.3.7 การแยกลักษณะเด่นของภาพด้วยตัวกรองเกเบอร์ (Gabor Filter)

โครงงานได้มีการนำเกเบอร์เวฟเลท (Gabor Wavelet) มาวิเคราะห์พื้นผิวของภาพ ซึ่งมีหลักการทำงานคือ พิจารณารูปแบบการเรียงตัวของพิกเซล ทำให้เราสามารถนำมาหาลักษณะเด่นของพื้นผิว (Texture Feature) ได้โดยการคำนวณหาค่าเฉลี่ย และค่าความแปรปรวนของภาพที่ผ่านกระบวนการกรองเกเบอร์ โดยทำนอร์มอลไลซ์การหมุน (Rotation Normalization) ที่มี

ลักษณะการเคลื่อนตัวเป็นวงกลมของแต่ละอิลิเมนท์ขององค์ประกอบ (Feature Element) ทั่วทั้งภาพและจะมีทิศทาง การเคลื่อนตัวที่เป็นลักษณะเด่นออกมาเหมือน ๆ กัน

ถ้ากำหนดให้ตำแหน่งของพิกเซลใด ๆ ในภาพคือ I(x,y) และขนาดของภาพนั้นคือ PxQ โดยจะมีความสัมพันธ์ดังสมการคอนโวลูชั่นดังนี้

$$G_{mn}(x,y) = \sum_{s}\sum_{t} I(x-s, y-t)\psi^{*}_{mn}(s,t) \tag{2.13}$$

จากสมการคอนโวลูชั่น รูปแบบการแปลงดีสครีตเกเบอร์เวฟเลต

โดย s และ t คือ ตัวแปรขนาดของหน้ากากตัวกรอง (Filter Mask Size)

ψ^{*} คือ คอนจูเกตเชิงซ้อนของ $\psi(x,y)$

ψ คือ ระดับของฟังก์ชั่นความคล้ายกัน (Class of Self-similar Function) โดยได้จาก การแผ่ขยายตัวและการหมุนตัวของเวฟเลท ดังนี้

$$\Psi(x,y) = \frac{1}{2\Pi\sigma_x\sigma_y}\exp\left[-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\right)\right]\exp(j2\Pi Wx) \tag{2.14}$$

ซึ่ง W คือความถี่ของการมอดูเลท

และจะได้ฟังก์ชั่นความคล้ายกันของเกเบอร์เวฟเลท (Self-similar Gabor Wavelet) ดังนี้

$$\Psi_{mn}(x,y) = a^{-m}\Psi(\tilde{x},\tilde{y}) \tag{2.15}$$

เมื่อ m และ n เจาะจงด้วยสเกล (Scale) และการปรับตัว (Orientation) ของเวฟเลท ตามลำดับ M = 0 ,1, ... M-1, n=0, 1, ... N-1 และ

$$\tilde{x} = a^{-m}(x\cos\theta + y\sin\theta) \tag{2.16}$$

$$\tilde{y} = a^{-n}(-x\sin\theta + y\cos\theta) \tag{2.17}$$

โดยที่ a > 1 และ $\theta = n\Pi / N$

ตัวแปรในสมการข้างต้นนี้มีค่าดังนี้

$$a = (U_h / U_l)^{\frac{1}{M-1}} \tag{2.18}$$

$$W_{m,n} = a^m U_l \tag{2.19}$$

$$\sigma_{x,m,n} = \frac{(a+1)\sqrt{2\ln 2}}{2\Pi a^m (a-1)U_l} \tag{2.20}$$

$$\sigma_{y,m,n} = \frac{1}{2\Pi \tan\left(\frac{\Pi}{2N}\right)\sqrt{\frac{U_h^2}{2\ln 2} - \left(\frac{1}{2\Pi\sigma_{x,m,n}}\right)^2}} \tag{2.21}$$

2.3.7.1 การแสดงออกของพื้นผิวและการกอบกู้คืนของพื้นผิว

เราสามารถคำนวณหาการแสดงออกพื้นผิวโดยใช้การแปลงเกเบอร์ (Gabor transform) โดยกระบวนการคำนวณความคล้ายคลึงกันของพื้นผิว (Texture Similarity) และการนอร์มอลไลซ์การหมุน

2.3.7.1 การแสดงออกของพื้นผิว

หลังจากที่เราใช้ตัวกรองเกเบอร์บนรูปภาพแล้ว ผลลัพธ์ที่ได้คือความแตกต่างของการปรับตัวที่แตกต่างกันที่สเกล โดยเราจะได้อาเรย์ของขนาด (Array of Magnitude) ดังสมการนี้

$$E_{(m,n)} = \sum_x \sum_y |G_{mn}(x,y)| \tag{2.22}$$

เมื่อ m = 0, 1,…,M-1; n = 0, 1, …,N-1

ค่าของขนาด (Magnitude) เหล่านี้ประกอบไปด้วยความแตกต่างของสเกลและการปรับตัวของรูปภาพ จุดประสงค์หลักของการกอบกู้พื้นผิวภาพพื้นฐาน (Texture-based Retrieval) ก็เพื่อที่จะค้นหารูปภาพที่มีองค์ประกอบคล้ายกัน หรือค้นหาบริเวณที่มีความคล้ายคลึงกันของพื้นผิว ซึ่งมันเป็นการคาดคะเนภาพที่เรากำลังสนใจ หรือบริเวณที่เรากำลังพิจารณาที่มีพื้นผิวเป็นเนื้อเดียวกัน (Homogenous Texture) โดยที่ค่าเฉลี่ยของขนาดคือ μ_{mn} และค่าเบี่ยงเบนมาตรฐานของขนาดที่ได้จากการแปลงสัมประสิทธิ์ คือ σ_{mn} โดยตัวแปรทั้งหมดนี้แทนการดึงองค์ประกอบของบริเวณที่พื้นผิวเป็นเนื้อเดียวกัน

$$\mu_{mn} = \frac{E(m,n)}{P \times Q} \tag{2.23}$$

$$\sigma_{mn} = \frac{\sqrt{\sum_x \sum_y (|G_{mn}(x,y) - \mu_{mn})^2}}{P \times Q} \tag{2.24}$$

ในองค์ประกอบของเวคเตอร์ f นี้แสดงถึงการแสดงออกของพื้นผิว (Texture Representation) โดยที่สร้างมาจากค่าเฉลี่ยของขนาด μ_{mn} และค่าเบี่ยงเบนมาตรฐานของขนาดที่ได้จากการเปลี่ยนแปลงสัมประสิทธิ์ σ_{mn} ให้เป็นส่วนประกอบของลักษณะเด่น ยกตัวอย่างเช่น มีขนาดสเกลคือ 5 และ 6 ค่าการปรับตัว เพราะฉะนั้นเราจะได้องค์ประกอบของเวคเตอร์ f ดังนี้

$$f = (\mu_{00}, \sigma_{00}, \mu_{01}, \sigma_{01}, \ldots, \mu_{45}, \sigma_{45}) \tag{2.25}$$

รูปที่ 2.20 รูปแบบของค่าเฉลี่ยขององค์ประกอบลักษณะเด่นของภาพ μ_{mn}
(ก) รูปภาพฟาง **(ข)** ผลการแปลงเกเบอร์ของภาพ (ก)
(ค) ภาพที่ได้จากการหมุนภาพ (ก) 90° **(ง)** ผลของการแปลงเกเบอร์ของภาพ (ค)

ดังภาพที่ 2.20 ได้แสดงให้เห็นถึงความแตกต่างของ 2 พื้นผิวภาพและผลของการแปลงเกเบอร์ที่ได้โดยภาพ (ค) หมุนไป 90° จากภาพ (ก) และจากภาพ (ข) เป็นผลการแปลงเกเบอร์ของภาพ (ก) สังเกตได้ว่าลักษณะทิศทางที่โดดเด่นอยู่ที่การปรับภาพที่ค่า 2 (60°) ในขณะที่ภาพ (ข) สังเกตได้ว่าลักษณะทิศทางที่โดดเด่นอยู่ที่การปรับภาพที่ค่า 5 (150°)

2.3.7.2 การวัดหาค่าการหมุนตัวที่ไม่เปลี่ยนแปลงความคล้ายคลึงกัน (Rotation Invariant Similarity) ในการวัดความคล้ายคลึงขององค์ประกอบบนพื้นผิวภาพที่เข้ามาทำการตรวจสอบ

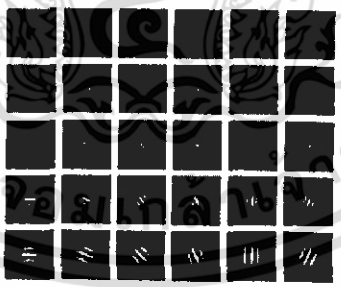
โดยกำหนดให้เป็น Q และเป้าหมายของภาพที่ต้องการตรวจสอบค้นหาในฐานข้อมูลเป็น T โดยมีสมการดังนี้

$$D(Q,T) = \sum_{m}\sum_{n} d_{mn}(Q,T) \tag{2.26}$$

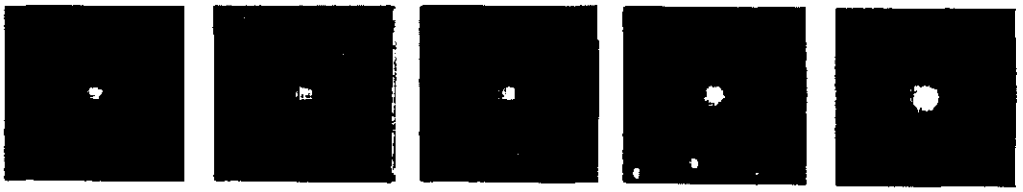
เมื่อค่าระยะห่าง (Distance) คือ

$$d_{mn} = \sqrt{(\mu_{mn}^{Q} - \mu_{mn}^{T})^2 - (\sigma_{mn}^{Q} - \sigma_{mn}^{T})^2} \tag{2.27}$$

เนื่องจากว่าการวัดค่าความคล้ายคลึงกันของภาพ ไม่ใช่เป็นการหมุนตัวที่ไม่เปลี่ยนแปลง (Rotation Invariant) แต่เป็นเพราะความคล้ายคลึงกันของพื้นผิวภาพด้วยความแตกต่างของทิศทาง จากตัวอย่างในรูปที่ (ก) และ (ค) ทั้งสองภาพนี้คือรูปแบบเดียวกัน แต่แตกต่างกันที่การปรับหมุนภาพเท่านั้น ซึ่งผลของภาพจะมีระยะห่าง (Distance) สูงมาก ถ้าเราทำการวัดจุดพิกเซลโดยตรง โดยในจุดประสงค์ของการกรองเกเบอร์นี้เราต้องการให้ได้การวางตัวของลักษณะส่วนโค้งที่เด่นในบริเวณทั่วใบหน้า ไม่ว่าจะเป็นส่วนโค้งของคิ้ว ปาก ตา โดยดึงองค์ประกอบของส่วนโค้งโดยทั่วทั้งภาพ ผลที่ได้นี้ เราจะคำนวณหาพลังงานรวม (Total Energy) ของแต่ละการปรับตัวของภาพ โดยที่การปรับตัวที่มีค่าพลังงานรวมสูงสุดนี้เราเรียกว่า ทิศทางที่โดดเด่น (Domminant Direction) โดยที่จะเป็นองค์ประกอบส่วนหนึ่งของเวคเตอร์ f



รูปที่ 2.21 ส่วนจริงของสเกลคือ 5 และ 6 ค่าการปรับตัว



รูปที่ 2.22 ขนาดของเกเบอร์เมื่อกำหนดให้ 5 สเกลที่แตกต่าง

2.4 การตรวจสอบใบหน้าของผู้ใช้

ในการตรวจสอบใบหน้าของผู้ทำการล็อกอินว่าเป็นใบหน้าของผู้ใช้ คนใดในระบบ จะใช้การหาค่าความเด่นบนใบหน้าของบุคคลซึ่งแต่ละบุคคล จะมีจุดเด่นบนใบหน้าบริเวณต่าง ๆ แตกต่างกันไป

โครงงานนี้ มีการนำตัวกรองเกเบอร์มาใช้เป็นเทคนิคในการหาจุดเด่นบนใบหน้า โดยจะมีจุดอ้างอิงที่ใช้ด้วยกัน 12 จุดคือ

- หางคิ้วขวา
- หางคิ้วซ้าย
- หัวคิ้วขวา
- หัวคิ้วซ้าย
- หางตาขวา
- หางตาซ้าย
- หัวตาขวา
- หัวตาซ้าย
- ปลายจมูกด้านขวา
- ปลายจมูกด้านซ้าย
- มุมปากด้านขวา
- มุมปากด้านซ้าย

เมื่อทำการเพิ่มผู้ใช้คนใหม่เข้าสู่ระบบ จำเป็นต้องมีการเก็บข้อมูลใบหน้าของผู้ใช้ เพื่อเก็บค่าลักษณะ ณ จุดดังกล่าวแต่ละจุดในรูปแบบเอกซ์เอ็มแอล (xml)

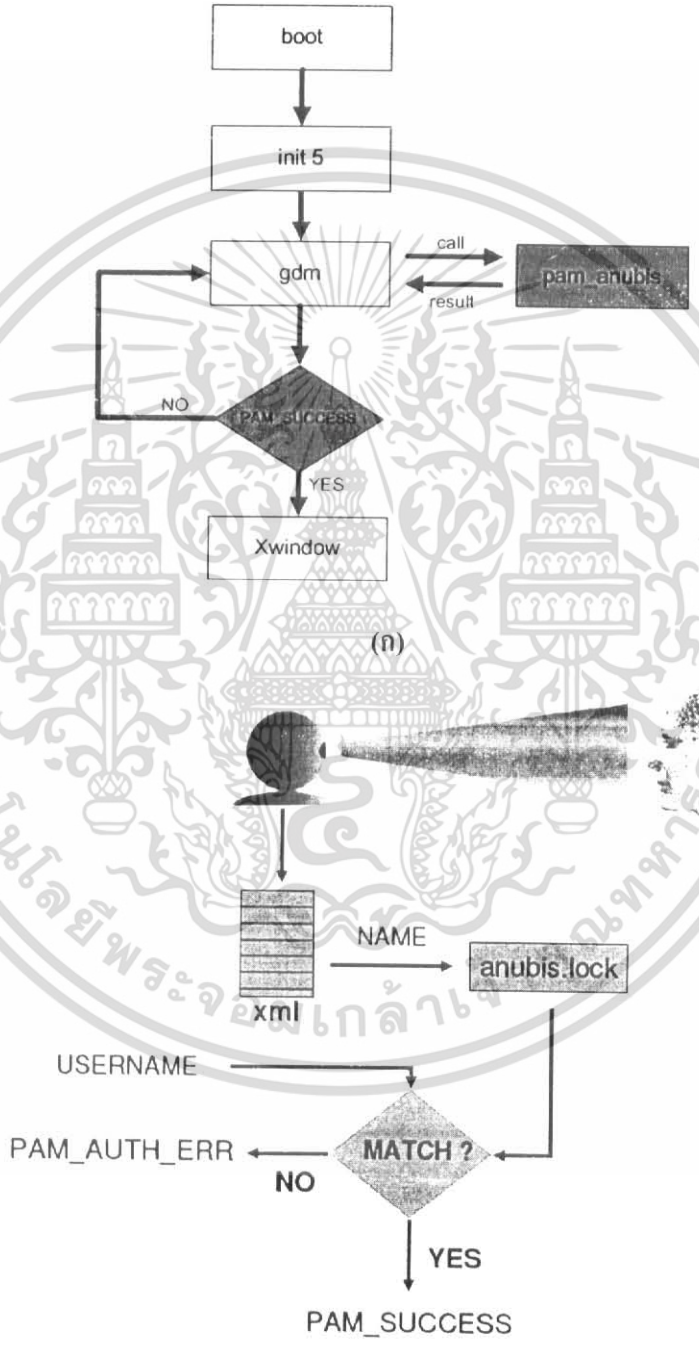
เมื่อมีการล็อกอินก็จะมีการตรวจสอบหาจุดเด่นบนใบหน้าของผู้ทำการล็อกอินด้วยตัวกรองเกเบอร์ แล้วนำข้อมูลที่ได้ตรวจสอบหาความคล้ายคลึงกันกับข้อมูลของใบหน้าของผู้ใช้ในระบบโดยนำหลักการของ Face Graph Matching ช่วยในการรู้จำใบหน้า

ทั้งนี้ในโครงงานได้กำหนดค่า เธรโชลด์ (Threshold) ที่ 0.8 หากการตรวจเทียบใบหน้าผู้ทำการล็อกอินกับใบหน้าของผู้ใช้ในระบบ มีค่าความคล้ายคลึง (similarity) สูงกว่าหรือเท่ากับ 0.8 จะถือว่าผู้ทำการล็อกอินคือผู้ใช้ในระบบคนดังกล่าว

บทที่ 3

การออกแบบซอฟต์แวร์

3.1 โครงสร้างซอฟต์แวร์ส่วนพิสูจน์ตน



รูปที่ 3.1 (ก) แสดงโครงสร้างซอฟต์แวร์การเรียกใช้มอดูลพิสูจน์ตน

รูปที่ 3.1 (ข) แสดงโครงสร้างซอฟต์แวร์ในการพิสูจน์ตนผู้ใช้

3.1.1 Input/Output Specification

Input Specification ข้อมูลรับเข้า คือ ชื่อบัญชีผู้ใช้ที่จะเข้าใช้งานระบบ และภาพใบหน้าของผู้ใช้คนนั้นซึ่งได้จากกล้องเว็บแคม

Output Specification ข้อมูลออก คือ Xwindow

3.1.2 functional Specification

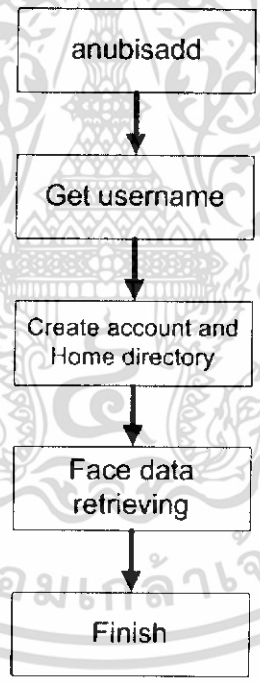
1. pam_anubis มอดูลที่ใช้ในการพิสูจน์ตน

pam_sm_authenticate() ฟังก์ชั่นหลักสำหรับการพิสูจน์ตนของมอดูล PAM

pam_get_user() ดึงค่าข้อมูลผู้ใช้ สำหรับการประมวลผล

pam_set_item() ตั้งค่าข้อมูลสำหรับการพิสูจน์ตน

3.2 โครงสร้างซอฟต์แวร์ส่วนเพิ่มชื่อบัญชีผู้ใช้



รูปที่ 3.2 แสดงโครงสร้างซอฟต์แวร์ส่วนการเพิ่มชื่อบัญชีผู้ใช้

3.2.1 Input/Output Specification

Input Specification ข้อมูลรับเข้า คือ ชื่อบัญชีผู้ใช้ที่จะเพิ่มเข้าสู่ระบบ และภาพใบหน้าของผู้ใช้คนนั้นซึ่งได้จากกล้องเว็บแคม

Output Specification ข้อมูลออก คือ ชื่อบัญชีผู้ใช้คนใหม่ถูกเพิ่มเข้ามาในระบบและข้อมูล ไดเรกทอรีของผู้ใช้ถูกเก็บในฐานข้อมูล

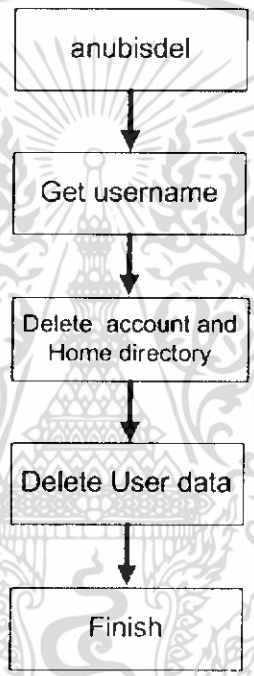
3.2.2 functional Specification

anubisadd

execl() เพื่อรันคำสั่ง adduser เพื่อเพิ่มผู้ใช้ในระบบและสร้าง home directory

getpwnam() เพื่อดึงค่าข้อมูลในไฟล์ /etc/passwd ของผู้ใช้คนดังกล่าว

3.3 โครงสร้างซอฟต์แวร์ส่วนลบชื่อบัญชีผู้ใช้



รูปที่ 3.3 แสดงโครงสร้างซอฟต์แวร์ส่วนการลบชื่อบัญชีผู้ใช้

3.3.1 Input/Output Specification

Input Specification ข้อมูลรับเข้า คือ ชื่อบัญชีผู้ใช้ที่จะลบออกจากระบบ

Output Specification ข้อมูลออก คือ ชื่อบัญชีผู้ใช้คนนั้น รวมถึงข้อมูลของผู้นั้นถูกลบจากระบบ

3.3.2 functional Specification

anubisdel

execl() เพื่อเรียกคำสั่ง deluser เพื่อลบผู้ใช้งานในระบบ

getpwnam() ดึงข้อมูลจากไฟล์ /etc/passwd เพื่อใช้ในการลบผู้ใช้ออกจากระบบ

3.4 อุปกรณ์ที่ใช้ในการพัฒนา

- Linux-PAM
- Logitech Quick Zoom web camera
- OpenCV (Opensource Computer Vision)
- C language
- Editor VI
- GNU C/C++ compiler
- ระบบปฏิบัติการ GNU/Linux (Debian 3.1) kernel version 2.6

กล้องเว็บแคม

ภาพที่ 3.4 กล้องเว็บแคม Logitech Quick Zoom

คุณสมบัติเฉพาะ

High-quality VGA sensor

Thin 2.1 metre USB cable

Manual focus

Video capture : up to 640 x 480 pixels

Still image capture : up to 640 x 480 pixels

Fram rate : up to 30 frames per second (with recommended system)

3.5 กลุ่มผู้ใช้โปรแกรม

กลุ่มผู้ใช้โปรแกรมที่เกี่ยวข้องนั้นสามารถจำแนกได้เป็นดังนี้ คือ

3.5.1 กลุ่มผู้ใช้งานอินุกซ์ทั่วไป ทั้งนี้เมื่อทำการล็อกอินเข้าระบบ ไม่จำเป็นต้องจดจำรหัสผ่านเช่นเดิม ทำให้การใช้งาน สะดวกขึ้น และมีความปลอดภัยกับระบบเพิ่มมากขึ้น

3.5.2 ผู้ดูแลระบบที่เป็นอินุกซ์ เนื่องจากสามารถเพิ่มและลบชื่อบัญชีผู้ใช้ในระบบได้ และการดูแล เรื่องความปลอดภัยในการล็อกอินเข้าใช้งานของผู้ใช้งานนั้น ก็จะมีประสิทธิภาพเพิ่มมากขึ้น ไม่ต้องกังวลการแอบอ้างนำรหัสผ่านของบุคคลอื่นมาใช้เพื่อผลประโยชน์อันหนึ่งอันใดก็ตาม

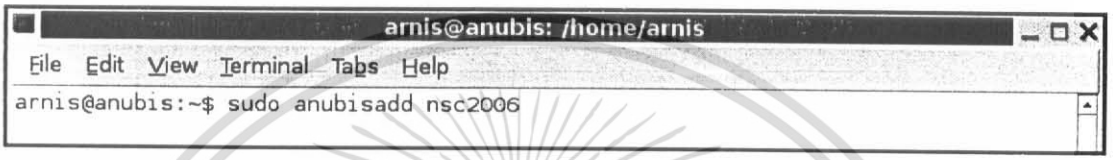
บทที่ 4

การทดลองและผลการทดลอง

4.1 การเพิ่มชื่อบัญชีผู้ใช้ในระบบ

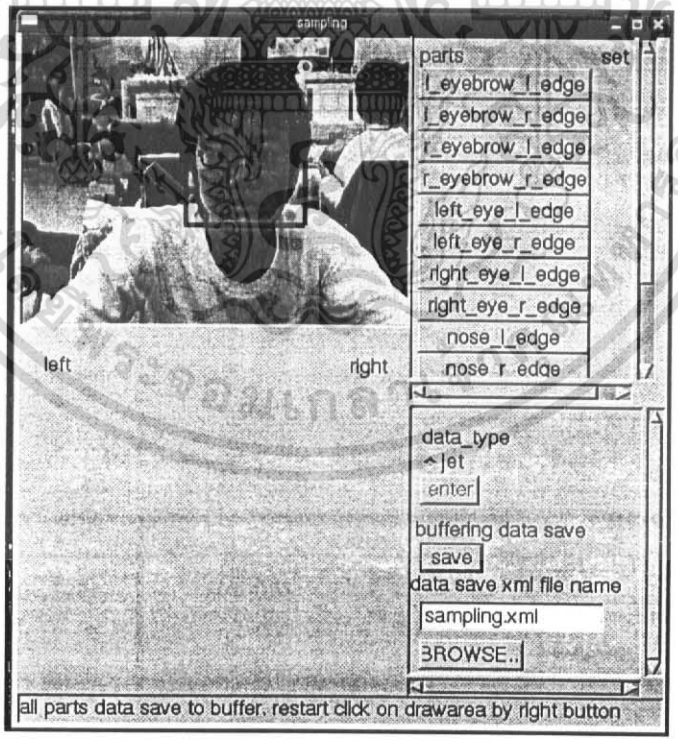
สำหรับการเพิ่มชื่อบัญชีผู้ใช้ในระบบนั้น ผู้ที่มีสิทธิ์ในการเพิ่มชื่อบัญชีผู้ใช้ในระบบนั้นจะมีเพียงผู้ดูแลระบบหรือ Administrator หรือ root ในระบบปฏิบัติการลินุกซ์

ระบบจะสแกนใบหน้าของผู้ใช้คนใหม่

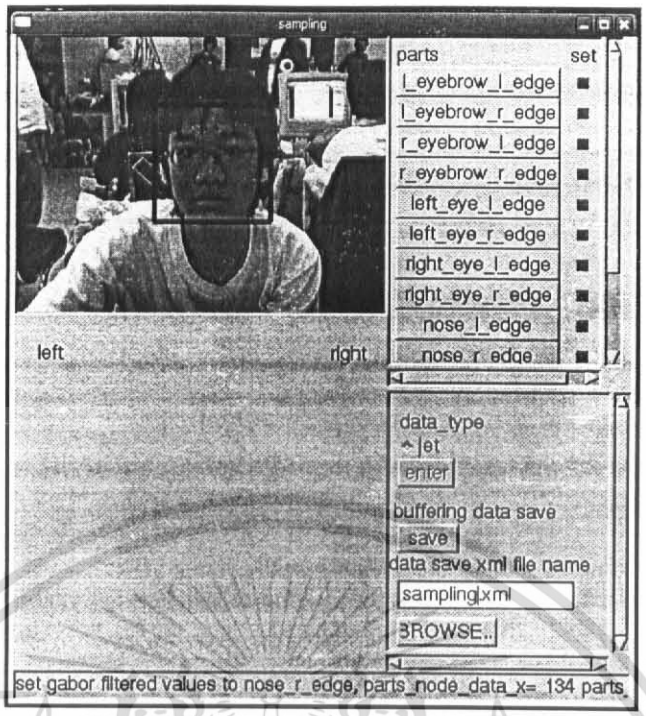


รูปที่ 4.1 แสดงการใช้คำสั่งเพิ่มชื่อบัญชีผู้ใช้

ดังรูปที่ 4.1 เป็นการใช้งานคำสั่งเพิ่มชื่อบัญชีผู้ใช้ในระบบ โดยพิมพ์คำสั่ง "sudo anubisadd" ตามด้วยชื่อผู้ใช้คนใหม่ที่จะเพิ่มเข้าไปในระบบ ระบบจะแสดงไดอะล็อกให้กำหนดตำแหน่งของจุดอ้างอิงที่กำหนดให้เพื่อใช้อ้างอิงในการล็อกอินครั้งต่อ ๆ ไป

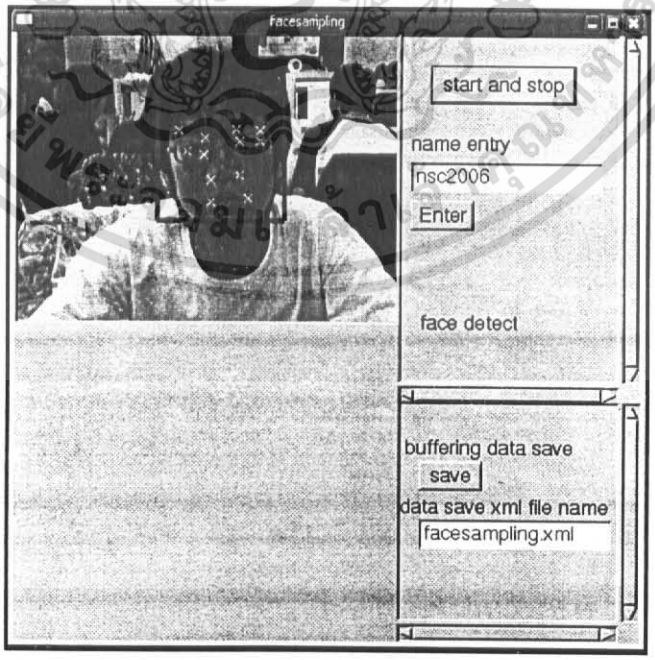


รูปที่ 4.2 แสดงไดอะล็อกก่อนทำการกำหนดตำแหน่งของจุดอ้างอิง



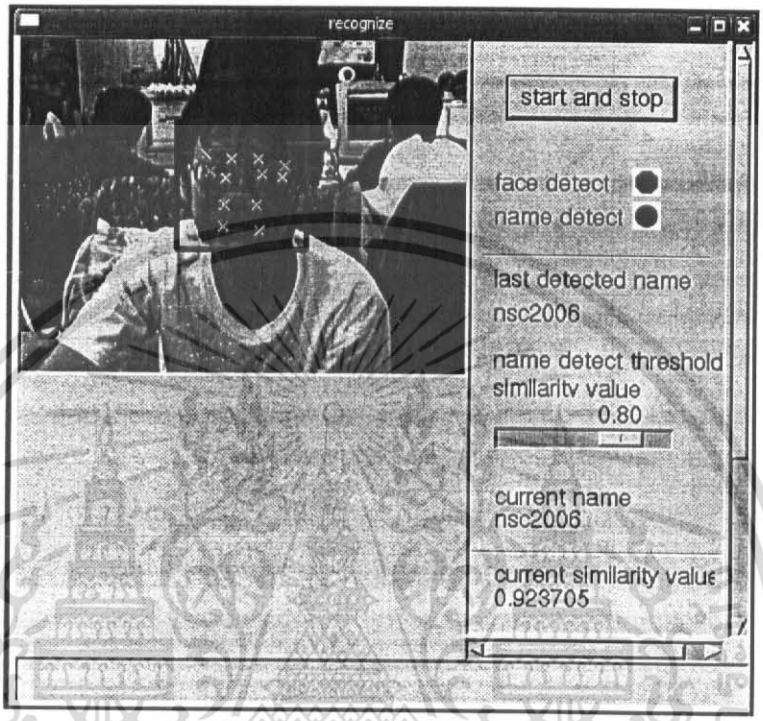
รูปที่ 4.3 แสดงไดอะล็อกหลังทำการกำหนดตำแหน่งของจุดอ้างอิง

เมื่อทำการกำหนดตำแหน่งของจุดอ้างอิงเรียบร้อยแล้วดังโดยจุดที่ได้ทำการกำหนดเรียบร้อยแล้วจะมีจุดสีเขียวขึ้นไว้รูปที่ 4-3 ก็ทำการบันทึกข้อมูลของผู้ใช้คนใหม่ลงในไฟล์ จากนั้นก็จะต้องทำการเทรนข้อมูลอีกเพื่อให้ได้ค่าเฉลี่ยในการนำมาเป็นข้อมูลอ้างอิง โดยไดอะล็อกที่จะใช้ในการเทรนข้อมูลแสดงดังรูปที่ 4-4



รูปที่ 4.4 แสดงไดอะล็อกสำหรับการเทรนข้อมูล

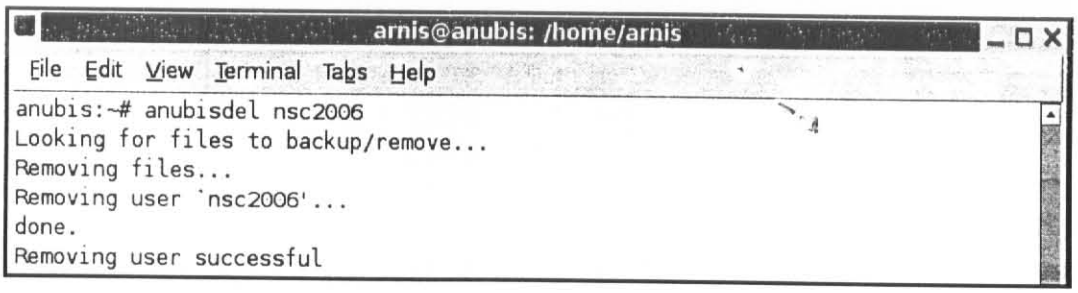
การเทรนข้อมูลทำได้โดยใส่ชื่อผู้ใช้คนใหม่ลงไป แล้วกดปุ่ม "start and stop" ให้ตำแหน่งของจุดอ้างอิงที่กำหนดไว้ในครั้งแรกนั้นตรงกับตำแหน่งที่ต้องการที่สุด (ตรงกับตำแหน่งที่กำหนดในครั้งแรกที่สุด) เพื่อให้เกิดความคลาดเคลื่อนน้อยที่สุด แล้วกดปุ่ม "start and stop" เพื่อบันทึกข้อมูลของจุดอ้างอิงของตำแหน่ง ณ เวลานั้น



รูปที่ 4.5 แสดงไดอะล็อกที่มีการเทรนข้อมูลแล้ว

4.2 การลบชื่อบัญชีผู้ใช้ในระบบ

การลบชื่อบัญชีผู้ใช้ในระบบ ผู้ที่มีสิทธิ์กระทำการดังกล่าวก็จะมีเพียงผู้ดูแลระบบเท่านั้น ระบบจะรับชื่อผู้ใช้ที่ต้องการลบและทำการลบแฟ้มข้อมูลต่าง ๆ ของผู้ใช้คนนั้น แสดงข้อความเมื่อเสร็จสิ้นกระบวนการลบชื่อบัญชีผู้ใช้ออกจากระบบ



รูปที่ 4.6 แสดงการใช้คำสั่งลบชื่อบัญชีผู้ใช้

4.3 การตรวจสอบผู้ใช้

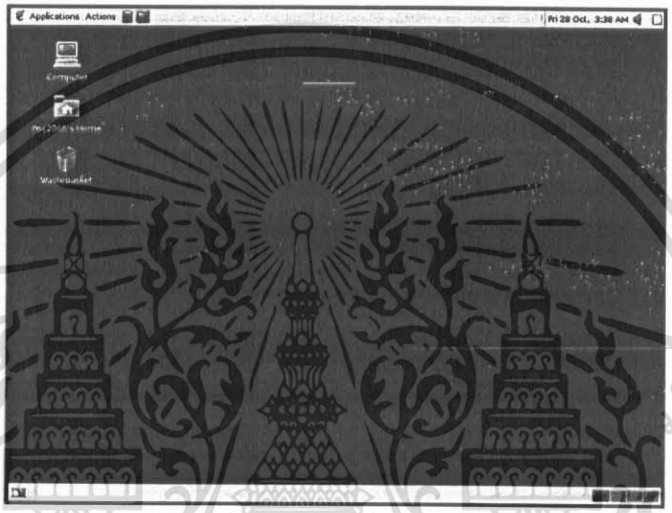
ในการตรวจสอบผู้ใช้ มีการทดลองดังต่อไปนี้

ผู้ใช้งานพิมพ์ชื่อบัญชีผู้ใช้ของตนเอง

กล้องจะทำการบันทึกใบหน้าของผู้ใช้และนำไปเปรียบเทียบกับข้อมูลใบหน้าของชื่อบัญชีผู้ใช้งานที่ได้รับ

แสดงผลการตรวจสอบ

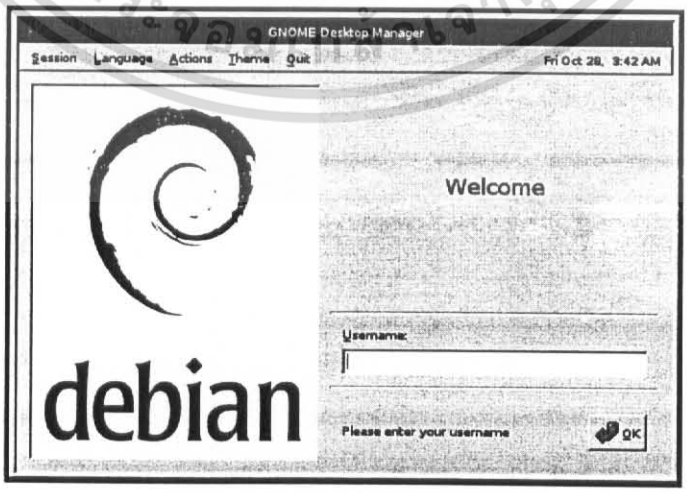
4.3.1 การตรวจสอบใบหน้าผ่าน



รูปที่ 4.7 แสดงผลการตรวจสอบใบหน้าผ่าน

เมื่อผลการตรวจสอบใบหน้าผ่านแล้วระบบก็จะให้เชลล์ (shell) กับผู้ใช้คนดังกล่าวในการใช้งานต่อไป

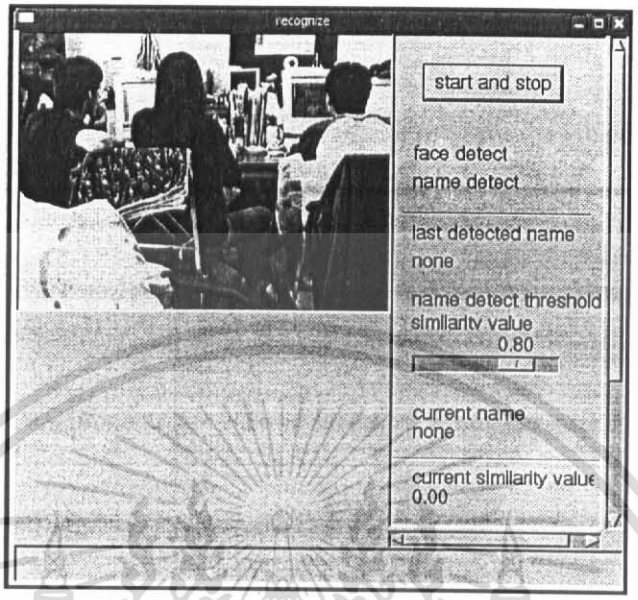
4.3.2 การตรวจสอบใบหน้าไม่ผ่าน



รูปที่ 4.8 แสดงผลการตรวจสอบใบหน้าไม่ผ่าน

4.3.3 การตรวจสอบโดยไม่มีใบหน้าบุคคล

หากไม่มีใบหน้าของบุคคลใด ๆ ก็จะไม่สามารถตรวจสอบได้ดังรูปที่ 4-9

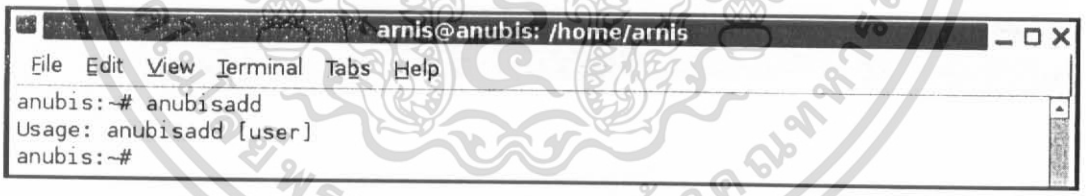


รูปที่ 4.9 แสดงการตรวจสอบที่ไม่มีใบหน้าบุคคล

4.4 การใช้งานที่ไม่ถูกต้อง

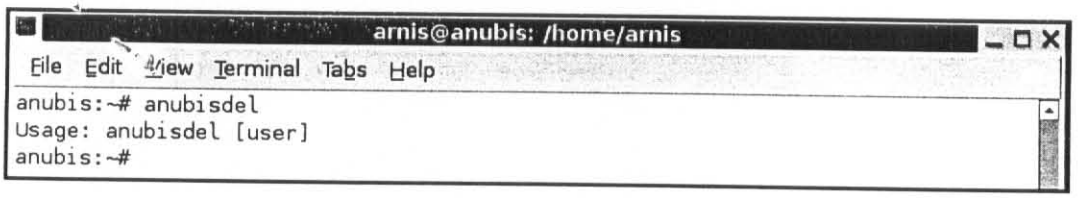
การใช้งานของผู้ดูแลระบบที่ไม่ถูกต้อง จะมีโอกาสเกิดขึ้นได้สองกรณีคือ

4.4.1 เพิ่มชื่อบัญชีผู้ใช้งานในระบบไม่ถูกต้อง แสดงผลดังนี้



รูปที่ 4.10 แสดงผลของคำสั่งเพิ่มผู้ใช้งานที่ไม่ถูกต้อง

4.4.2 ลบชื่อบัญชีผู้ใช้งานในระบบไม่ถูกต้อง แสดงผลดังนี้

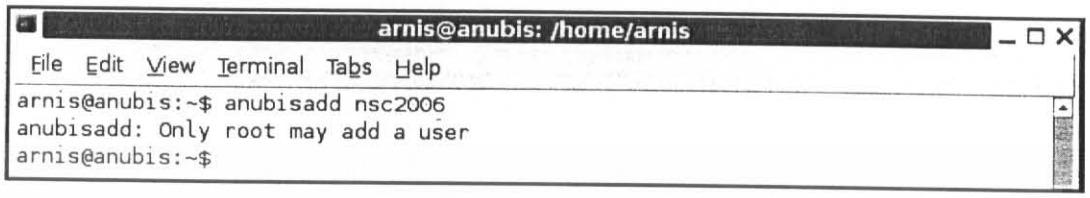


รูปที่ 4.11 แสดงผลของคำสั่งลบผู้ใช้งานที่ไม่ถูกต้อง

4.5 การเพิ่มหรือลบชื่อบัญชีผู้ใช้โดยไม่มีสิทธิ์ของผู้ดูแลระบบ

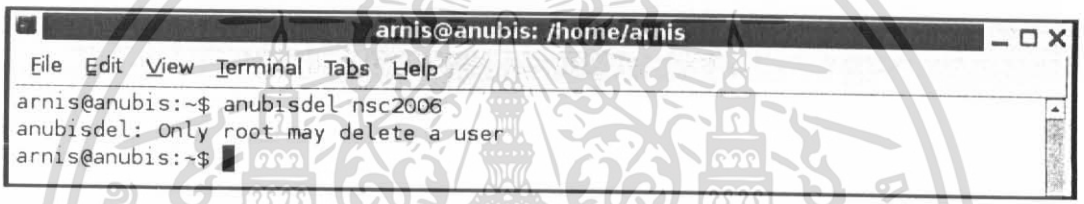
ในการเพิ่มหรือลบชื่อบัญชีผู้ใช้ในระบบโดยไม่มีสิทธิ์ของผู้ดูแลระบบในการกระทำดังกล่าวระบบจะแสดงผลดังนี้

4.5.1 การใช้คำสั่งเพิ่มชื่อผู้ใช้โดยไม่มีสิทธิ์ของผู้ดูแลระบบ



รูปที่ 4.12 แสดงการเพิ่มชื่อบัญชีผู้ใช้โดยไม่มีสิทธิ์ของผู้ดูแลระบบ

4.5.1 การใช้คำสั่งเพิ่มชื่อผู้ใช้โดยไม่มีสิทธิ์ของผู้ดูแลระบบ



รูปที่ 4.13 แสดงการลบชื่อบัญชีผู้ใช้โดยไม่มีสิทธิ์ของผู้ดูแลระบบ

4.6 การใช้งานระบบโดยใช้ชื่อบัญชีผู้ใช้ที่ไม่มีในระบบ

หากมีการล็อกอินเพื่อเข้าใช้งานระบบโดยใช้ชื่อบัญชีผู้ใช้ที่ไม่มีอยู่จริง ระบบจะแสดงผลดังนี้ เพื่อให้ผู้ใช้พิมพ์ชื่อใหม่

รูปที่ 4.14 แสดงการล็อกอินโดยชื่อผู้ใช้ที่ไม่มีในระบบ

4.7 ผลการทดลองหาความผิดพลาดในการตรวจสอบผู้ใช้

การทดสอบการล็อกอินด้วยผู้ใช้ในระบบ ทั้งหมด 10 คนปรากฏผลดังตารางต่อไปนี้

ตารางที่ 4.1 แสดงประสิทธิภาพในการตรวจสอบผู้ใช้

ผู้ล็อกอิน	ชื่อผู้ใช้ที่แสดงผล	ค่า similarity สูงสุด			ค่าเฉลี่ย
		ครั้งที่1	ครั้งที่2	ครั้งที่ 3	
user1	user1	0.918	0.850	0.923	0.897
user2	user2	0.780	0.802	0.821	0.801
user3	user3	0.883	0.902	0.855	0.880
user4	user1	0.771	0.811	0.860	0.814
user5	user5	0.681	0.693	0.641	0.671
user6	user6	0.707	0.681	0.743	0.710
user7	user7	0.735	0.784	0.741	0.753
user8	user8	0.851	0.820	0.789	0.820
user9	user9	0.837	0.780	0.808	0.808
user10	user10	0.820	0.800	0.824	0.814

จากข้อมูลข้างต้น เมื่อเพิ่มผู้ใช้ให้กับระบบ และทำการทดสอบว่าแอพลิเคชันสามารถแสดงผลชื่อผู้ใช้ได้ตรงกับผู้ล็อกอินหรือไม่อย่างไร

สามารถตรวจพบชื่อผู้ใช้ได้ถูกต้อง คิดเป็นร้อยละ 90

ค่าฉลี่ยของค่าความคล้ายคลึง (similarity) สูงสุด คิดเป็นร้อยละ 79.68

บทที่ 5
บทสรุปและวิจารณ์

5.1 บทสรุป

จากผลการทดลองที่ได้พบว่าแอพลิเคชันสามารถพิสูจน์ตนผู้ใช้งานระบบได้โดยสามารถใช้ใบหน้าในการพิสูจน์ตนได้ ผู้ใช้งานไม่จำเป็นต้องจดจำรหัสผ่านหรือพกพาบัตรหรือกุญแจเพื่อใช้ในการพิสูจน์ตน ผู้ดูแลระบบเพิ่มและลบผู้ใช้งานได้ และทำให้ระบบมีความปลอดภัยเพิ่มขึ้นเนื่องจากลดการแอบอ้างนำรหัสผ่านของบุคคลอื่นมาแอบอ้างเพื่อการเข้าใช้งาน อีกทั้งเพิ่มทางเลือกในการพิสูจน์ตนให้กับระบบด้วย

5.2 วิจารณ์สิ่งที่ได้จากโครงงาน

การพิสูจน์ตนด้วยการใช้ กระบวนการ PAM นั้นเกิดความสะดวกกับระบบเองและผู้ดูและระบบที่สามารถจัดการกระบวนการในการพิสูจน์ตนได้ ตามความต้องการและตามความเหมาะสม โดยสามารถเลือกใช้มอดูลที่มีความแตกต่างกันได้โดยไม่ต้องยึดติดกับรูปแบบใดรูปแบบหนึ่ง อีกทั้งการเปลี่ยนแปลงกระบวนการในการพิสูจน์ตนนั้น สามารถทำได้ง่ายโดยไม่ต้องทำการเปลี่ยนแปลงโค้ดของ แอพลิเคชั่น ที่มีการพิสูจน์ตน และวิธีการทางชีวมาตรนั้นก็เป็นวิธีที่มีความแม่นยำ ทั้งนี้ขึ้นอยู่กับวิธีการในการนำข้อมูลชีวมาตรมาประมวลผล หรืออัลกอริทึมที่ใช้ด้วย แต่โดยทั่วไปแล้ววิธีการทางชีวมาตรก็มีการนำไปประยุกต์ใช้กันหลายองค์กร นอกจากวิธีการใช้ใบหน้าแล้ว ยังมีรูปแบบอื่น ๆ อีกที่สามารถนำมาใช้งานได้

5.3 ปัญหา อุปสรรค และแนวทางแก้ไข

1. เนื่องด้วยเทคโนโลยีชีวมาตรนั้น มีการใช้งานกันในระดับเฉพาะกลุ่ม แม้จะเป็นที่รู้จักกันอย่างกว้างขวางก็ตาม จึงมีข้อจำกัดที่เกิดขึ้นในการนำเทคโนโลยีชีวมาตรมาใช้กับกระบวนการในแบบอื่น ๆนอก เหนือจากที่มีการใช้งานกันในปัจจุบัน

2. เอกสารที่เกี่ยวข้องในส่วนของ PAM นั้นนับได้ว่ายังมีไม่มาก และที่มีอยู่นั้นก็อาจจะยังไม่ได้ถือเป็นข้อมูลเชิงลึกมาก

3. เอกสารที่เกี่ยวข้องในส่วนของ Face Recognize โดยส่วนใหญ่จะมีการนำทฤษฎีทางคณิตศาสตร์ชั้นสูงมาใช้ จึงทำให้ยากต่อการทำความเข้าใจในหลาย ๆ ส่วน

4. การสร้างแซร์ไลบราลี่ หรือมอดูลนั้นหากเกิดปัญหาซึ่งทำการดีบักเพื่อหาจุดผิดพลาดยาก จึงเสียเวลาแก้ไขระยะหนึ่ง ซึ่งบางครั้งต้องทำการรีสตาร์ทเครื่องจึงกลับมาเป็นปกติ

5. การล็อกอินของผู้ใช้งานจำเป็นจะต้องมีลักษณะใบหน้าที่เหมือนเดิมหากยิ้ม หรือหัวเราะซึ่งทำให้องค์ประกอบต่างๆ บนใบหน้าเปลี่ยนแปลงไปนั้น ก็จะส่งผลต่อประสิทธิภาพของระบบแม้จะเป็นบุคคล คนเดียวกันก็ตาม

5.4 แนวทางในการพัฒนา

ดังที่ได้กล่าวไว้แล้วว่า เทคโนโลยีทางชีวมาตรนั้น เป็นวิธีการที่ได้รับความนิยม และมีประสิทธิภาพ แต่กระบวนการในการนำเทคโนโลยีชีวมาตรมาประยุกต์ใช้งาน ยังไม่มีความหลาก หลายมากนัก ทั้งนี้ก็เนื่องมา จากข้อจำกัดในด้านต่างๆ ทั้งด้านเทคโนโลยีซึ่งกระบวนการที่ทำงานร่วมกับเทคโนโลยีชีวมาตรอาจยังไม่อยู่ในระดับที่สูงเพียงพอที่จะนำมาใช้งานร่วมกันได้ หรือด้านเงินทุนซึ่งเทคโนโลยีชีวมาตรบางรูปแบบนั้นจำเป็นต้องมีค่าใช้จ่ายในปริมาณที่สูง

โครงงาน การพิสูจน์ตนด้วยชีวมาตรนี้ เป็นโครงงานที่พัฒนาต่อจากโครงงานระบบต้นแบบการล็อกอินเข้าลินุกซ์ ด้วยลายนิ้วมือ ซึ่งได้พัฒนารูปแบบของการพิสูจน์ตนจากลายนิ้วมือ มาเป็นการใช้ใบหน้าซึ่งต่างก็เป็นเทคโนโลยีชีวมาตรเช่นกัน และแนวทางในการพัฒนาต่อนั้นนอกสามารถทำได้โดยอาจเปลี่ยนจากรูปแบบทั้งสอง เป็นรูปแบบอื่นๆ ทั้ง เสียง จังหวะการพิมพ์ ลายเซ็น ม่านตา หรือเทคโนโลยีชีวมาตรรูปแบบอื่นๆ อีก แม้กระทั่งมีการใช้งานมากกว่าหนึ่งรูปแบบในระบบก็ตาม หากมีความเหมาะสมแล้ว ก็จะส่งผลดีทั้งต่อความปลอดภัยของระบบเอง และความสะดวกในการใช้งานของผู้ใช้ด้วย

เนื่องด้วยระบบ หรือรูปแบบทางชีวมาตรนั้นมีหลายรูปแบบ หากมีการพัฒนาในขั้นต่อไป โดยใช้รูปแบบทางชีวมาตรอื่นๆ หรือนำไปประยุกต์ใช้กับการล็อกอินของแอพลิเคชันอื่น รวมไปถึงการนำไปประยุกต์ใช้กับเทคโนโลยีที่ต่างออกไป ก็จะเกิดประโยชน์สูงขึ้น

บรรณานุกรม

เอกสารอ้างอิงที่เป็นปริญญานิพนธ์

[1] ภรายุทธ วังวรัญญูและสุจิตรา ไพบูลย์วาณิชย์ " ระบบพิสูจน์ตน" ปริญญานิพนธ์วิศวกรรมศาสตรบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง 2543

[2] กีรพัฒน์ อรุณรังษีและเกรียงไกร นิตรานนท์ "ระบบต้นแบบในการล็อกอินเข้าลีนุกซ์ด้วยลายนิ้วมือ" ปริญญานิพนธ์วิศวกรรมศาสตรบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง 2547

เอกสารอ้างอิงที่เป็นหนังสือ

[3] Charlie Kaufman ,Radia Perlman and Mike Speciner 2002.Network Security Private Communication in a Public world ,USA,Prentice Hall PTR

[4] Charlie Lai 1996.Makin Login Services Independent of Authentication Technologies

เอกสารอ้างอิงที่เป็นเว็บไซต์

[4] "User Authentication HOWTO" [Online].Available: http://www.linux.com/howtos/User-Authentication-HOWTO/x115.shtml

[5] "FOCUS on Sun and Linux: Pluggable Authentication Modules, Part II" [Online].Available: http://www.securityfocus.com/infocus/1390

[6] "Pluggable Authentication Modules" [Online].Available: http://en.wikipedia.org/wiki/Pluggable_authentication_modules

[7] "Sample PAM Application" [Online].Available: http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/pam-sample-appl.html

[8] "Sample PAM Module" [Online].Available: http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/pam-sample-module.html

[9] "pam_sm_authenticate" [Online].Available: http://www.opengroup.org/onlinepubs/008329799/pam_sm_authenticate.htm

[10] "pam_tim" [Online].Available: http://www.opensource.apple.com/darwinsource/10.3/pam_modules-13/pam_tim/pam_tim.c

[11] "Biometricts A Journal of the International Biometric Society" [Online].Available: http://tibs.org/biometrics/

[12] "Biometrics Consortium" [Online].Available: http://www.biometrics.org

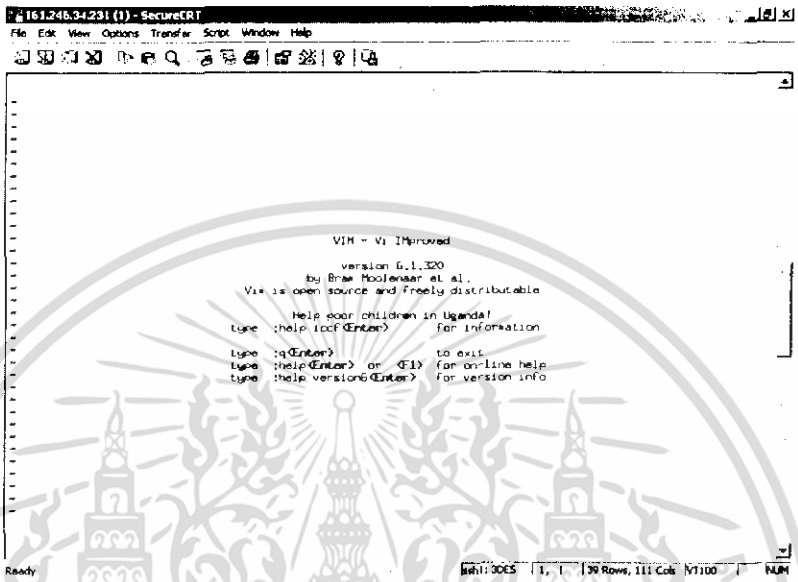
[13] "International Biometrics" [Online].Available : http://www.biometricgroup.com

[14] "International Association of Biometrics(iAfB)" [Online].Available :

http://www.iafb.org.uk

ภาคผนวก

Editor VI



การทำงาน ของ editor ชนิดนี้แบ่งเป็น 2 โหมด

1. โหมดคำสั่ง (command mode)
2. โหมดแก้ไขข้อความ (editing mode)

สามารถทำการสลับการทำงานระหว่าง 2 โหมดได้โดย กดปุ่ม ESC หรือ <Ctrl + [>
(ในกรณีที่ไม่แน่ใจว่าอยู่ในโหมดคำสั่งหรือไม่สามารถกด ESC ซ้ำได้หากอยู่ในโหมดคำสั่งอยู่แล้วจะมีเสียงบี๊บ เกิดขึ้น)

การใช้งาน

เรียก ใช้ vi ได้โดยตรง จาก shell prompt

$ vi

รูปแบบ

$ vi [file name] สร้างไฟล์ใหม่หรือเรียกไฟล์ที่มีอยู่แล้วมาแก้ไข

การใส่ข้อความ

การเข้า อิดิเตอร์ครั้งแรกเป็นการเข้าสู่โหมดคำสั่ง หากต้องการเขียนข้อความจากอิดิเตอร์ ต้องใช้คำสั่ง insert โดยการกด i หรือคำสั่ง append โดยการกด a จึงจะสามารถเขียนข้อความลงไปได้

A	แก้ไขข้อความแบบต่อท้ายบรรทัด
a	แก้ไขข้อความแบบต่อเคอร์เซอร์
I	แก้ไขข้อความแบบแทรกต้นบรรทัด
i	แก้ไขข้อความแบบแทรกที่เคอร์เซอร์
O	แก้ไขข้อความแบบแทรกบรรทัดก่อนบรรทัดปัจจุบัน
o	แก้ไขข้อความแบบแทรกบรรทัดต่อจากบรรทัดปัจจุบัน

การควบคุมเคอร์เซอร์

ขณะอยู่ในโหมดแก้ไขข้อความจะไม่สามารถทำการควบคุมเคอร์เซอร์ได้ ดังนั้นจึงต้องทำการเปลี่ยนไปอยู่ในโหมดคำสั่งก่อนจึงจะสามารถควบคุมได้ การควบคุมจะใช้คีย์พื้นฐาน 4 คีย์ คือ

h	เลื่อนไปทางซ้าย
l	เลื่อนไปทางขวา
k	เลื่อนขึ้นข้างบน
j	เลื่อนลงข้างล่าง

การลบข้อความ

ต้องอยู่ในโหมดคำสั่งเช่นกัน

x	ลบข้อความที่เคอร์เซอร์ 1 ตัว
X	ลบข้อความหน้าเคอร์เซอร์ 1 ตัว
dd	ลบบรรทัดที่เคอร์เซอร์อยู่ทั้งบรรทัด
D	ลบข้อความตั้งแต่ตำแหน่งเคอร์เซอร์ไปจนสุดบรรทัด

สามารถ คัดลอกข้อความได้โดยใช้คำสั่ง yy คัดลอกบรรทัดปัจจุบันทั้งบรรทัดและวางยังตำแหน่งที่ต้องการโดยคำสั่ง p (ต่อจากบรรทัดปัจจุบัน) หรือ P (หน้าบรรทัดปัจจุบัน)

การค้นหา

/ ค้นหาคำจากเคอร์เซอร์ไปจนถึงท้ายแฟ้มข้อมูล

? ค้นหาคำจากเคอร์เซอร์ไปจนถึงต้นแฟ้มข้อมูล

n ค้นหาต่อไปในทิศทางเดิม

N ค้นหาต่อไปในทิศทางตรงข้ามจากทิศทางเดิม

ในโหมดคำสั่งยังแบ่งเป็นอีก 2 โหมด

คือโหมดคำสั่งทั่วไปดังที่กล่าวมาแล้วและโหมดคำสั่ง extended

ในโหมดคำสั่ง ex มักขึ้นต้นด้วยเครื่องหมาย ':'

:q ออกจากโปรแกรม vi หากข้อมูลได้รับการแก้ไขแต่ยังไม่ได้จัดเก็บ vi จะแจ้งเตือนและยังไม่ให้ออกจากโปรแกรม

:q! ออกจากโปรแกรม vi โดยไม่มีการจัดเก็บข้อมูล แม้ข้อมูลถูกแก้ไขก็ตาม

:w จัดเก็บข้อมูลทับไฟล์ชื่อเดิม

:w [file name] จัดเก็บข้อมูลในไฟล์ใหม่โดยการระบุชื่อไฟล์ลงไป

:wq! จัดเก็บข้อมูลทับชื่อเดิมแล้วออกจากโปรแกรม

:x! จัดเก็บข้อมูลทับชื่อเดิมแล้วออกจากโปรแกรม

**** การใช้คำสั่งในโหมด extended เช่น คำสั่ง :wq! เพียงเข้าสู่โหมดคำสั่งแล้วพิมพ์ ':' จากนั้นก็พิมพ์ 'wq!' ได้เลยโดยไม่ต้องพิมพ์ ':' ซ้ำอีกครั้ง ****