ระบบรักษาความปลอดภัยผ่านเครือข่ายอินเตอร์เน็ต พร้อมทั้งระบุตัวบุคคล

Security System Via Internet with People Identification System

นายธนพงษ์ ชื่นอุระจิตร

THANAPONG CHUENURAJIT

นายธนภัทร์ ชำนาญธรรม

TANAPAT CHAMNANTHAM

นายธานินทร์ โสภา

TANIN SOPA

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2553

Security System Via Internet with People Identification System

THANAPONG CHUENURAJIT

TANAPAT CHAMNANTHAM

TANIN SOPA

THIS THESIS IS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

BACHELOR OF ENGINEERING IN INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

ACADEMIC YEAR 2010

หัวข้อปริญญานิพนธ์	ระบบรักษาความปลอดภัยผ่านเครือข่ายอินเตอร์เน็ตพร้อมทั้งระบุตัวบุคคล	
รายชื่อนักศึกษา	นายธนพงษ์ ชื่นอุระจิตร	รหัสนักศึกษา 50010605
	นายธนภัทร์ ชำนาญธรรม	รหัสนักศึกษา 50010617
	นายธานินทร์ โสภา	รหัสนักศึกษา 50010687
ปริญญา	วิศวกรรมศาสตรบัณฑิต	
สาขาวิชา	วิศวกรรมสารสนเทศ	
พ.ศ.	2553	
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ดร. พนารัตน์ เชิญถนอมวงศ์	

ปริญญานิพนธ์ฉบับนี้ ได้รับการอนุมัติให้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรวิศวกรรมศาสตรบัณฑิต คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

.....

(ดร. พนารัตน์ เชิญถนอมวงศ์)

อาจารย์ผู้ควบคุมปริญญานิพนธ์

หัวข้อปริญญานิพนธ์	ระบบรักษาความปลอดภัยผ่านเครือข่ายอินเตอร์เน็ตพร้อมทั้งระบุตัวบุคคล		
รายชื่อนักศึกษา	นายธนพงษ์	ชื่นอุระจิตร	รหัสนักศึกษา 50010605
	นายธนภัทร์	ชำนาญธรรม	รหัสนักศึกษา 50010617
	นายธานินทร์	โสภา	รหัสนักศึกษา 50010687
ปริญญา	วิศวกรรมศาสตรบัณฑิต		
สาขาวิชา	วิศวกรรมสารสนเทศ		
พ.ศ.	2553		
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ดร. พนารัตน์ เชิญถนอมวงศ์		

บทคัดย่อ

ปัจจุบันการติดต่อสื่อสารและประยุกต์ใช้งานบนเครือข่ายอินเตอร์เน็ตมีความหลากหลายและใช้งานครอบคลุมกว้างขวาง โดยอินเตอร์เน็ตได้เข้ามามีบทบาททางด้านงานการควบคุมต่างๆ เนื่องจากเราสามารถนำคุณสมบัติของอินเตอร์เน็ตมาประยุกต์ใช้งานเพื่อควบคุมเครื่องจักรจากสถานที่ที่อยู่ห่างไกลผ่านทางเครือข่ายอินเตอร์เน็ต โดยไม่จำเป็นที่ผู้ควบคุมต้องทำงานในสถานที่ที่เครื่องมือติดตั้งอยู่ จึงเป็นที่มาในการสร้างโครงงานชิ้นนี้ กล่าวคือโครงงานที่ได้พัฒนา ระบบรักษาความปลอดภัยผ่านเครือข่ายอินเตอร์เน็ตพร้อมทั้งระบุตัวบุคคล โดยการทำงานหลักจะเป็นการติดต่อกับกล้องโดยควบคุมการบังคับทิศทางของกล้องผ่านเครือข่ายอินเตอร์เน็ต และทำการรับข้อมูลภาพที่ได้จากการถ่ายจากกล้องมาทำการตรวจสอบเพื่อระบุตัวบุคลว่าเป็นผู้ที่ได้รับอนุญาตให้เข้ามาใช้งานในพื้นที่นั้นๆหรือว่าเป็นผู้บุกรุก ดังนั้นเราก็สามารถที่จะตรวจสอบดูเหตุการณ์ต่างๆที่อยู่ในบริเวณนั้นโดยที่ผู้ควบคุมอยู่ที่อื่น พร้อมทั้งยังได้มีการนำเซนเซอร์ตรวจจับการเคลื่อนไหวมาใช้เพื่อตรวจสอบผู้บุกรุก รวมทั้งพัฒนาระบบการแจ้งเตือนไปยังโทรศัพท์มือถือของผู้ควบคุมเมื่อมีการบุกรุกเข้ามาในระบบ ซึ่งเราสามารถนำเอาหลักการเบื้องต้นนี้ไปประยุกต์ใช้งานในด้านการรักษาความปลอดภัยหรืองานที่ต้องการตรวจสอบเหตุการณ์ที่อยู่ห่างไกลออกไป

Thesis Title	Security System Via Internet with People Identification System	
Student	Mr. Thanapong Chuenurajit	Student ID. 50010605
	Mr. Tanapat Chamnantham	Student ID. 50010617
	Mr. Tanin Sopa	Student ID. 50010687
Degree	Bachelor of Engineering	
Program	Information Engineering	
Year	2010	
Thesis Advisor	Dr. Panarat Cherntanomwong	

ABSTRACT

Nowadays, applications of communication and internet have been used in a variety of fields. As known, internet is an important role in the control system, especially the system needed to be remotely controlled where the controller / or the officer does not need to be in place of the control system. Therefore, in the project, the security system via internet with people identification system is developed. The main part is to control the security camera via internet and then the picture taken from the camera are identified that whether the people in the picture are in the system or not. Additionally, the movement sensors are used to detect the attacker. Moreover, the alarm SMS system is developed to send a short message to the officer if the system found the attacker. This system can be used in applications of security or remotely monitoring and controlling system.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ ได้ดำเนินการจนสำเร็จลุล่วงได้ด้วยดี เพราะความร่วมมือของคณะผู้จัดทำ และความกรุณาจาก ดร.พนารัตน์ เชิญถนอมวงศ์ อาจารย์ที่ปรึกษา ผู้ซึ่งให้การสนับสนุน ชี้แนวทางให้คำปรึกษาอย่างดีมาโดยตลอด และขอขอบคุณอาจารย์ทุกๆท่านที่คอยอบรมสั่งสอน และให้ความรู้ หากขาดบุคคลดังกล่าวแล้ว คณะผู้จัดทำคงไม่สามารถที่จะทำชิ้นงานนี้สำเร็จลงได้

ขอขอบคุณสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมสารสนเทศ ที่ได้เอื้อเฟื้อสถานที่ ในการจัดทำปริญญานิพนธ์ และขอบคุณเพื่อนๆ พี่ๆ น้องๆ ทุกคนที่คอยเป็นกำลังกาย กำลังใจในการทำงาน

ขอขอบพระคุณบุคคลที่สำคัญที่สุด นั่นคือ บิดา มารดา และบุคคลในครอบครัวซึ่งได้ดูแลเอาใจใส่ คอยอบรมสั่งสอน พร้อมทั้งให้โอกาสในการศึกษาอย่างเต็มที่ ให้กำลังใจและความรักเสมอมา

คุณค่าและประโยชน์อันพึงมีจากปริญญานิพนธ์ฉบับนี้ คณะผู้จัดทำขอมอบแด่ผู้มีพระคุณทุกท่าน ทั้งที่ได้เอ่ยนาม และมิได้เอ่ยนาม สุดท้ายนี้หวังเป็นอย่างยิ่งว่าปริญญานิพนธ์ฉบับนี้คงจะเป็นแนวทางและเป็นประโยชน์สำหรับผู้ที่สนใจ เพื่อเป็นการนำไปใช้หรือประยุกต์ใช้งานต่อไป

คณะผู้จัดทำรู้สึกซาบซึ้งและขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

คณะผู้จัดทำ

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

รูปที่ หน้า

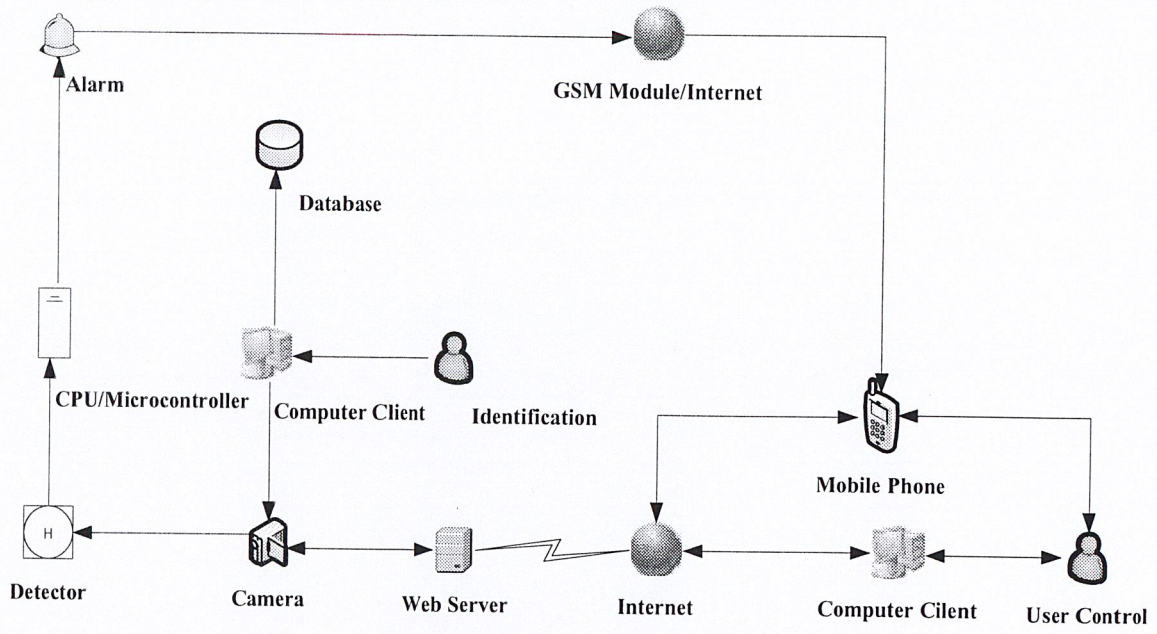
สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 แนวคิดและที่มาของปัญหา

เนื่องจากเทคโนโลยีในปัจจุบัน ได้มีการพัฒนาไปอย่างต่อเนื่อง เพื่อตอบสนองต่อความต้องการของผู้ใช้ที่ต้องการความสะดวกสบาย และความปลอดภัยในชีวิตและทรัพย์สิน เทคโนโลยีอย่างหนึ่งที่ได้มีการพัฒนาอยู่อย่างต่อเนื่องในปัจจุบันก็คือ เทคโนโลยีกล้องวงจรปิด (CCTV) ซึ่งเป็นเทคโนโลยีที่นำมาใช้ในการรักษาความปลอดภัย โดยกล้องวงจรปิดจะทำการส่งสัญญาณภาพจากกล้องวงจรปิด ที่ได้ทำการติดตั้งไว้ในจุดต่างๆ มายังจอรับภาพที่ได้ติดตั้งอยู่ในห้องควบคุม โดยประโยชน์ของกล้องวงจรปิดก็คือ เพื่อตรวจการณ์ สังเกตการณ์การเคลื่อนไหวและสิ่งผิดปกติในบริเวณที่ต้องการตรวจจับ ซึ่งสามารถที่จะป้องกันเหตุร้ายที่อาจเกิดขึ้นในอนาคต รวมทั้งยังช่วยในการจับคนร้ายหรือเป็นหลักฐานช่วยในการยืนยันการทำคดี ซึ่งในการตรวจสอบสังเกตการณ์การเคลื่อนไหวจากกล้องวงจรปิดนั้นมีการจำกัดไว้ว่าต้องดูภายในห้องควบคุมที่มีการติดตั้งจอภาพไว้ ซึ่งไม่ได้รับความสะดวกสบาย และอาจไม่ทันต่อเหตุการณ์ที่กำลังเกิดขึ้น ดังนั้นโครงงานนี้จึงได้มีการพัฒนากล้องวงจรปิด (CCTV) ที่สามารถติดตามสังเกตการณ์การเคลื่อนไหวในสถานที่ที่ต้องการได้ทุกที่ทุกเวลา โดยสามารถสังเกตการณ์และควบคุมกล้องผ่านเครือข่ายอินเตอร์เน็ตบนเครื่องคอมพิวเตอร์ พร้อมทั้งเพิ่มอุปกรณ์ตรวจจับการเคลื่อนไหวของผู้บุกรุก ประกอบขึ้นมาเพื่อให้การรักษาความปลอดภัยนั้นมีประสิทธิภาพมากยิ่งขึ้น รวมทั้งการส่งข้อความแจ้งเตือนผ่านทางโทรศัพท์เคลื่อนที่จึงทำให้ศักยภาพของระบบรักษาความปลอดภัยโดยอยู่บนพื้นฐานของเทคโนโลยีกล้องวงจรปิด (CCTV) นั้นมีประสิทธิภาพมากยิ่งขึ้น

โดยภาพรวมของทั้งระบบแสดงได้ดัง Block Diagram ดังรูปที่ 1.1



รูปที่ 1.1 ภาพรวมระบบ

1.2 จุดประสงค์

1. เพื่อศึกษาระบบรักษาความปลอดภัยด้วยเทคโนโลยีกล้องวงจรปิด (CCTV) และหลักการทำงานของระบบ
2. เพื่อศึกษาและพัฒนาซอฟต์แวร์ (Software) สำหรับควบคุมกล้องวงจรปิด
3. เพื่อศึกษาและพัฒนาซอฟต์แวร์ (Software) สำหรับรับ-ส่งข้อมูลผ่านทางคอมพิวเตอร์และโทรศัพท์เคลื่อนที่
4. เพื่อศึกษาระบบการแจ้งเตือน
5. เพื่อศึกษาการทำงานของ Image Processing สำหรับระบุตัวบุคคล

1.3 ขอบเขตของโครงงาน

1. มีการประยุกต์ใช้ทฤษฎีและโปรแกรมที่ได้ศึกษามาเพื่อใช้ในการควบคุมกล้องและสามารถตรวจสอบความปลอดภัยในแต่ละสถานที่ในทุกๆมุมที่ต้องการ
2. มีส่วนของซอฟต์แวร์ที่ใช้ในการรับ-ส่ง และเก็บข้อมูลภาพไว้ในระบบ
3. มีการใช้ระบบควบคุมการทำงานกล้องผ่านระบบอินเตอร์เน็ตโดยใช้คอมพิวเตอร์

4. มีการส่งข้อความแจ้งเตือนจากระบบไปยังโทรศัพท์เคลื่อนที่ เมื่อระบบตรวจพบการเคลื่อนไหวของผู้บุกรุก
5. มีส่วนของซอฟต์แวร์ในการทำ Image Processing เพื่อทำการจดจำใบหน้าสำหรับระบุตัวบุคคล

1.4 ผลที่คาดว่าจะได้รับ

1. ระบบที่พัฒนาขึ้นสามารถควบคุมกล้องวงจรปิดเพื่อสังเกตการณ์ในสถานที่ที่ต้องการ ได้ทุกที่ทุกเวลา
2. เรียนรู้การพัฒนาโปรแกรมด้วย Visual Basic
3. สามารถพัฒนาโปรแกรมที่ใช้ในการควบคุมกล้องวงจรปิดผ่านเครือข่ายอินเตอร์เน็ตได้
4. เรียนรู้และพัฒนาการใช้โปรแกรมควบคุม Servo Motor ที่พัฒนาขึ้นโดยภาษา C
5. สามารถนำหลักการ Image Processing มาประยุกต์ใช้ในการตรวจจับใบหน้า
6. สามารถที่จะส่งข้อความแจ้งเตือนไปยังโทรศัพท์เคลื่อนที่ได้

1.5 อุปกรณ์ที่ต้องใช้

1.5.1 ฮาร์ดแวร์

1. กล้องวงจรปิด (Webcam)
2. Servo Motor
3. ไมโครคอนโทรลเลอร์ AVR Atmega328
4. คอมพิวเตอร์
5. โทรศัพท์เคลื่อนที่
6. PIR Motion Sensor

1.5.2 ซอฟต์แวร์

1. Visual Basic
2. Matlab

1.6 ขั้นตอนการดำเนินงาน

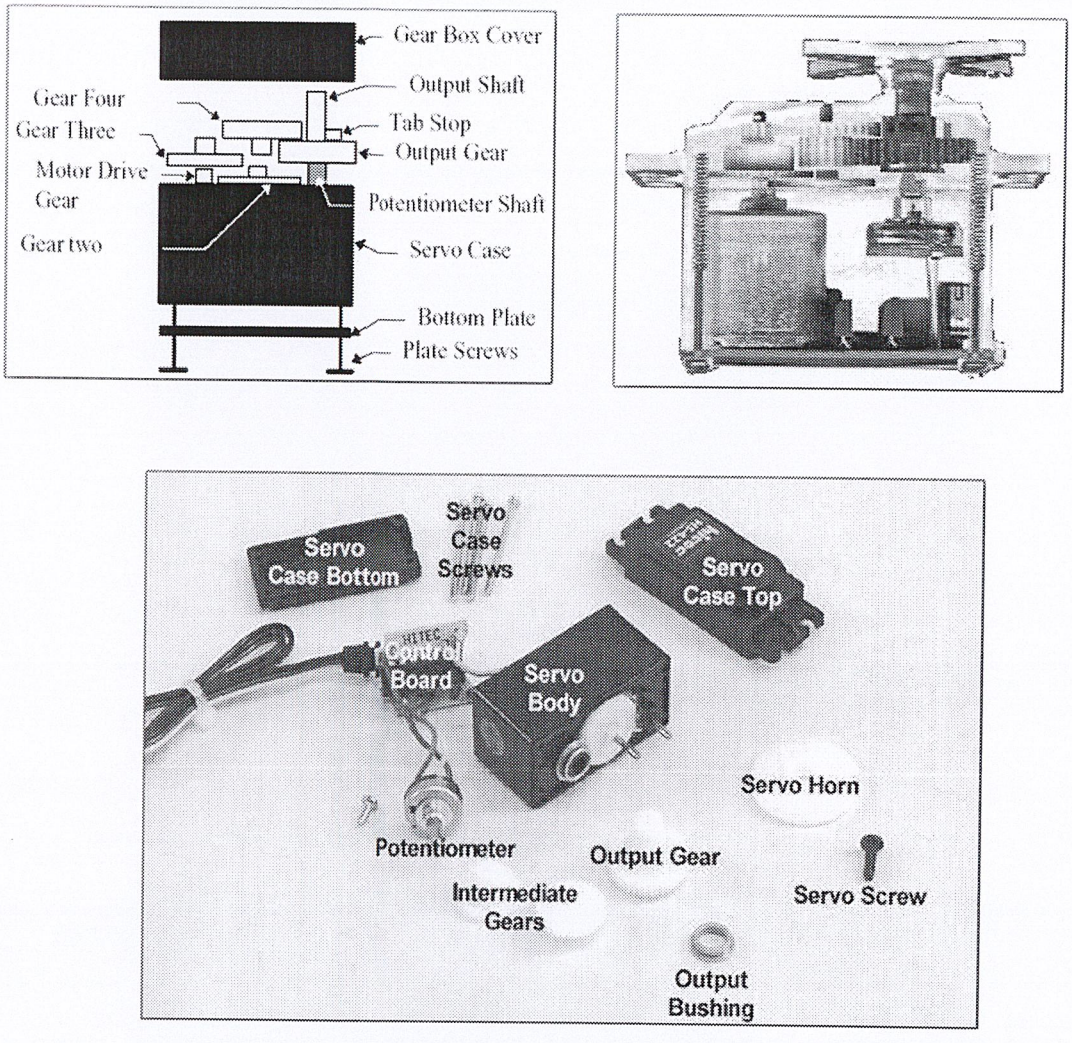
ID	Task Name	มิ.ย. 53	ก.ค. 53	ส.ค. 53	ก.ย. 53	ต.ค. 53	พ.ย. 53	ธ.ค. 53	ม.ค. 54	ก.พ. 54
1	ศึกษาการทำงานของกล้องวงจรปิด									
2	ศึกษาหลักการควบคุม Servo Motor									
3	ศึกษาการเขียนโปรแกรม Visual Basic									
4	ศึกษาหลักการส่งข้อความผ่าน SMS									
5	ออกแบบและพัฒนาโปรแกรมควบคุม Servo Motor									
6	ทดสอบโปรแกรมควบคุมกล้องวงจรปิดโดย Servo Motor และนำไปเชื่อมต่อทางอินเตอร์เน็ต									
7	ออกแบบและทดสอบการส่งข้อความแจ้งเตือน									
8	ศึกษาการทำ Image Processing									
9	ออกแบบและทดสอบโปรแกรมการทำ Image Processing									
10	ทดสอบระบบทั้งหมดและปรับปรุงแก้ไข									
11	จัดทำเอกสารปริญญานิพนธ์									

บทที่ 2
ทฤษฎีและหลักการ

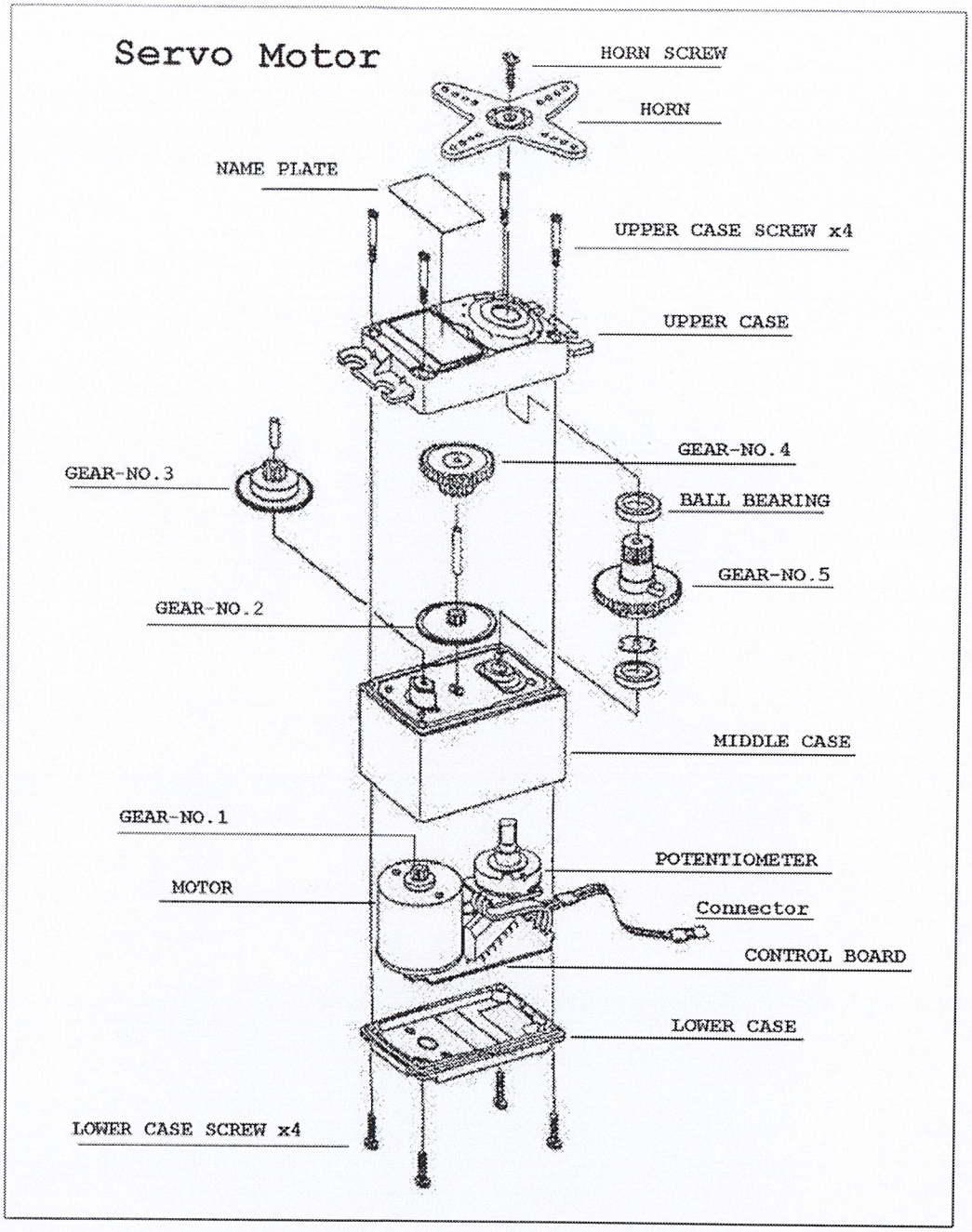
2.1 เซอร์โวมอเตอร์ (Servo Motor)

เซอร์โวมอเตอร์ คือ มอเตอร์ไฟฟ้ากระแสตรง (DC Motor) ที่ถูกประกอบรวมกับ ชุดเกียร์ และ ส่วนควบคุม ต่างๆ ไว้ในโมดูลเดียวกัน หรือ ภายในกล่องพลาสติกเดียวกัน โดยมอเตอร์ชนิดนี้จะมีสายต่อใช้งานเพียง 3 เส้นเท่านั้น คือ VCC,GND และ สายสัญญาณควบคุม (Control Line) ซึ่งสามารถควบคุมให้มอเตอร์หมุนซ้าย หรือ ขวาได้จากสายสัญญาณเพียงเส้นเดียว โดยสัญญาณที่ใช้ควบคุมนี้จะเป็นสัญญาณพัลส์วิดมอดดูเลชัน (PWM) แบบ TTL Level ระดับแรงดันที่จ่ายให้มอเตอร์นี้จะอยู่ในช่วงประมาณ 4 ถึง 6 โวลต์ ขึ้นอยู่กับคุณสมบัติของมอเตอร์แต่ละตัว ข้อดีของมอเตอร์ชนิดนี้ก็คือ จะมีขนาดเล็กน้ำหนักเบา ให้แรงบิตสูง กินพลังงานน้อย และสามารถควบคุมด้วยแรงดันลอจิกที่เป็น TTL ได้โดยตรงไม่จำเป็นต้องต่อวงจรขับ (Driver) อื่นๆ เพราะมอเตอร์ชนิดนี้จะมีวงจรควบคุมบรรจุไว้ภายในอยู่แล้ว ซึ่งมอเตอร์ชนิดนี้สามารถควบคุมให้หมุนไปในตำแหน่ง หรือ ทิศทางองศาที่ต้องการได้ โดยอาศัยสัญญาณความกว้างพัลส์ที่ป้อนให้มอเตอร์ แต่เซอร์โวมอเตอร์นี้จะหมุนได้แค่เพียงในช่วงประมาณ 180 องศา หรือ ครึ่งรอบเท่านั้น หรือ บางรุ่นอาจหมุนได้ถึง 210 องศา แต่จะไม่สามารถหมุนเป็นวงรอบได้ เนื่องจากโครงสร้างภายในจะประกอบด้วย ตัวต้านทานชนิดปรับค่าได้ (VR) ที่ทำหน้าที่ตรวจสอบตำแหน่งการหมุนของมอเตอร์ และตัวต้านทานนี้จะถูกยึดติดกับแกนหมุนของมอเตอร์ ซึ่งจากการที่ตัวต้านทานปรับค่านี้ไม่สามารถหมุนเป็นวงรอบได้ ดังนั้นเซอร์โวมอเตอร์จึงถูกออกแบบให้หมุนได้เพียงแค่ประมาณ 180 องศา หรือ ครึ่งรอบเท่านั้น เพื่อป้องกันความเสียหายที่จะเกิดกับตัวต้านทานปรับค่าได้

ส่วนประกอบต่างๆของเซอร์โวมอเตอร์แสดงได้ดังรูปที่ 2.1 และโครงสร้างรวมถึงส่วนประกอบภายในเซอร์โวมอเตอร์แสดงได้ดังรูปที่ 2.2



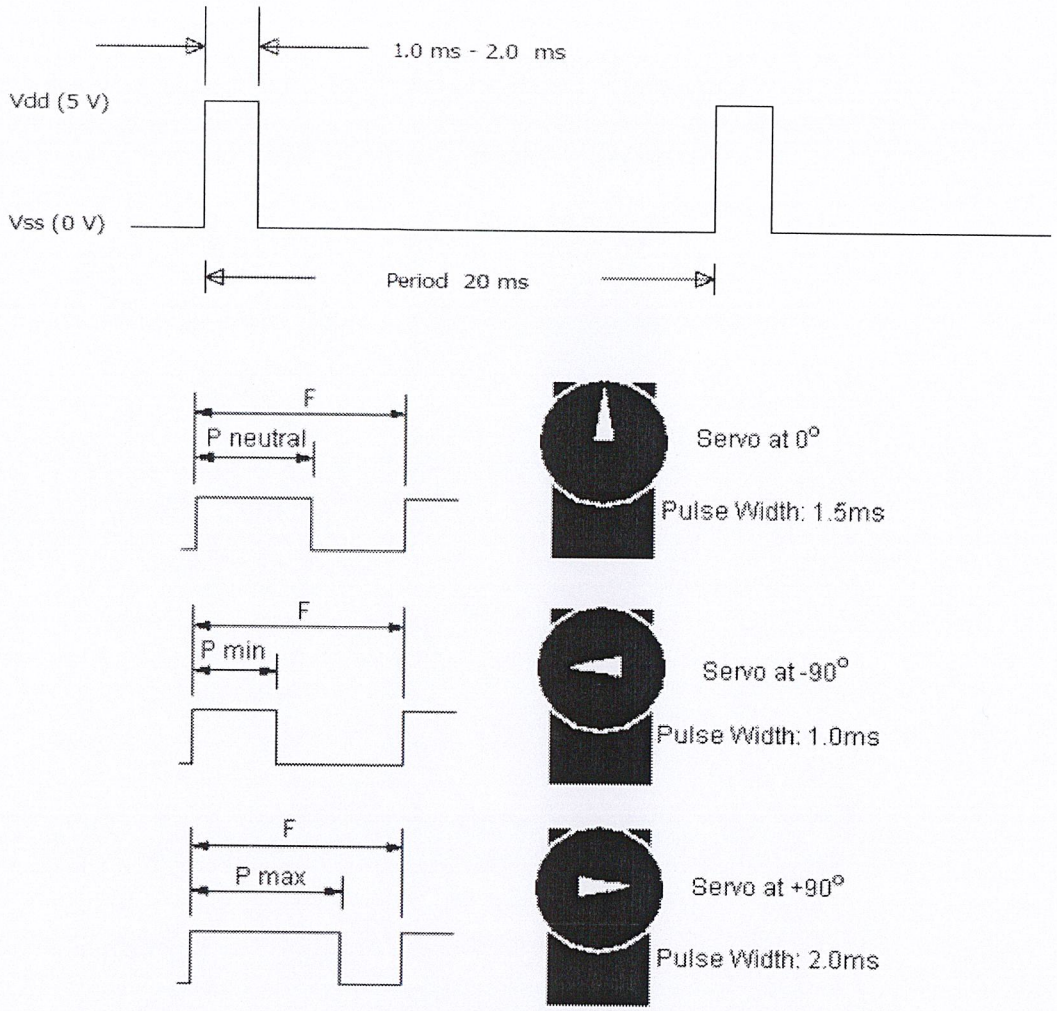
รูปที่ 2.1 ส่วนประกอบต่างๆของเซอร์โวมอเตอร์ [1]



รูปที่ 2.2 โครงสร้างและส่วนประกอบภายในของเซอร์โวมอเตอร์ [1]

2.1.1 หลักการทำงานของเซอร์โวมอเตอร์

การควบคุมการทำงานของเซอร์โวมอเตอร์ทำได้โดยการป้อนสัญญาณความกว้างพัลส์ให้กับมอเตอร์ซึ่งตำแหน่งและทิศทางการหมุนของมอเตอร์นี้จะขึ้นอยู่กับขนาดของความกว้างของพัลส์นั้นๆ โดยทั่วไปแล้วความกว้างของสัญญาณพัลส์จะมีจุดให้อ้างอิง 3 จุด ดังรูปที่ 2.3 คือ



รูปที่ 2.3 แสดงการหมุนของเซอร์โวมอเตอร์เมื่อมีสัญญาณพัลส์รูปแบบต่างๆเข้ามา [1]

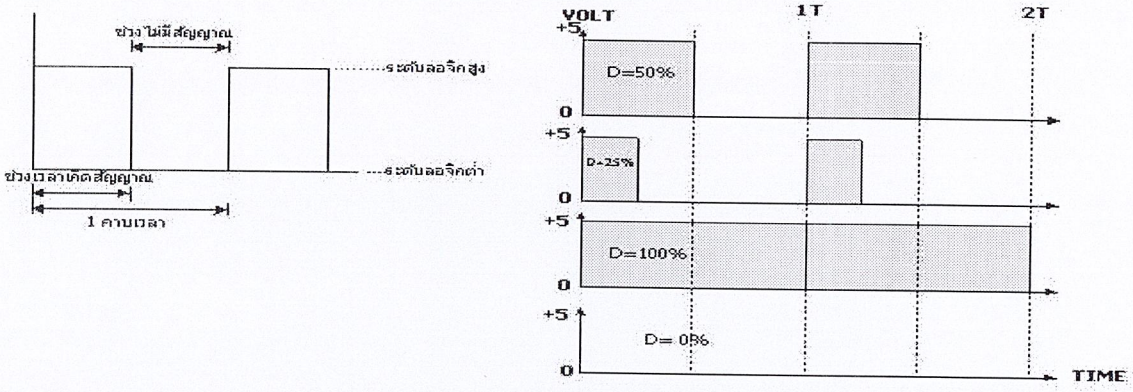
- สัญญาณความกว้างพัลส์ขนาด 1.5 ms จะควบคุมให้เซอร์โวมอเตอร์หมุนไปอยู่ที่ตำแหน่งมุม 0 องศา หรือ จุดกึ่งกลางของมอเตอร์
- สัญญาณความกว้างพัลส์ขนาด 1 ms จะควบคุมให้เซอร์โวมอเตอร์หมุนไปอยู่ที่ตำแหน่งมุม - 90 องศา หรือในทิศทางทวนเข็มนาฬิกา
- สัญญาณความกว้างพัลส์ขนาด 2 ms จะควบคุมให้เซอร์โวมอเตอร์หมุนไปอยู่ที่ตำแหน่งมุม + 90 องศา หรือในทิศทางตามเข็มนาฬิกา

ส่วนการที่จะควบคุมให้มอเตอร์หมุนเป็นมุมอื่นๆ นั้นก็สามารถทำได้โดยการป้อนสัญญาณพัลส์เป็นระดับความกว้างต่างๆ โดยอ้างอิงจากจุด ทั้ง 3 จุดที่กล่าวมานี้ ตัวอย่างเช่น ถ้าต้องการให้มอเตอร์หมุนไปที่มุม -45 องศา เราก็จะต้องป้อนสัญญาณพัลส์ที่มีความกว้าง 1.25 ms เป็นต้น และ สัญญาณพัลส์นี้จะต้องจ่ายให้มอเตอร์ทุกๆ 20 ms (Period) เพื่อรักษาสภาพตำแหน่งของมอเตอร์ไว้

2.1.2 พัลส์วิดช์มอดูเลชัน PWM (Pulse width modulation)

พัลส์วิดช์มอดูเลชัน เป็นเทคนิคการปรับความกว้างของสัญญาณพัลส์ เนื่องจากการนำไปใช้ในการควบคุม DC Motor โดยการให้สัญญาณพัลส์ แล้วทำการปรับสัญญาณพัลส์เพื่อเป็นการปรับความเร็วในการหมุนของมอเตอร์ โดยจะเป็นการปรับเปลี่ยนที่สัดส่วน และความกว้างของสัญญาณพัลส์ โดยความถี่ของสัญญาณพัลส์จะไม่มีการเปลี่ยนแปลง หรือเป็นการเปลี่ยนแปลงที่ค่าของดิวตี้ไซเกิล (Duty Cycle) นั้นเอง ซึ่งค่าของดิวตี้ไซเคิล คือช่วงความกว้างของพัลส์ที่มีสถานะลอจิกสูง โดยคิดสัดส่วนเป็นเปอร์เซ็นต์จากความกว้างของพัลส์ทั้งหมด ยกตัวอย่างเช่น ถ้าหากค่าดิวตี้ไซเคิลมีค่าเท่ากับเท่ากับ 50% ก็หมายถึงใน 1 รูปสัญญาณพัลส์จะมีช่วงของสัญญาณที่เป็นสถานะลอจิกสูงอยู่ครึ่งหนึ่ง และสถานะลอจิกต่ำอยู่อีกครึ่งหนึ่ง และในทำนองเดียวกันถ้าหากค่าดิวตี้ไซเคิลมีค่ามาก หมายความว่าความกว้างของพัลส์ที่เป็นสถานะลอจิกสูงจะมีความกว้างมากขึ้น หากค่าดิวตี้ไซเคิลมีค่าเท่ากับ 100% ก็หมายความว่าจะไม่มีสถานะลอจิกต่ำเลย ซึ่งค่าดิวตี้ไซเคิลสามารถ จะหาได้จากค่าความสัมพันธ์ดังสมการ (1)

ค่าดิวตี้ไซเคิล = (ช่วงของสัญญาณพัลส์/คาบเวลาทั้งหมดของสัญญาณ) x 100% (1)



รูปที่ 2.4 ความกว้างของพัลส์ขนาดต่างๆ และค่าดิวตี้ไซเคิล ของช่วงพัลส์ที่มีความถี่คงที่ [2]

หลักการคำนวณองศาการหมุนของเซอร์โวมอเตอร์

สัญญาณความกว้างพัลส์ขนาด 1 ms มอเตอร์หมุนอยู่ตำแหน่ง -90 องศา

สัญญาณความกว้างพัลส์ขนาด 2 ms มอเตอร์หมุนอยู่ตำแหน่ง +90 องศา

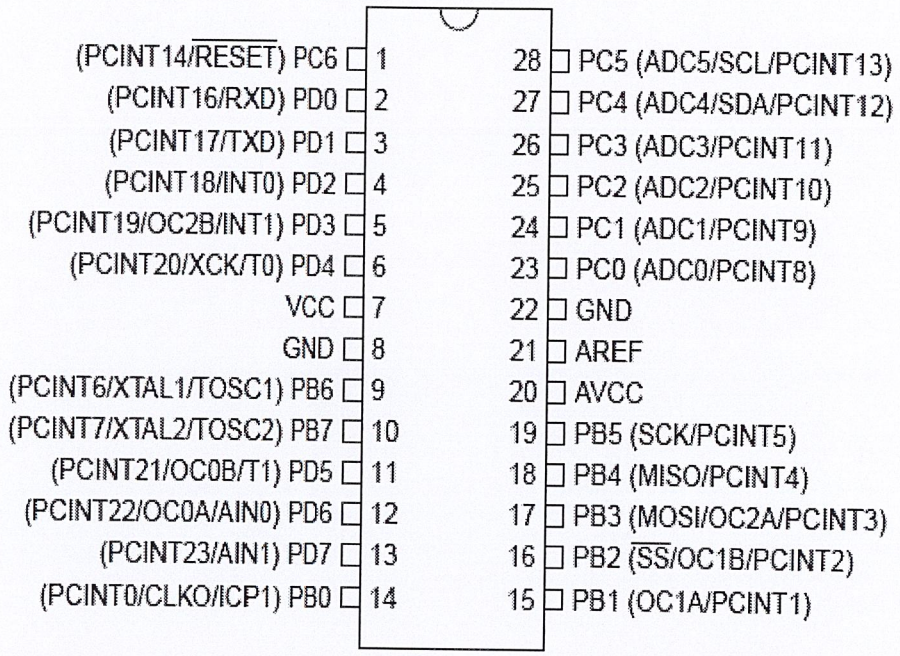
ผลต่างของสัญญาณความกว้างพัลส์ 1 ms มอเตอร์อยู่ตำแหน่งต่างกัน 180 องศา

ดังนั้นถ้าต้องการหาขนาดสัญญาณความกว้างพัลส์ที่ต้องป้อนให้กับเซอร์โวมอเตอร์ให้เพิ่มหรือลดทีละ X องศา จะคำนวณโดยนำค่า 1 ms คูณด้วย X แล้วทำการหารด้วย 180 องศา เช่น ถ้าต้องการเพิ่มหรือลดทีละ 1 องศา คำนวณ (1 ms x 1 องศา) หารด้วย 180 องศา เท่ากับ 0.005 ms

2.2 ไมโครคอนโทรลเลอร์ AVR

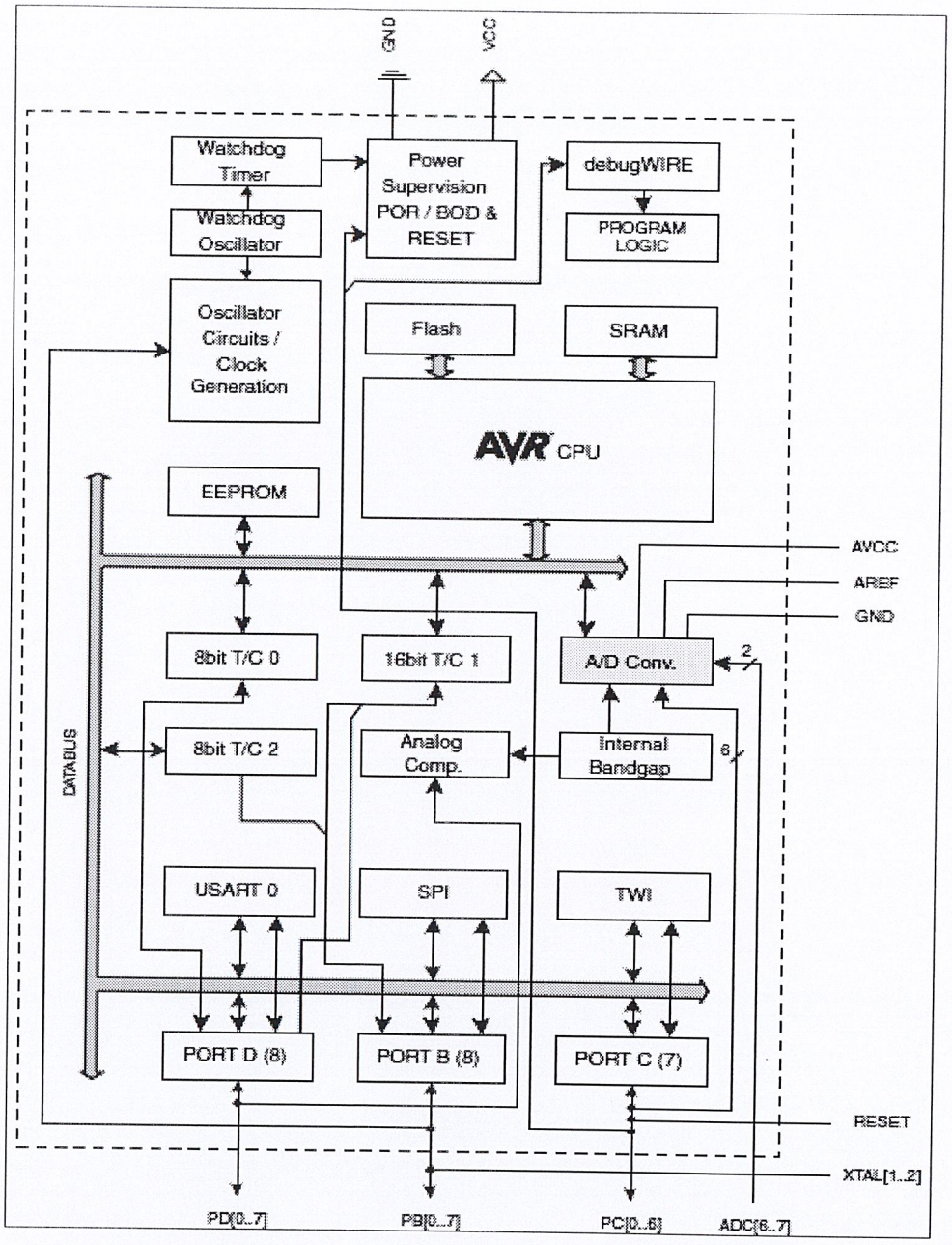
ไมโครคอนโทรลเลอร์ AVR เป็นไอซีไมโครคอนโทรลเลอร์ของบริษัท Atmel มีสถาปัตยกรรมภายในเป็นแบบ RISC (Reduced Instruction Set Computer) โดยใช้สัญญาณนาฬิกาเพียง 1 ลูกในการปฏิบัติงานใน 1 คำสั่ง โดยจะประกอบด้วยหน่วยความจำโปรแกรมภายในที่เป็นแบบแฟลช โปรแกรมข้อมูลได้แบบ In-System Programmable และในบางเบอร์ยังสามารถมีการกำหนดตำแหน่งของหน่วยความจำที่สร้างเป็นบูตโหลดเดอร์ (เขียนโปรแกรมเพื่อติดต่อกับเครื่องคอมพิวเตอร์ หรือไอซีตัวอื่นๆ และยังสามารถโปรแกรมให้กับตัวเองได้) มีขนาดของหน่วยความจำตามเบอร์ของไอซีแต่ละตัว คุณสมบัติของไอซีเบอร์ Atmega328 มีดังต่อไปนี้

2.2.1 คุณสมบัติทางเทคนิคของ ATmega328



รูปที่ 2.5 ตำแหน่งขาการทำงานของไมโครคอนโทรลเลอร์ Atmega328 [3]

- เป็นไมโครคอนโทรลเลอร์ขนาด 8 บิตมีประสิทธิภาพสูง ใช้พลังงานต่ำ
- มีโครงสร้างสถาปัตยกรรมภายในแบบ Advance RISC
  - มีคำสั่งควบคุมการทำงานไมโครคอนโทรลเลอร์ 130 คำสั่ง ส่วนมากจะทำสำเร็จในรอบสัญญาณนาฬิกาเดี่ยว
  - มีจำนวนรีจิสเตอร์ทั่วไปขนาด 32 x 8
- มีหน่วยความจำโปรแกรมภายในแบบ Flash ขนาด 32 K bytes มีการโปรแกรมได้แบบ In-System Self-Programmable
- มีหน่วยความจำภายในแบบ EEPROM ขนาด 1 K bytes
- มีหน่วยความจำ Flash SRAM 2 K bytes
- เขียน/ลบ ได้ถึง 10,000 ครั้ง สำหรับหน่วยความจำแบบ Flash และ 100,000 ครั้งสำหรับหน่วยความจำแบบ EEPROM
- กำหนดการ Boot Code Section ในตำแหน่งต่างๆ และ Lock Bits ได้
- Programming Lock for Software Security ป้องกันข้อมูล
- Timer/Counters ขนาด 8-บิต 2 ตัว และมี Separate Prescaler โหมด Compare อีก 1 ตัว
- Timer/Counters ขนาด 16-บิต 1 ตัว with Separate Prescaler, Compare Mode, and Capture
- มีพัลส์วิดช์มอดูเลชัน (PWM) 6 ช่องสัญญาณ
- ADC 10 บิต จำนวน 8 ช่องสัญญาณ
- สามารถตรวจสอบการขัดจังหวะการทำงานจากการเปลี่ยนแปลงของขาอินพุต เอาท์พุต
- สามารถทำการโปรแกรมผ่าน USART
- มีการติดต่อแบบ Master/Slave SPI Serial Interface
- ใช้งาน RC Oscillator ภายในไอซี และภายนอกไอซีได้
- ระดับอุณหภูมิที่สามารถทำงานได้ -40 °C ถึง 85 °C
- ความเร็วสูงสุดที่สามารถทำงานได้ 0 - 4 MHz ที่แรงดัน 1.8 – 5.5 V
  และ 0 – 10 MHz ที่แรงดัน 2.7 - 5.5 V
- การทำงานที่พลังงานต่ำ ความถี่ 1 MHz ที่ 1.8 V
  - การทำงาน Active Mode : ใช้กระแสไฟ 240 μA
  - การทำงาน Power-down Mode : ใช้กระแสไฟ 0.1 μA
  - การทำงาน Power-save Mode : ใช้กระแสไฟ 0.75 μA



รูปที่ 2.6 สถาปัตยกรรมภายในคอนโทรลเลอร์เบอร์ Atmega328 [3]

2.2.2 การสื่อสารข้อมูลแบบอนุกรม (Serial Communication)

จากการเรียนรู้ที่ผ่านมาการรับส่งข้อมูลผ่านทางพอร์ทจะเป็นการสื่อสารแบบขนาน เพราะเวลาส่งข้อมูลขนาด 1 ไบต์ต้องใช้ขาสัญญาณในการส่งเท่ากับจำนวนบิตทั้งหมดคือ 8 ขา เพื่อที่จะลดจำนวนขาในการสื่อสาร จึงต้องมีการสื่อสารแบบอนุกรมเข้ามาช่วย ถึงแม้ว่าการสื่อสารแบบอนุกรมจะใช้ขาสัญญาณที่น้อยกว่า และสามารถส่งได้ไกลกว่า การสื่อสารแบบ

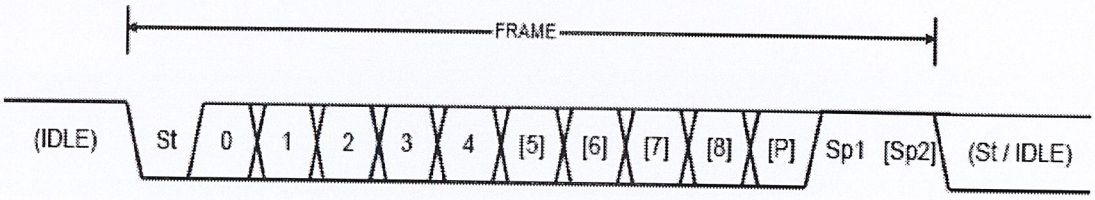
อนุกรมก็ยังมีข้อด้อยเรื่องความเร็วในการสื่อสารที่น้อยกว่าแบบขนาน และการเพิ่มเติมวงจรเพื่อแปลงการสื่อสารแบบอนุกรมให้เป็นแบบขนาน

รูปแบบการสื่อสารแบบอนุกรมจะมีอยู่ 3 แบบคือ

- การสื่อสารแบบทิศทางเดียว (Simplex) ซึ่งสามารถรับหรือส่งได้เพียงอย่างเดียวเท่านั้น
- การสื่อสารแบบสองทางครึ่งอัตรา (Half Duplex) ซึ่งสามารถรับและส่งได้แต่ไม่พร้อมกัน
- การสื่อสารแบบสองทางเต็มอัตรา (Full Duplex) ซึ่งสามารถรับและส่งได้ในเวลาเดียวกัน

2.2.3 การสื่อสารข้อมูลแบบ UART (Universal Asynchronous Receiver Transmitter)

การสื่อสารข้อมูลแบบ UART เป็นการสื่อสารอนุกรมในรูปแบบ Full Duplex ซึ่งใช้ขา Rx ในการรับข้อมูล และใช้ขา Tx ในการส่งข้อมูล การสื่อสารจะเป็นแบบ Asynchronous ดังนั้นจึงไม่มีขาสัญญาณในการ Synchronize ข้อมูล ทำให้ฝ่ายรับและฝ่ายส่งจำเป็นที่จะต้องรู้รูปแบบของข้อมูล และความเร็วในการสื่อสาร การใช้งาน UART จะเอาไปประยุกต์ใช้กับมาตรฐานการสื่อสารอนุกรมแบบ RS232 หรือ RS485 เป็นต้นรูปแบบของข้อมูล (Frame Format) ในการสื่อสารของ UART จะมีรูปแบบดังรูปที่ 2.7



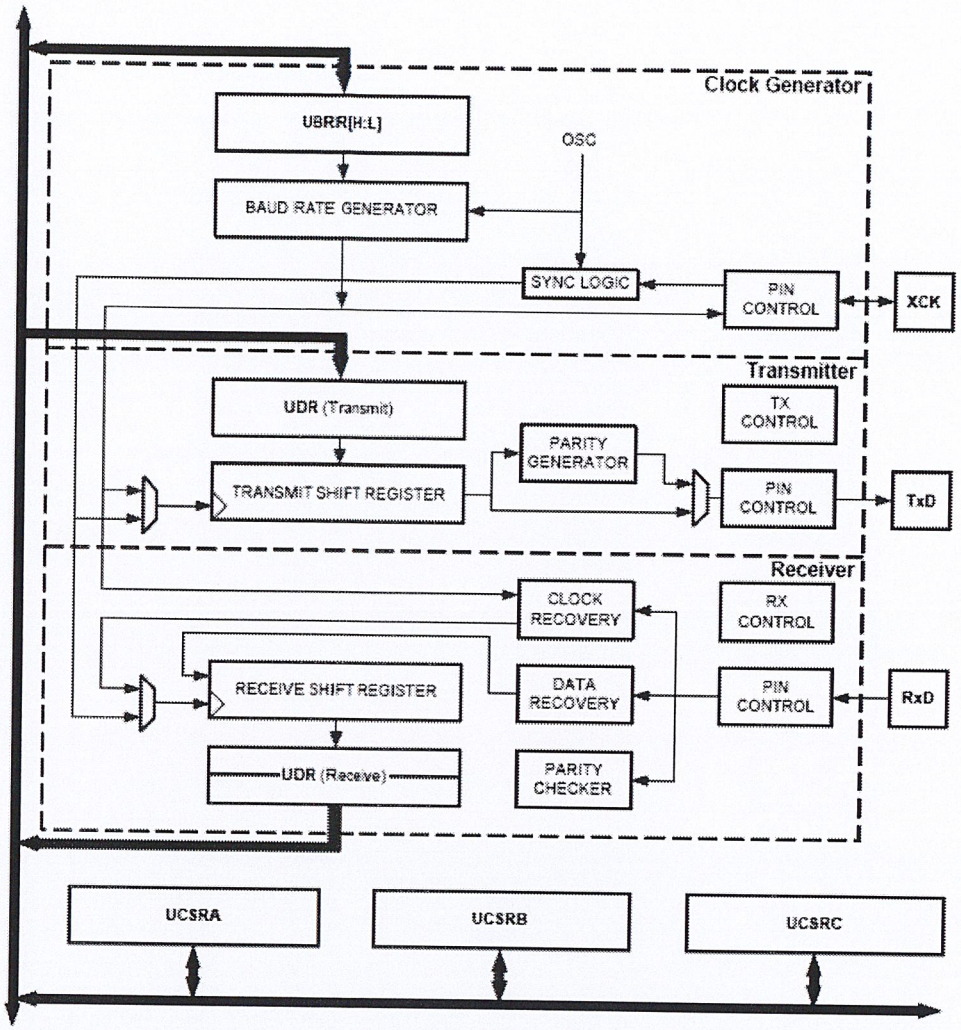
รูปที่ 2.7 Frame Format [4]

IDLE เป็นสภาวะของระดับสัญญาณที่ไม่มีการรับหรือส่งข้อมูล ปกติมีค่าเป็น High

- St (Start bit) เป็นบิตเริ่มต้นของข้อมูล ปกติมีค่าเป็น Low
- N (1–8) เป็นค่าข้อมูลของแต่ละบิต
- P (Parity) เป็นบิตในการตรวจสอบความถูกต้องของข้อมูลโดยการนับจำนวนบิตที่มีค่าเป็น 1 ว่าเป็น
- จำนวนคู่หรือคี่
- Sp (Stop bit) เป็นบิตสิ้นสุดข้อมูลซึ่งอาจจะมี 1 หรือ 2 บิตขึ้นอยู่กับการกำหนด ค่าปกติจะมีค่าเป็น High

2.2.4 การเขียนโปรแกรมควบคุม UART ของไมโครคอนโทรลเลอร์ AVR

โครงสร้างการทำงานของ UART จะมีลักษณะ ดังรูปที่ 2.8



รูปที่ 2.8 โครงสร้างการทำงานของ UART [4]

จากรูปด้านบนจะเห็นได้ว่า UART จะรองรับการทำงานแบบ Synchronous เพิ่มเติมด้วย หรือเรียกว่า USART โดยจะมีขา XCK เพื่อใช้ในการ Synchronize ข้อมูล แต่ในที่นี้จะกล่าวถึงเฉพาะการทำงานแบบ Asynchronous เท่านั้น รีจิสเตอร์ที่เกี่ยวข้องกับการทำงานของ UART จะมีอยู่ 5 รีจิสเตอร์ด้วยกันคือ UCSRnA, UCSRnB, UCSRnC, UDRnและ UBRRn ซึ่งรีจิสเตอร์แต่ละตัวมีหน้าที่ต่างๆ ดังนี้

- **UDRn** (UART I/O Data Register) เป็นรีจิสเตอร์ที่ใช้รับและส่งข้อมูล

- **UCSRnA** (UART Control and Status Register A) เป็นรีจิสเตอร์ที่ใช้ในการควบคุมการทำงานและตรวจสอบสถานะต่างๆ ของ UART ซึ่งมีรายละเอียดของบิตต่างๆ

- RXCn เป็นบิตบอกสถานะของการรับข้อมูล ซึ่งจะมีค่าเป็น 1 เมื่อได้รับข้อมูลเรียบร้อยแล้ว
- TXCn เป็นบิตบอกสถานะของการส่งข้อมูล จะมีค่าเป็น 1 เมื่อส่งข้อมูลเสร็จเรียบร้อยแล้ว ซึ่งสามารถเคลียร์ค่าให้เป็นลอจิก 0 ได้โดยการเขียน ลอจิก 1 ไปที่บิตนี้
- UDREn เป็นบิตบอกสถานะของรีจิสเตอร์ UDRn ว่าพร้อมที่จะรับข้อมูลใหม่เพื่อไปส่งได้หรือไม่ ค่าบิตจะเป็นลอจิก 1 เมื่อพร้อมที่จะส่งข้อมูลได้
- FEn เป็นบิตบอกสถานะของการรับข้อมูลที่ผิดพลาดซึ่งเกิดจาก Stop bit มีค่าเป็นลอจิก 0
- DORn เป็นบิตบอกสถานะของการส่งการได้รับข้อมูลมาใหม่โดยที่ยังไม่ได้อ่านข้อมูลเก่าออกไปจากรีจิสเตอร์ UDRn
- UPEn เป็นบิตบอกความผิดพลาดเมื่อตรวจสอบพาริตี้แล้วไม่ถูกต้อง
- U2Xn เป็นบิตที่ใช้ในการความคุมความเร็วในการสื่อสารให้เพิ่มขึ้น 2 เท่าถ้ามีการกำหนดค่าเป็นลอจิก 1
- MPCMn เป็นบิตที่ใช้ในการกำหนดให้เป็นโหมดการสื่อสารแบบหลายหน่วยประมวลผล

-UCSRnB (UART Control and Status Register B) เป็นรีจิสเตอร์ที่ใช้ในการควบคุมการทำงานและตรวจสอบสถานะต่างๆ ของ UART ซึ่งมีรายละเอียดของบิตต่างๆ

- RXCIEn เป็นบิตที่กำหนดให้มีการเกิดอินเตอร์รัพท์ เมื่อได้รับข้อมูลเรียบร้อยแล้ว
- TXCIEn เป็นบิตที่กำหนดให้มีการเกิดอินเตอร์รัพท์ เมื่อส่งข้อมูลเสร็จเรียบร้อยแล้ว
- UDRIEn เป็นบิตที่กำหนดให้มีการเกิดอินเตอร์รัพท์ เมื่อรีจิสเตอร์ UDRn พร้อมส่งข้อมูล
- RXENn เป็นบิตที่กำหนดให้ UART สามารถรับข้อมูลได้
- TXENn เป็นบิตที่กำหนดให้ UART สามารถส่งข้อมูลได้
- UCSZn2 เป็นบิตที่ใช้กำหนดจำนวนข้อมูลที่จะสื่อสารใน 1 ครั้ง
- RXB8n เป็นบิตข้อมูลที่ได้รับเพิ่มเติมในกรณีที่ขนาดข้อมูลเกิน 8 บิต
- TXB8n เป็นบิตข้อมูลที่ใช้ส่งเพิ่มเติมในกรณีที่ขนาดข้อมูลเกิน 8 บิต

-UCSRnC (UART Control and Status Register C) เป็นรีจิสเตอร์ที่ใช้ในการควบคุมการทำงานและตรวจสอบสถานะต่างๆ ของ UART ซึ่งมีรายละเอียดของบิตต่างๆ

UMSELn1, UMSELn0 เป็นบิตในการเลือกโหมดการสื่อสารของ UART ซึ่งมีทั้งหมด 4 โหมดตามค่าต่างๆ ดังตารางที่ 2.1

ตารางที่ 2.1 การกำหนดโหมดในการสื่อสาร

UMSELn1	UMSELn0	โหมด
0	0	Asynchronous
0	1	Synchronous
1	0	Reserved
1	1	Mater SPI

- UPMn1, UPMn0 เป็นบิตในการเลือกรูปแบบพาริตี้เพื่อตรวจสอบข้อมูล ซึ่งจะมีค่าต่างๆ ดังตารางที่ 2.2

ตารางที่ 2.2 การกำหนดพาริตี้

UPMn1	UPMn0	โหมด
0	0	Disable
0	1	Reserved
1	0	Even Parity
1	1	Odd parity

- USBSn เป็นบิตในการกำหนดจำนวน Stop bit ถ้าเป็นลอจิก 0 จะมี 1 บิต ถ้าเป็นลอจิก 1จะมี 2 บิต
- UCSZn1, UCSZn0 รวมถึง UCSZn2 ที่อยู่ในรีจิสเตอร์ UCSRnB จะทำหน้าที่ในการกำหนดจำนวนบิตของข้อมูลที่สื่อสารแต่ละครั้งดังตารางที่ 2.3

ตารางที่ 2.3 การกำหนดขนาดข้อมูล

UCSZn2	UCSZn1	UCSZn0	ขนาดข้อมูล
0	0	0	5 bit
0	0	1	6 bit
0	1	0	7 bit
0	1	1	8 bit
1	0	0	Reserved
1	0	1	Reserved
1	1	0	Reserved
1	1	1	9 bit

- UCPOLn เป็นบิตที่ใช้กำหนดความสัมพันธ์ระหว่างข้อมูลและสัญญาณนาฬิกา ซึ่งใช้ในโหมด Synchronous เท่านั้น

UBRRnL, UBRRnH (UART Baud Rate Register) เป็นรีจิสเตอร์ที่ใช้กำหนดความเร็วในการสื่อสารซึ่งค่าที่กำหนดต้องมีความสัมพันธ์กับสัญญาณนาฬิกาที่ป้อนให้ชิพทำงาน

ตารางที่ 2.4 การคำนวณค่า UBRR จาก Baud Rate

โหมด	สูตรคำนวณ
Asynchronous(U2Xn=0)	$UBRRn = \frac{f_{OSC}}{16BAUD} - 1$
Asynchronous(U2Xn=1)	$UBRRn = \frac{f_{OSC}}{8BAUD} - 1$

2.3 การติดต่อกับพอร์ตอนุกรม (Serial Port)

ในการประยุกต์ใช้งานอุปกรณ์เชื่อมต่อนั้น ได้มีการใช้งานพอร์ตคอมพิวเตอร์เชื่อมต่อไม่ว่าจะเป็น พอร์ตขนานหรือเรียกกันทั่วไปว่าพอร์ตปริ้นเตอร์ ซึ่งติดตั้งอยู่บนเมนบอร์ดของคอมพิวเตอร์ทุกเครื่องอยู่แล้ว นอกจากนี้ก็ยังมีอีกพอร์ตหนึ่งที่สามารถใช้งานทางด้านนี้เช่นกัน นั้นคือพอร์ตอนุกรม ซึ่งประกอบด้วย รายละเอียดดังต่อไปนี้

2.3.1 พื้นฐานการสื่อสารแบบอนุกรม

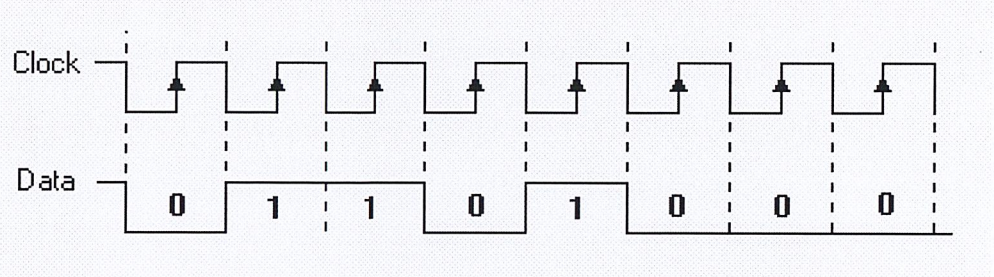
ถึงแม้ว่าการสื่อสารแบบอนุกรมในเครื่องคอมพิวเตอร์นั้น จะมีความเร็วในการสื่อสารช้ากว่าแบบขนาน ทั้งนี้ก็เพราะว่าการเคลื่อนย้ายข้อมูลแบบอนุกรมนั้นเป็นการส่งข้อมูลครั้งละ 1 บิต แต่พอร์ตขนาน นั้นสามารถส่งข้อมูลได้ครั้งละหลายๆบิตพร้อมกัน ส่งผลให้การสื่อสารข้อมูลแบบอนุกรมมีความเร็วต่ำกว่าแบบขนาน

แต่ว่าการส่งข้อมูลแบบอนุกรมนั้นมีข้อที่เหนือกว่าการส่งข้อมูลแบบขนานคือ การสามารถส่งข้อมูลได้ในระยะทางที่ไกลกว่าแบบขนาน อีกทั้งสายสัญญาณที่ใช้ยังมีน้อยกว่าการส่งข้อมูลแบบขนานอีกด้วย การสื่อสารแบบอนุกรมสามารถแบ่งออกเป็น 3 รูปแบบ ดังนี้

1. Simplex สามารถส่งข้อมูลได้อย่างเดียวเป็นการสื่อสารแบบทางเดียว
2. Half – Duplex สามารถส่งข้อมูลไปยังปลายทางและสามารถรับข้อมูลจากปลายทางได้แต่ไม่สามารถทำการส่งและรับข้อมูลได้ในเวลาเดียวกัน
3. Full – Duplex สามารถรับและส่งข้อมูลได้ในเวลาเดียวกัน

นอกจากนี้ยังสามารถแบ่งประเภทของการสื่อสารแบบอนุกรมตามลักษณะสัญญาณการส่งได้อีก 2 แบบ

1. การสื่อสารแบบซิงโครนัส (Synchronous) สำหรับการสื่อสารแบบซิงโครนัสนี้จะใช้สัญญาณนาฬิกาควบคุมการรับส่งสัญญาณ เช่น สายคีย์บอร์ดคอมพิวเตอร์ โดยจะมีสายสัญญาณเส้นหนึ่งเป็น สายสัญญาณนาฬิกา ส่วนอีกเส้นหนึ่งเป็นสายของข้อมูล (และมักมีสายกราวด์ด้วย)



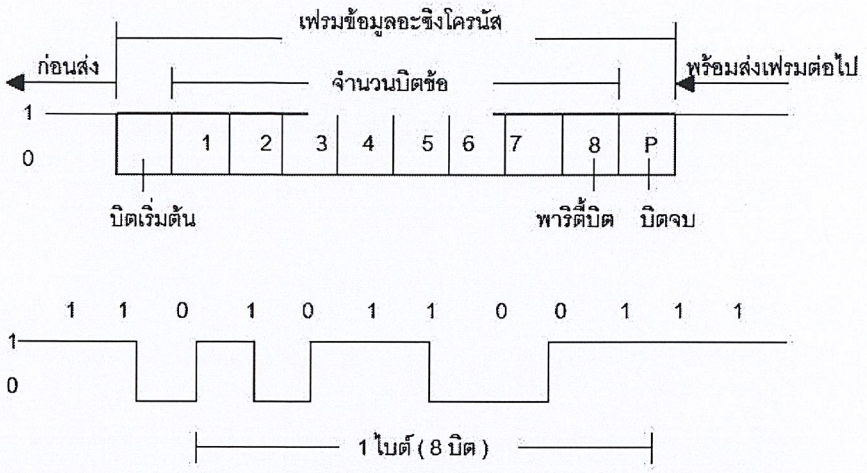
รูปที่ 2.9 ลักษณะสัญญาณของการสื่อสารแบบซิงโครนัส [5]

สำหรับการสื่อสารแบบซิงโครนัสนี้เหมาะสำหรับการทำงานในระยะใกล้ ข้อมูลที่จะส่งมีไม่มากนัก เพราะถ้าระยะทางไกลขึ้นจะทำให้สัญญาณนาฬิกามีปัญหา อีกทั้งต้องมีสายหลายเส้นทำให้สิ้นเปลืองมากขึ้น

2. การสื่อสารแบบอะซิงโครนัส (Asynchronous) สำหรับการสื่อสารแบบอะซิงโครนัสนั้นจะใช้สายข้อมูลเพียงตัวเดียว แต่จะใช้รูปแบบการส่งข้อมูลหรือ Bit Patten เป็นตัวกำหนดว่าส่วนไหนเป็นส่วนเริ่มต้นข้อมูล ส่วนไหนเป็นตัวข้อมูล ส่วนไหนจะเป็นส่วนตรวจสอบความถูก

ต้องของข้อมูลและส่วนไหนเป็นส่วนปิดท้ายของข้อมูลโดยต้องกำหนดให้สัญญาณนาฬิกาเท่ากันทั้งภาคส่งและภาครับ ซึ่งจะมีอุปกรณ์พิเศษที่ชื่อว่า UART หรือ Universal Asynchronous Receiver / Transmitter คอยควบคุมการรับและส่งข้อมูล

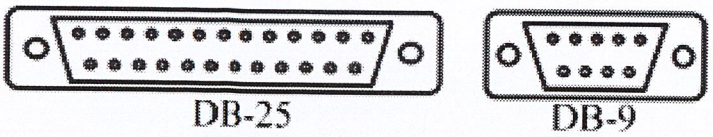
แต่สำหรับมาตรฐานของการส่งข้อมูลแบบอนุกรมอีกแบบ ที่ได้รับความนิยมอย่างสูงตั้งแต่อดีตถึงปัจจุบัน โดยใช้งานกันอย่างแพร่หลายทั้งการสื่อสารและการควบคุมทางอุตสาหกรรมนั้นก็คือมาตรฐาน RS-232



รูปที่ 2.10 ลักษณะสัญญาณของการสื่อสารแบบอะซิงโครนัส [5]

2.3.2 มาตรฐาน RS-232

โดยปกติไมโครคอมพิวเตอร์จะมีพอร์ตอนุกรมที่เรียกว่า RS 232 อยู่ในตัว โดยพอร์ตนี้ทำหน้าที่รับและส่งข้อมูลในแบบอนุกรมเรียกว่า Universal Asynchronous Adapter มาตรฐาน RS 232 ได้จัดพิมพ์ขึ้นเมื่อปี ค.ศ.1969 โดยที่ RS ย่อมาจาก Recommend Standard ส่วน 232 เป็นหมายเลขบ่งบอกของมาตรฐานตัวนี้ส่วน C เป็นหมายเลขท้ายสุดของมาตรฐานฉบับนี้ จุดประสงค์ของมาตรฐานนี้คือเพื่อบรรยายคุณลักษณะของการเชื่อมต่ออุปกรณ์รับส่งข้อมูลปลายทาง (Data Terminal Equipment: DTE) กับอุปกรณ์สื่อสารข้อมูล (Data Communication Equipment : DCE) ซึ่งจะขึ้นอยู่กับผู้ผลิตความเร็วและระยะทางของการเชื่อมต่อ RS232 นั้นสามารถเชื่อมต่อการถ่ายโอนข้อมูลได้ประมาณ 0-20000 บิตต่อวินาที ส่วนความยาวของสายเชื่อมต่อสัญญาณตามมาตรฐานของ RS-232 จำกัดอยู่ที่ 50 ฟุต พอร์ตอนุกรมส่วนใหญ่จะมีรูปร่างขึ้นอยู่กับมาตรฐานของ RS-232 คือ มีขาคอนเนคเตอร์ทั้งแบบ 25 ขาและแบบ 9 ขาแสดงได้ดังรูปที่ 2.11



รูปที่ 2.11 DB25 connector และ DB9 connector [6]

สัญญาณพื้นฐานของ RS-232 ที่กำหนดให้แต่ละขาของคอนเนคเตอร์แสดงดังตารางที่ 2.5

ตารางที่ 2.5 D Type 9 Pin and D Type 25 Pin Connectors

Common Name	Description	Pin numbers 25-pin connector	Pin numbers 9-pin connector
TxD	Transmit Data	2	3
RxD	Receive	3	2
RTS	Request To Send	4	7
CTS	Clear To Send	5	8
DSR	Data Set Ready	6	6
SG	Signal Ground	7	5
CD	Carrier Detect	8	1
DTR	Data Terminal Data	20	4
RI	Ring Indicator	22	9

หน้าที่ของแต่ละขา

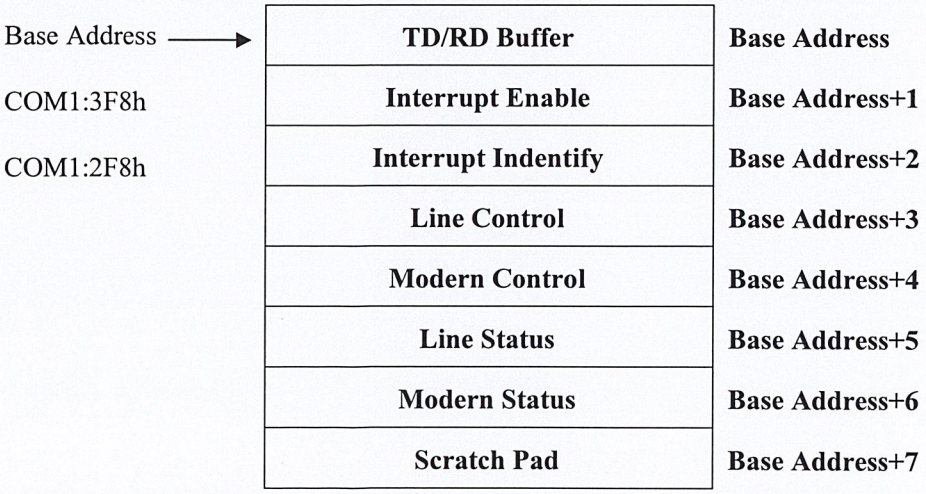
- **Transmit Data (TxD)** เป็นสัญญาณที่ส่งออกจาก DTE(หรือโมโครคอมพิวเตอร์) ไปยังโมเด็มหรือต่อเข้าโดยตรงกับไมโครคอมพิวเตอร์ ข้อมูลแบบอนุกรมจะถูกส่งออกจากคอมพิวเตอร์ด้วยขานี้ สถานะของขานี้จะมีค่าเท่ากับ “1” หรือเทียบเท่ากับบิตหยุด
- **Receive Data (RxD)** เป็นทางของสัญญาณเข้าไปยัง DTE หรือ โมโครคอมพิวเตอร์ ข้อมูลแบบอนุกรมจะรับเข้าเครื่องคอมพิวเตอร์ด้วยขานี้ เมื่อไม่มีสัญญาณเข้ามาขานี้จะมีสภานะทางลอจิกเป็น “1”
- **Request To Send (RTS)** สัญญาณที่ขานี้จะเป็นส่วนที่บอกโมเด็มว่า UART พร้อมที่จะส่งข้อมูลซึ่งขานี้ใช้สำหรับส่งสัญญาณไปยังโมเด็มหรือเครื่องพิมพ์ เป็นการร้องขอที่จะส่งสัญญาณมาทางขา 2 สัญญาณนี้ใช้คู่กับ CTS (Clear To Send) อุปกรณ์รับหากได้

สัญญาณ RTS จะตรวจสอบตัวเองว่าพร้อมจะรับสัญญาณได้หรือยัง หากพร้อมที่จะรับก็จะส่งสัญญาณออกไปที่ขา CTS

- **Clear To Send (CTS)** สัญญาณที่ขานี้จะเป็นส่วนที่แสดงว่าโมเด็มพร้อมที่จะส่งข้อมูล เมื่อสัญญาณนี้อยู่ในสภาวะออฟ (แรงดันมีค่าเป็นลบ หรือ ลอจิก 1) ซึ่งหมายความว่าอุปกรณ์พร้อมที่จะรับข้อมูล
- **Data Set Ready (DSR)** สัญญาณที่ขานี้จะเป็นตัวบอก UART ว่าโมเด็มพร้อมที่จะทำการเชื่อมต่อเมื่อสัญญาณนี้อยู่ในสภาวะออน (ลอจิก 0) เป็นการบอกโมโครคอมพิวเตอร์หรือฝ่ายส่งว่าโมเด็มต่อเข้ากับสายโทรศัพท์เรียบร้อยแล้วและพร้อมที่จะส่งได้แล้ว โมเด็มที่มีการหมุนหมายเลขอัตโนมัติจะส่งสัญญาณนี้ออกไปบอกให้คอมพิวเตอร์รู้ว่าต่อโทรศัพท์ได้สำเร็จแล้ว
- **Signal Ground (SG)** ขากราวนด์ทำหน้าที่เป็นระดับแรงดันอ้างอิงสำหรับทุกๆสัญญาณ
- **Carrier Detect (CD)** โมเด็มจะทำการส่งสัญญาณนี้ให้กับเครื่องคอมพิวเตอร์เมื่อได้รับสัญญาณ Carrier จากโมเด็มปลายทางอีกฝั่งหนึ่ง
- **Data Terminal Ready (DTR)** สัญญาณดังกล่าวจะตรงกันข้ามกับสัญญาณ DSR นั่นคือสัญญาณที่ขานี้จะเป็นตัวบอกโมเด็มว่า UARTพร้อมที่จะทำการเชื่อมต่อ
- **Ring Indicator (RI)** จะทำงานเมื่อโมเด็มได้รับสัญญาณ Ringing จากโครงข่าย PSTN สัญญาณทั้งหมดนี้

การโปรแกรมพอร์ตอนุกรม

รีจิสเตอร์หลักที่ใช้สำหรับการสื่อสารทางพอร์ตอนุกรม RS-232 คือ Line Control Register (LCR) Line Status Register (LSR) และ บัฟเฟอร์ตัวส่งและรับแสดงดังรูปที่ 2.12



รูปที่ 2.12 รีจิสเตอร์หลักในการสื่อสารทางพอร์ตอนุกรม [6]

ตำแหน่งของ Primary Port (COM1) โดยทั่วไปกำหนดไว้ที่ 3F8h และ Secondary Port (COM2) กำหนดไว้ที่ 2F8h ตำแหน่งดังกล่าวนี้จะถูกกำหนดค่าในหน่วยความจำ BIOS และตำแหน่งของแต่ละพอร์ตจะถูกจัดเก็บไว้ที่ตำแหน่งดังตารางที่ 2.6 โดยที่แต่ละพอร์ตจะมีค่าตำแหน่งและอินเตอร์รัพเป็นค่าเฉพาะตัวเพื่อไม่ให้สับสนในการติดต่อกับอุปกรณ์อื่น

ตารางที่ 2.6 แสดงค่าตำแหน่งและ IRQ ของแต่ละ COM port ต่างๆ

Name	ADDRESS	IRQ
COM1	3F8	4
COM2	2F8	3
COM3	3F8	4
COM4	2F8	3

ค่าตำแหน่งของ COM Port นี้จะเป็น Base Address ในการอ้างอิง Register ที่ใช้ในการควบคุมและเก็บค่าสถานะการทำงานของชิพ UART ซึ่งจะมีค่ารีจิสเตอร์ที่เกี่ยวข้องอยู่ทั้งหมด 8 ตัว โดยจะเข้าถึงรีจิสเตอร์เหล่านี้ได้โดยการใช้คำสั่ง inportb () และ outportb () ของภาษา C ดังตารางที่ 2.7 DLAB (Divisor Latch Access Bit) จะเป็นตัวเลือกในการเข้าถึงรีจิสเตอร์ว่าจะทำหน้าที่ใดซึ่งจะถูกกำหนดโดย LCR

ตารางที่ 2.7 แสดงตำแหน่งของรีจิสเตอร์ต่างๆที่เกี่ยวข้องกับ COM PORT

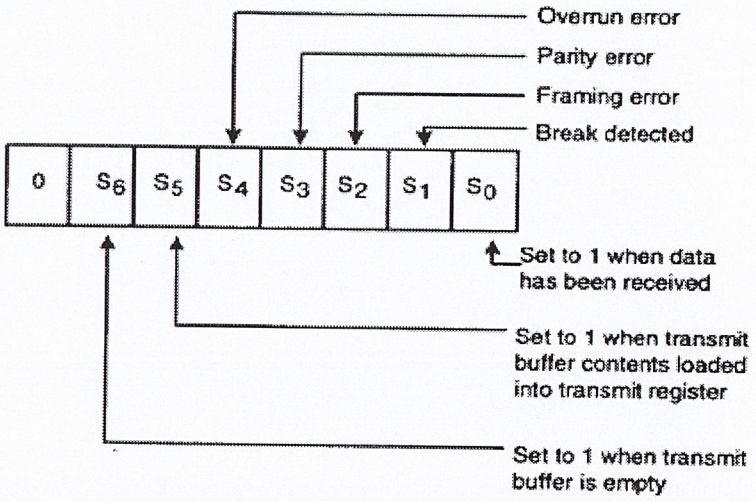
Base Address	DLAB	Read/Write	Abr.	Register Name
+0	=0	Write	-	Transmitter Holding Buffer
	=0	Read	-	Receiver buffer
	=1	Read/Write	-	Divisor Latch Low Byte
+1	=0	Read/Write	IER	Interrupt Enable Register
	=1	Read/Write	-	Divisor Latch High Byte
+2	-	Read	IIR	Interrupt identification Register
	-	Write	FCR	FIFO Control Register
+3	-	Read/Write	LCR	Line Control Register
+4	-	Read/Write	MCR	Modern Control Register
+5	-	Read	LSR	Line Status Register

ตารางที่ 2.7 แสดงตำแหน่งของรีจิสเตอร์ต่างๆที่เกี่ยวข้องกับ COM PORT (ต่อ)

+6	-	Read	MSR	Modern Status Register
+7	-	Read/Write	-	Scratch Register

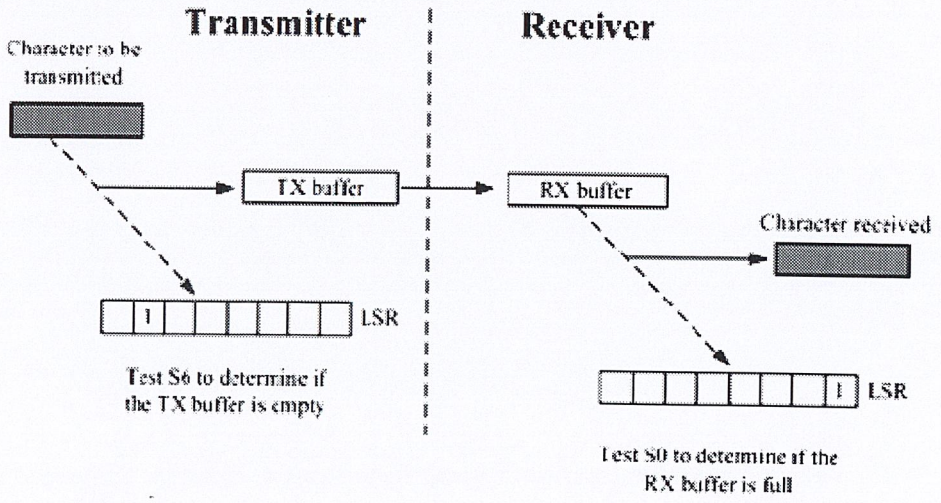
Line Status Register (LSR)

LSR เป็นรีจิสเตอร์ในการกำหนดสถานะของการบัฟเฟอร์ส่งและรับ เมื่อมีความผิดพลาดเกิดขึ้นในการส่งบิตที่แสดงการผิดพลาดจะถูกกำหนดให้เป็น "1" โดยบิตต่างๆแสดงดังรูปที่ 2.13



รูปที่ 2.13 รีจิสเตอร์ LSR [6]

ในการส่งข้อมูลจะต้องมีการตรวจสอบเพื่อป้องกันการทับกันของข้อมูลในบัฟเฟอร์โดยการตรวจสอบที่บิต 6 S โดยที่เมื่อบิตนี้เป็น "1" เมื่อบิตนี้ว่าง



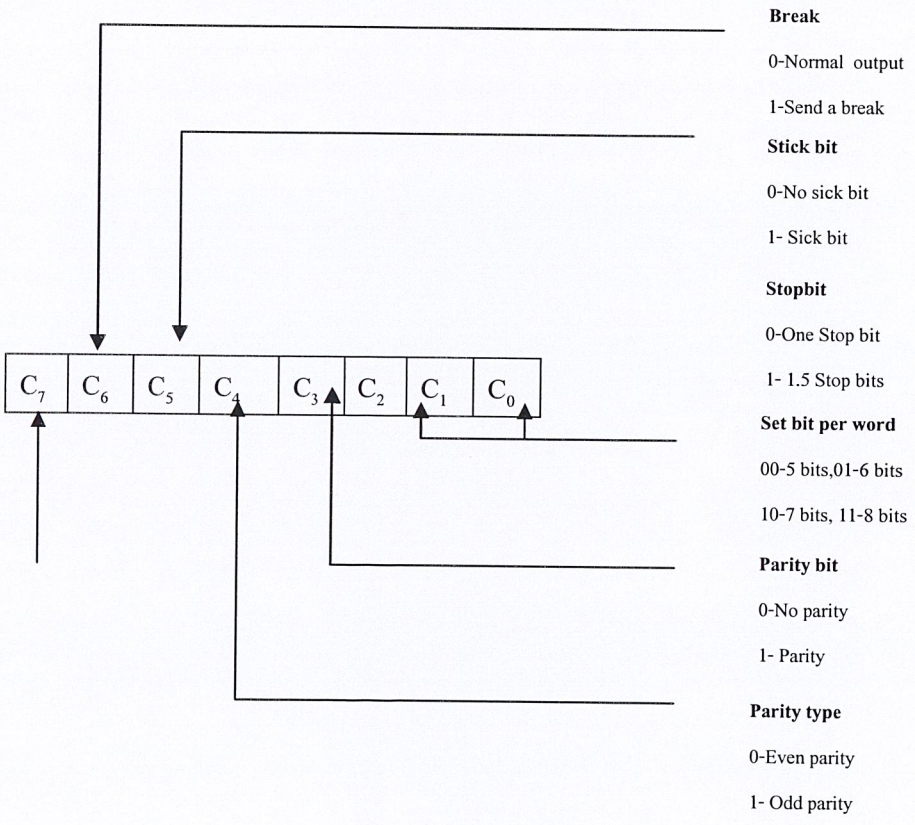
รูปที่ 2.14 แสดงค่าในรีจิสเตอร์ LRS ในกรณีที่มีการรับและส่งข้อมูล [6]

Line Control Register (LCR)

LCR เป็นรีจิสเตอร์ในการกำหนดค่าต่างๆในการสื่อสาร ซึ่งประกอบไปด้วยจำนวนของบิตต่อตัวอักษร จำนวนพาริตี้บิต จำนวนของ stop bit โดย MSB (C7) บิตจะถูกกำหนดให้เป็นค่า "0" เพื่อการเข้าถึงรีจิสเตอร์ที่ใช้ส่งและรับ ในกรณีกลับกันถ้าถูกกำหนดให้เป็น "1" จะเป็นการกำหนดอัตราบอด อัตราบอดกำหนดได้โดยการโหลดตัวหารขนาด 16 บิตเข้าสู่ตำแหน่งบัฟเฟอร์ที่ใช้ในการส่งและรับรวมทั้งตำแหน่งถัดไปด้วย ค่าที่จะทำการโหลดนั้นขึ้นอยู่กับความถี่ของคริสตัลที่ต่ออยู่กับ IC อัตราบอดสามารถคำนวณได้ดังสมการ (2)

$$Baud\ rate = \frac{clock\ \ frequency}{16 \times N} \qquad (2)$$

ตัวอย่างเช่นต้องการส่งข้อมูล 9600 บอด สามารถคำนวณหาค่า N ได้เท่ากับ $\frac{1.8432 \times 10^6}{9600 \times 16} = 12(000Ch)$ ในตารางที่ 2.8 แสดงถึงการกำหนดอัตราบอดต่างๆ



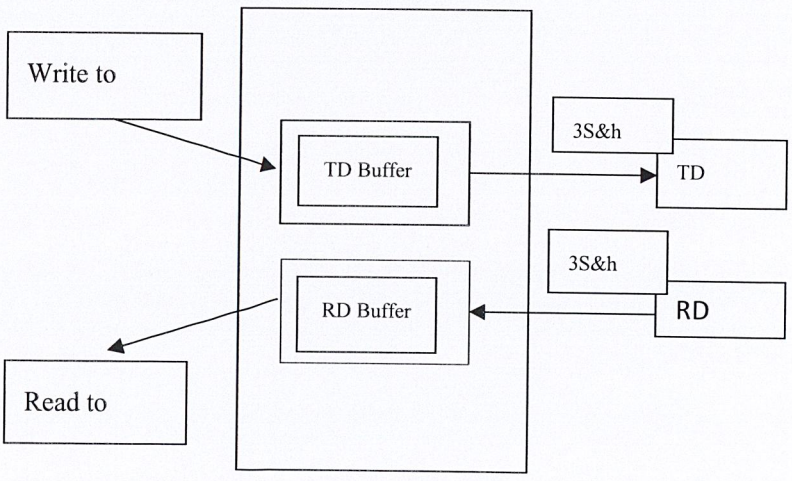
รูปที่ 2.15 รีจิสเตอร์ LRS [6]

ตารางที่ 2.8 แสดงค่าที่ใช้ในการกำหนดอัตราบอด

Speed(BPS)	Divisor(Dec)	Divisor Latch High Byte	Divisor Latch Low Byte
50	2304	09h	00h
300	384	01h	80h
600	192	00h	C0h
2400	48	00h	30h
4800	24	00h	18h
9600	12	00h	0Ch
19200	6	00h	06h
38400	3	00h	03h
57600	2	00h	02h
115200	1	00h	01h

ตำแหน่งรีจิสเตอร์

ตำแหน่งของรีจิสเตอร์หลักแสดงดังรูปที่ 2.15 ในการที่จะโหลดตัวหารเพื่อกำหนดอัตราบอดนั้นเริ่มแรกทำการกำหนดให้บิตที่ 7 ของรีจิสเตอร์ LCR เป็น “1” จากนั้น LSB จะถูกโหลดเข้าตำแหน่งตัวหารของ LSB และ MSB เข้าสู่ตำแหน่งของตัวหารของรีจิสเตอร์ MSB ขั้นสุดท้ายทำการกำหนดบิตที่ 7 ของรีจิสเตอร์ LCR ให้กลับมาเป็นเลข “0” เมื่อบิตที่ 7 ถูกกำหนดให้เป็น “0” การอ่านข้อมูลจากตำแหน่งหลักจะอ่านจากบัฟเฟอร์ RD และการเขียนจะทำการเขียนไปยังบัฟเฟอร์ TD ดังรูปที่ 2.16

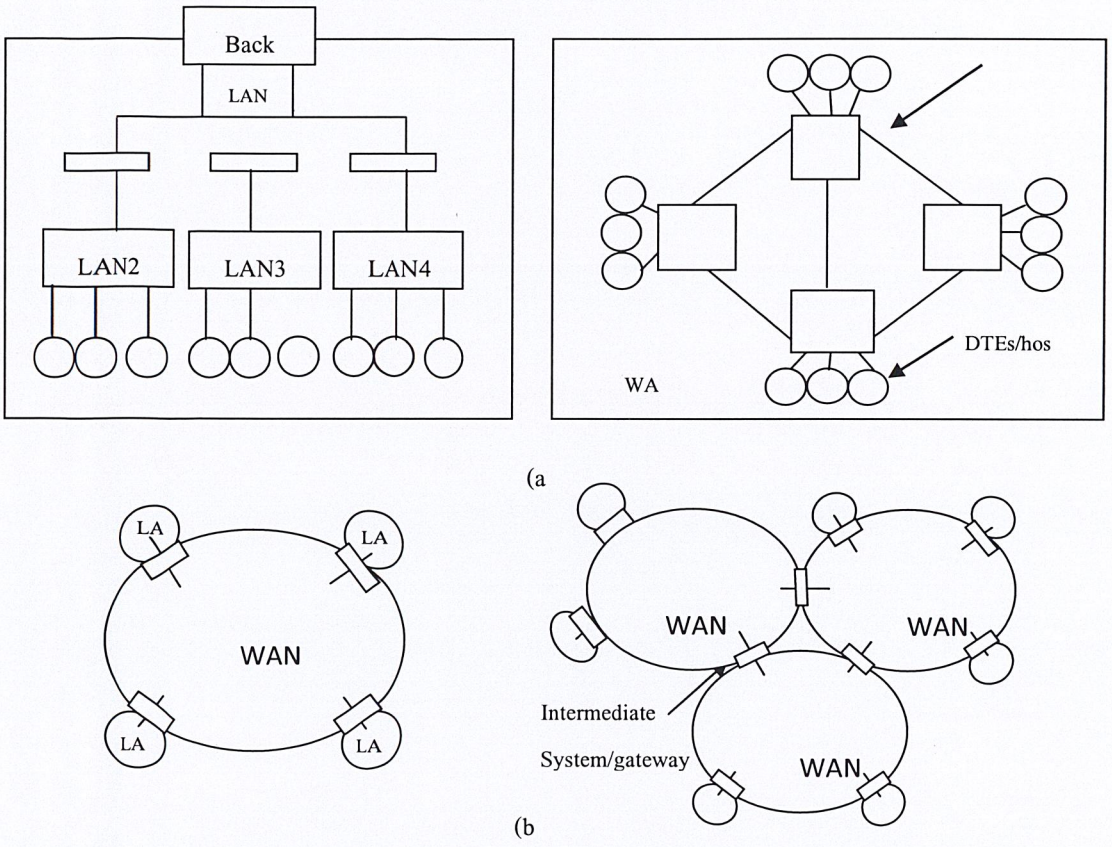


รูปที่ 2.16 การอ่านและเขียนข้อมูลจากบัฟเฟอร์ TD/RD [6]

2.4 เครือข่ายอินเตอร์เน็ต

อินเตอร์เน็ต (Internet) คือ การที่เครือข่ายสองเครือข่ายหรือมากกว่า เชื่อมต่อเข้าด้วยกัน และการทำงานเสมือนเป็นเครือข่ายเดียวกัน โยงเน็ตเวิร์คที่เป็นส่วนประกอบของอินเตอร์เน็ตคือ subnetwork (subnet) ซึ่งอาจเป็นเครือข่าย Local Area Network (LAN) หรือ Wide Area Network (WAN) อุปกรณ์ที่ใช้ในการเชื่อมต่อสองเครือข่ายเข้าด้วยกันก็คือ Intermediate System (IS) หรือ Internetworking (IWU) การเชื่อมโยงระหว่างระบบที่แตกต่างกัน จำเป็นต้องมีมาตรฐานการติดต่อกัน ซึ่งเรียกเป็นศัพท์เฉพาะว่าโพรโตคอล (Protocol)

2.4.1 สถาปัตยกรรมอินเตอร์เน็ต (Internet Architectures)

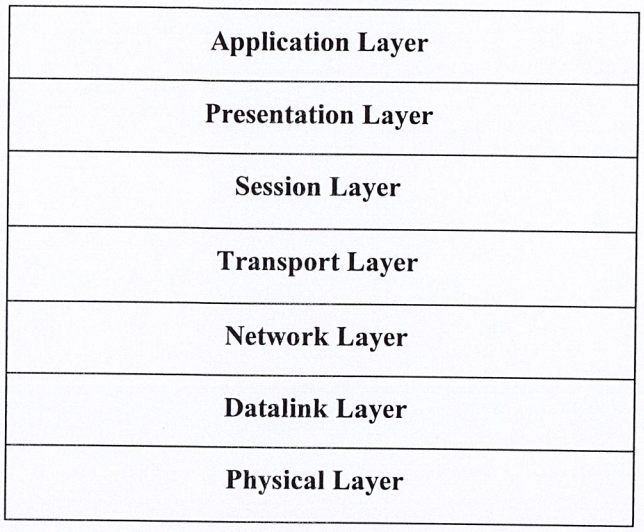


รูปที่ 2.17 แสดงสถาปัตยกรรมของอินเตอร์เน็ต [7]

ในรูป (a) แสดงตัวอย่าง 2 ตัวอย่างของเครือข่ายเดี่ยว (Single Network) ซึ่งอย่างแรกเป็น Site-wide LAN ซึ่งประกอบขึ้นจากชัดของแลนซึ่งถูกต่อเข้ากับเครือข่ายหลัก (Backbone) อุปกรณ์ที่ใช้ต่อแลนกับเครือข่ายหลัก ถ้าแลนทุกเครือข่ายใช้ระบบเดียวกันก็จะใช้ Bridge ถ้าต่างชนิดกันก็จะใช้ Router ตัวอย่างที่ 2 เป็นตัวอย่างของ WAN เดี่ยวๆในรูป (b) แสดงถึงเครือข่ายอินเตอร์เน็ตซึ่งประกอบไปด้วย Network ทั้ง 2 ชนิดข้างต้น

2.4.2 OSI โมเดล

องค์ประกอบมาตรฐานสากล ISO (International Organization for Standardization) ได้กำหนดมาตรฐานของเครือข่าย โดยจัดแบ่งตามกิจกรรมของเครือข่าย ออกเป็นงานย่อยๆ และกำหนดโมเดลแบ่งเป็นชั้นๆ ตามลำดับ เรียกว่ามาตรฐาน OSI (Open System Interconnection) โดยที่จะแบ่งกิจกรรมที่ซับซ้อนในเครือข่ายออกเป็นงานย่อยๆ ซึ่งช่วยให้การออกแบบ ในการใช้งานเครือข่ายรวมถึงการเชื่อมโยงกันเป็นไปได้ด้วยความสะดวกและมีวิธีการทำงานอยู่ในกรอบเดียวกัน



รูปที่ 2.18 แสดงการแบ่งเครือข่ายออกเป็น OSI โมเดล [7]

ในแต่ละชั้นของ OSI โมเดล จะมีการติดต่อสื่อสารเป็นชั้นๆ ตามลำดับลงมาเช่น Application Layer ก็จะสื่อสารกับ Presentation Layer ตามลำดับจนไปถึงขั้นล่างสุด คือ Physical Layer

Application Layer เป็นชั้นบนสุดของโมเดล เป็นส่วนที่ทำให้การติดต่อสื่อสารระหว่างเครือข่ายกับผู้ใช้เป็นไปตามต้องการ ตัวอย่าง แอปพลิเคชั่นของเครือข่ายเช่น ระบบ E-mail, File Transfer และการขอเข้าใช้ระบบคอมพิวเตอร์ในเครือข่าย เป็นต้น Presentation Layer มีการกำหนดหน้าที่ไม่ชัดเจน และมีการนำไปใช้ไม่มาก ซึ่งหน้าที่หลักก็คือ เป็นส่วนที่จัดรูปและนำเสนอข้อมูลให้เป็นไปตามต้องการ รวมถึงการแปลงข้อมูล ในรูปมาตรฐาน ASCII หรือ EBCDIC การลดขนาดข้อมูล (Data Compression) การเข้ารหัสหรือ Session ให้ระบบคอมพิวเตอร์ทั้งสองฝั่งโดยทำหน้าที่ตั้งแต่เริ่มการติดต่อ ดูแลการส่งข้อมูลในการติดต่อครั้งนั้นๆ เป็นไปโดยไม่เกิดปัญหา จนถึงเลิกการติดต่อเมื่อเสร็จงาน

Transport Layer ทำหน้าที่ควบคุมปริมาณ และรายละเอียดการรับส่งข้อมูลให้เป็นไปตามกำหนดที่ตั้งไว้ และจัดการให้การเชื่อมโยงเครือข่ายเป็นไปด้วยความราบรื่น Transport Layer

จะเป็นชั้นสุดท้ายที่จัดการเรื่องเส้นทางในการรับ-ส่งข้อมูล และจัดการตรวจสอบความผิดพลาดของข้อมูล ซึ่งส่วนของ TCP (Transmission Control Protocol) ในโพรโตคอล TCP/IP ทำงานในระดับนี้

Network Layer ทำหน้าที่ควบคุมวิธีการส่งผ่านข้อมูลระหว่างเครือข่ายให้ถูกต้อง และเป็นไปตามเส้นทางที่กำหนด โดยจะจัดส่งผ่าน Package ข้อมูลผ่านอุปกรณ์ต่างๆ ไปยังเครือข่ายย่อยได้อย่างถูกต้องตามที่ต้องการ นอกจากนี้ยังจัดการดูแลเส้นทางในการส่งข้อมูล (Routing Table) และกลั่นกรอง Package ข้อมูลที่ส่งไปยังเครือข่ายเดียวกันไม่ให้ข้ามไปยังเครือข่ายอื่น ซึ่งจะช่วยลดปริมาณข้อมูลที่วิ่งบนเครือข่ายได้ส่วนหนึ่ง โพรโตคอล IP,TCP/IP และ IPX เป็นโพรโตคอลที่ทำงานอยู่ในเลเยอร์นี้

Data Link Layer ทำหน้าที่เรียกใช้งานหรือกำหนดช่องทางในการรับส่งข้อมูลที่ถูกต้อง เช่น Ethernet,Tokenring หรือ FDDI เป็นต้น รวมถึงลำดับและอัตราการรับ-ส่งข้อมูลหรือ Flow Control และสถานที่ที่จะส่งข้อมูลไป (Address) ทั้งนี้ Data Link Layer จะเป็นชั้นแรกที่จัดการแปลงข้อมูลจากบิตให้เป็นแพ็คเกจ โดยจะมีการเพิ่มข้อมูลเพื่อตรวจสอบผ่าน Checksum เพื่อดูว่าข้อมูลที่ได้รับมาถูกต้องครบถ้วน และถ้าได้รับแพ็คเก็จข้อมูลที่ไม่ถูกต้องก็จะเอาข้อมูลนั้นมาใช้งาน และบอกต้นทางส่งข้อมูลเดิมมาใหม่

Physical Layer รับผิดชอบดูแลในรายละเอียดในการส่งข้อมูลในด้านฮาร์ดแวร์ เช่น การควบคุม Network Interface Card การส่งสัญญาณแบบต่างๆ การเชื่อมต่อเข้ากับเครือข่ายต่างๆ โดยใช้ Physical Layer จะจัดสร้างสัญญาณทางไฟฟ้า หรือสัญญาณเสียง หรือสัญญาณที่จำเป็นในการสื่อสารโดยตรง

เนื่องจาก Network Layer ในแต่ละ End System (ES) จะเป็นตัวจัดการติดต่อแบบ end-to-end ของการบริการ Inter wide ไปยังผู้ใช้บริการ (NS-User)

โดย ISO ได้จัด Network Layer เป็น 3 โพรโตคอล (Sub Layer) ซึ่งทำงานร่วมกันเพื่อให้บริการใน Network Layer ได้แก่

- Sub Network Independent Convergence Protocol (SNICP)
- Sub Network Dependent Convergence Protocol (SNDCP)
- Sub Network Dependent Access Protocol (SNDAP)

โดยที่ SNICP จะเป็นตัวสนับสนุนการจัดการให้ผู้ใช้บริการ (NS-User) สามารถอินเตอร์เฟสกับอินเตอร์เน็ต ซึ่งมันจะมีหน้าที่เป็นตัวประสานฟังก์ชั่นต่างๆ ที่จำเป็นในการเลือกเส้นทางและการถ่ายข้อมูลของผู้ใช้ข้ามอินเตอร์เน็ต ซึ่งการทำงานไม่ขึ้นอยู่กับคุณสมบัติเฉพาะของเครือข่ายย่อย (Subnet)

SNDAP จะเป็นโพรโตคอลที่ติดต่อกับเครือข่าย (Subnet) ที่มีลักษณะเฉพาะในอินเตอร์เน็ต เช่น X.25 Packet Layer Protocol สำหรับเครือข่าย X.25 ซึ่งใช้บ่อยใน LAN เพราะว่า

การบริการและการทำงาน SNDAP แตกต่างจากเน็ตเวิร์คแบบอื่นๆ Sublayer ที่อยู่ตรงกลางคือ SNDCP จะเป็นตัวจัดการระหว่าง SNICP และ SNDAP

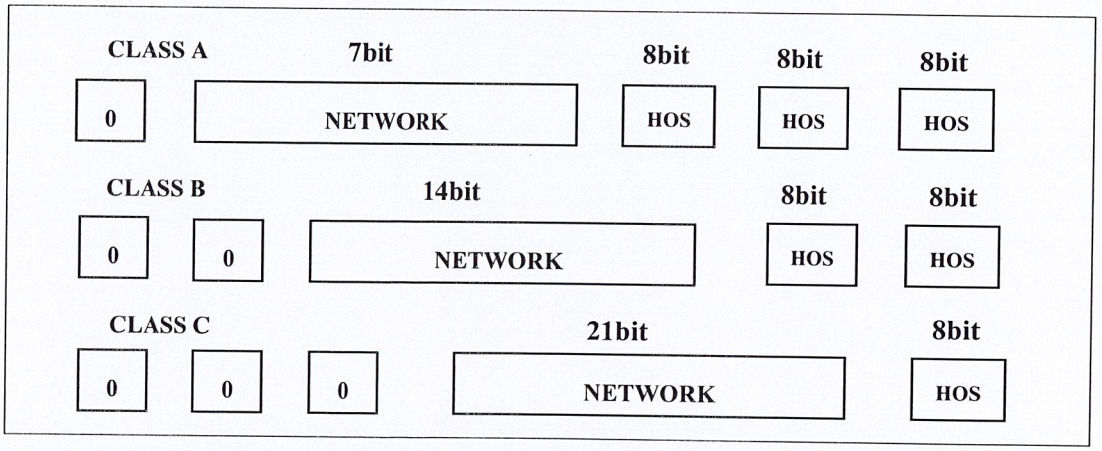
2.4.3 รูปแบบมาตรฐานโพรโตคอลของอินเตอร์เน็ต (Internet Protocol Standards)

อินเตอร์เน็ตโพรโตคอลที่ถูกใช้ในอินเตอร์เน็ต คือ TCP/IP (Transfer Control Protocol / Internet Protocol) ซึ่งรวมถึง Transport และ Application โพรโตคอล ซึ่งทั้งหมดของ TCP/IP จะกำหนด ให้เหมาะสมกับการใช้เชิงสาธารณะ โดย IP เป็น Internetwide Protocol ซึ่งทำให้ทั้งสอง Transport Protocol ที่ต่างสถานที่กันและต่าง Ess/Hosts กันสามารถแลกเปลี่ยนหน่วยข้อมูล (NSDUS) กันได้ ซึ่งหมายถึงว่าหลายๆ Network/Subnet และ ISO/Gateway ที่แตกต่างกันสามารถติดต่อสื่อสารกันได้อย่างสมบูรณ์

2.4.4 Internet IP

2.4.4.1 Address Structure

ในศัพท์ของ ISO เมื่อ 2 Network ติดต่อกันด้วย Host/ES ที่ติดกับอินเตอร์เน็ต Network เหล่านี้ ติดต่อกันโดยใช้ Network Service Access Point (NSAP) Address และ Subnet Point of Attachment (SNPA) สำหรับใน TCP/IP ก็จะมี IP Address และ NPA Address ตามลำดับ โดย NPA Address จะแตกต่างกันในแต่ละชนิดของ Network/Subnet และ IP Address ตามลำดับ โดย NPA Address จะเป็นรูปแบบเดียวกัน โครงสร้าง IP Address ดังรูป 2.23



รูปที่ 2.19 โครงสร้าง Address ที่ใช้ใน Class ต่างๆของเครือข่ายโดยมีทั้งหมด 32 บิต [7]

IP Address นี้มีการจัดแบ่งออกเป็นทั้งหมด 5 ระดับ (Class) แต่ที่ใช้งานทั่วๆไปจะมีเพียง 3 ระดับ โดยคอมพิวเตอร์ที่เชื่อมต่ออยู่มาก จะมีหมายเลขอยู่ใน Class A และลดหลั่นกันมาใน Class B และ Class C ตามลำดับ

ดังรูปที่ 2.19 จะเห็นว่าหมายเลข IP ของ Class A มีตัวแรกเป็น 0 และหมายเลขเครือข่าย (Network Number) ขนาด 7 บิต และมีหมายเลขเครื่องคอมพิวเตอร์ (Host Number) ขนาด 24 บิต ทำให้ในหนึ่งเครือข่ายของ Class A สามารถ มีคอมพิวเตอร์เชื่อมต่ออยู่ในเครือข่ายถึง 234 = 16 ล้านเครื่อง แต่ใน Class A จะมีหมายเลขเครือข่ายได้ 128 เครือข่ายแบบนี้เพียง 128 เครือข่ายเท่านั้น

สำหรับ Class B จะมีหมายเลขเครือข่ายแบบเครื่องคอมพิวเตอร์แบบ 16 บิต โดย 2 บิตแรก บังคับว่าต้องเป็น 10 (ในเลขฐาน 10) จึงทำให้มีเครื่องคอมพิวเตอร์ในเครือข่ายแบบนี้ได้ 64K เครื่อง

จะเห็นได้ว่าเมื่อเครือข่ายและเครื่องคอมพิวเตอร์ทีต่ออยู่ในอินเตอร์เน็ต มีหมายเลข IP Address ให้ใช้อ้างอิงได้ไม่ซ้ำกัน และมีความหมายให้ทราบถึงขนาดเครือข่าย และการติดต่อส่งผ่านข้อมูลจึงกระทำได้โดยไม่สับสน

2.4.4.2 รูปแบบของข้อมูล (Datagram)

รูปแบบของ IP data unit ก็คือ Datagram ซึ่งโครงสร้างของ Datagram เป็นดังรูปที่ 2.20

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td colspan="6">Version</td><td colspan="5">Header Length</td><td colspan="5">Type of service</td></tr>
<tr><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">Identification</td></tr>
<tr><td colspan="2">D</td><td colspan="2">M</td><td colspan="12">Fragment offset</td></tr>
<tr><td colspan="7">Time to live</td><td colspan="9">Protocol</td></tr>
<tr><td colspan="16">Header checksum</td></tr>
<tr><td colspan="16">Source IP Address</td></tr>
<tr><td colspan="16">Destination IP Address</td></tr>
<tr><td colspan="16">Option</td></tr>
<tr><td colspan="16">Data (65536 byte)</td></tr>
</table>

รูปที่ 2.20 Internet Datagram Format and Contents [7]

หน่วยข้อมูล IP (IP Datagram) แต่ละหน่วยจะประกอบด้วย ส่วนของข้อมูลที่รับมาจากส่วนของงาน TCP/IP หรือ UDP และส่วนของข้อมูลนำทาง (Header) ซึ่งมีรายละเอียดดังนี้

Version	รุ่นของข้อกำหนด IP
Header Length	ความยาวของข้อมูลนำทาง
Type of Service	วิธีการจัดเก็บข้อมูล
Total Length	ความยาวของหน่วยข้อมูล
Identification, Flags และ Fragment Offset	รายละเอียดที่เกี่ยวข้องกับการแบ่งย่อยข้อมูล ซึ่งจะถูกใช้ในการรวบรวมข้อมูล
Time to live	เวลาสูงสุดที่ใช้ในการเดินทาง ซึ่งกำหนดมาจากต้นทางโดยเวลาจะลดลงเรื่อยๆ ระหว่างทาง ถ้าลดลงถึง 0 หน่วย ข้อมูลนั้นจะถูกกำจัดไป
Protocol	ชนิดของข้อมูล UDP หรือ TCP
Header Checksum	ค่าตรวจสอบข้อมูลนำทาง
IP Address	หมายเลย Internetwide IP (NSP) ของเครื่องต้นทางและปลายทาง
Option	ข้อมูลอื่นๆ เช่น ข้อมูลเกี่ยวกับการรักษาความปลอดภัยบันทึกเส้นทางเดินของข้อมูล เวลาที่ข้อมูลนั้นมาถึง เป็นต้น

2.4.5 การแบ่งส่วนของข้อมูลและการประกอบขึ้นใหม่

ขนาดของข้อมูลของผู้ใช้ซึ่งอ้างอิง NSDU มีความจุได้ถึง 64 K หรือ 65536 bytes ต่อขนาดของหน่วยข้อมูล (Packet size) ที่สามารถติดต่อกันในระบบที่ต่างกันได้ตั้งแต่ 128 bytes สำหรับระบบ X.25 Packet Switching จนถึง 8000 bytes สำหรับบาง LAN ดังนั้นกระบวนการ Fragmentation และ Reassemble จึงถูกนำมาใช้เพื่อ ทำให้ขนาดของข้อมูลเล็กลง และสามารถส่งไปในระบบได้ และเมื่อถึงปลายทางไอพีก็จะทำการประกอบข้อมูล (Reassemble) ขึ้นมาใหม่ก่อนที่จะส่งผ่านไปยังผู้ใช้

อันดับแรกไอพีในโฮสต้นทางจะแยกข้อมูลของผู้ใช้ (NS-User), NSDU เป็น Datagram ซึ่งมี แอดเดรสไปยังไอพีในเกตเวย์ตัวแรกโดยไอพีในเกตเวย์จะไม่ Reassemble NSDU แต่จะปรับปรุงในขอบเขตที่เหมาะสม และส่ง Datagram ที่ได้รับไปยังเน็ตเวิร์คที่สอง (ถ้าเน็ตเวิร์คที่สองสามารถรองรับขนาดของ Datagram นี้) หรือทำการ Fragment Datagram ให้มีขนาดเล็กลง ซึ่งขั้นตอนนี้จะถูกทำซ้ำที่ เกตเวย์ตัวต่อไปเน็ตเวิร์คตัวสุดท้ายสามารถรองรับขนาดของแพ็คเก็จมากกว่าแพ็คเกจที่มันได้รับข้อมูล จึงถูกส่งได้โดยตรง โดยที่จะมีการปรับปรุงในบางส่วน Header

ของ Datagram เท่านั้น จากนั้น ไอพีในโฮสต์ปลายทางจะทำการประกอบข้อมูล (Reassemble) ที่ได้รับขึ้นมาใหม่และส่งผลที่ได้ (NSDU) ไปยังผู้ใช้ (NS-User)

ในการคิดค่าเวลาสูงสุดที่โฮสต์ต้นทางกำหนดให้เกตเวย์รอ Datagram (NSDU) ระหว่างการ Reassemble ซึ่งก็คือ Time to live ซึ่งจะถูกต้องโดยค่า IP ใน Host ต้นทาง ซึ่งจะมีค่าลดลงเรื่อยๆในแต่ละขั้นตอนของการ Process Datagram ตัวใหม่ ถ้ามันมีค่าถึง 0 ที่จุดใดๆ ระหว่างการ Process ในเกตเวย์หรือโฮสต์การ Reassemble ก็จะล้มเหลว และทุกๆการ Fragment ที่เกี่ยวกับ NSDU ก็จะถูกตัดทิ้ง

ค่า Time to live ในแต่ละ Datagram จะเป็นจำนวนเท่าของวินาที โดยที่จำนวนของมันจะถูกลดลงโดยแต่ละไอพีซึ่งจะเปลี่ยนแปลงไปตามค่าเวลาจริงในการส่งถ่ายข้อมูลของเน็ตเวิร์คที่ติดต่อด้วย

2.4.6 การเลือกเส้นทาง (Routing)

ในแต่ละเน็ตเวิร์ค (Subnet) ในอินเตอร์เน็ตจะมีชนิดของ PA Address ที่แตกต่างกัน ซึ่งระบบ (System Host) หรือเกตเวย์ที่ถูกต่อเข้ากับเน็ตเวิร์คจะสามารถส่ง Datagram ไปยังระบบอื่นได้ โดยตรงเฉพาะเน็ตเวิร์ค ที่เหมือนกันเท่านั้น ในการเลือกเส้นทาง (Routing) ให้ Datagram ข้ามไปยังหลายๆ Network IP ในแต่ละ Internetwide Gateway ต้องรู้ PA Address ของโฮสต์ปลายทาง

ซึ่งมี 2 วิธีการพื้นฐานที่ถูกใช้ในการหาเส้นทางภายในอินเตอร์เน็ตคือ Centralized และ Distributed ด้วยวิธีการ Centralized Routing ข้อมูลเกี่ยวกับการเลือกเส้นทางที่เกี่ยวข้องกับแต่ละเกตเวย์จะถูกดาวน์โหลดจาก Site ส่วนกลางโดยข้อมูล Network และ Special Network Management จะพยายามตรวจสอบเน็ตเวิร์คและโฮสต์ที่ถูกเพิ่มเข้า และถอดออกและข้อบกพร่องที่ถูกวินิจฉัยจะถูกถอดออก ในขณะที่ถูกตรวจสอบ

ด้วยวิธีการ Distributed Routing ทุกๆโฮสต์ และเกตเวย์จะร่วมกันในการแบ่งปัน ข้อมูลเกี่ยวกับการเลือกเส้นทางที่จะถูกจดจำไว้โดยแต่ระบบ ในรูปของ Routing Table ซึ่งจะมี NPA Address ไว้ในการส่งแต่ละ Datagram ซึ่งอินเตอร์เน็ตจะใช้วิธีการแบบนี้

ขั้นตอนการ Routing ที่เกี่ยวกับไอพีขั้นแรกจะอ่าน IP Address (NSAP) ปลายทางจากภายใน Datagram และใช้มันในการหาการตอบสนอง PA Address ของโฮสต์หรือเกตเวย์จาก Routing Table ในส่วนที่เพิ่มเติมชุดของ Routing Protocol จะถูกใช้เพิ่มและรักษาส่วนที่อยู่ในแต่ละ Routing Table ในแบบของ Distributed ซึ่งรูปแบบทั่วไปถูกใช้ภายใน Host IP

2.5 ระบบข้อความสั้น (Short Message Service : SMS)

SMS หรือ การส่งข้อความสั้นโดยลักษณะของการส่งข้อความสั้นจะมีลักษณะคล้ายกับการส่งข้อความไปยังเพจเจอร์ คือ ผู้ใช้สามารถส่งข้อความไปยังผู้รับ โดยที่ผู้รับสามารถกดอ่านได้

จากเครื่องโทรศัพท์มือถือได้ทันที ข้อดีของ SMS ที่ทำให้ต่างกับเพจเจอร์ก็คือ ผู้ใช้หรือผู้ที่ต้องการส่งข้อความสามารถพิมพ์ข้อความได้เองจากโทรศัพท์มือถือ และสามารถส่งไปยังโทรศัพท์มือถือของผู้รับได้ทันที SMS เป็นบริการมาตรฐาน ในการรับส่งข้อความระหว่างโทรศัพท์เคลื่อนที่ และอุปกรณ์อื่นๆสามารถส่งได้ในรูปแบบของ ตัวเลข ตัวอักษร และสัญลักษณ์ต่าง ๆ SMS ได้ถูกสร้างขึ้นมาครั้งแรกให้ทำงานร่วมกันโทรศัพท์เคลื่อนที่แบบดิจิตอล ระบบ GSM โดยข้อความแรก ได้ถูกส่งในเดือนธันวาคม 1992 จากเครื่องคอมพิวเตอร์ส่วนบุคคลไปสู่เครื่องโทรศัพท์เคลื่อนที่บนโครงข่ายระบบ GSM ของ Vodafone ในประเทศอังกฤษ ปัจจุบันบริการ SMS สนับสนุนโครงข่าย GSM,CDMA และ TDMA สำหรับการส่ง SMS ภาษาไทยจะส่งได้ 70 ตัวอักษร ภาษาอังกฤษส่งได้ 160 ตัวอักษรเนื่องจาก การรับ-ส่ง SMS เป็นเทคนิคการสื่อสารที่ไม่จำเป็นต้องใช้การสร้างวงจรสนทนา (Call Set-up) จึงทำให้สามารถรับหรือส่งข้อความได้ในขณะที่กำลังสนทนาอยู่ หรือในขณะที่เปิดเครื่องทิ้งไว้ บริการ SMS ไม่ใช่บริการแบบ real-time เนื่องจากการส่งข้อความต้องส่งผ่าน Platform กลาง คือ Short Message Service Center หรือ SMS-C ซึ่งเป็นอุปกรณ์ที่ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ติดตั้งไว้เพื่อให้บริการรับ-ส่งข้อความผ่านทางเครื่องลูกข่ายโทรศัพท์เคลื่อนที่ไปสู่เครื่องลูกข่ายเครื่องอื่น ๆ ได้

2.5.1 หลักการทำงานของ SMS

SMS ย่อมาจาก Short Message Service เป็นบริการส่งข้อความสั้นๆจากโทรศัพท์มือถือต้นทางผ่านชุมสายไปยังโทรศัพท์มือถือปลายทาง โดยสามารถส่งได้สูงสุด 160 ตัวอักษรต่อครั้งตามข้อกำหนดมาตรฐานขององค์การ ETSI (European Telecommunications Standards Institute) นอกจากนี้ยังสามารถส่งข้อความไปที่เครื่อง Fax , PC หรือ Internet address ได้อีกด้วย

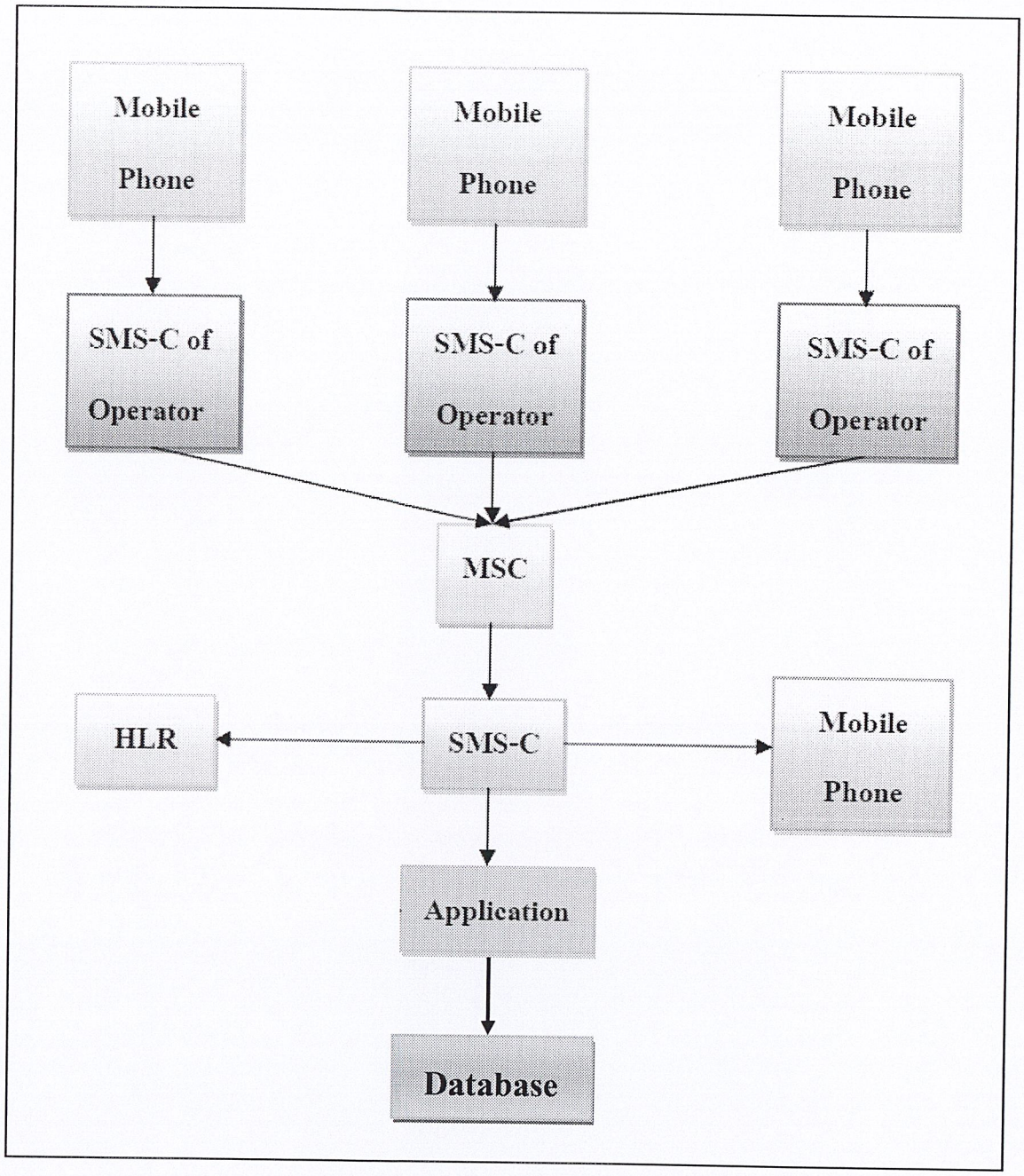
ระบบ SMS ในระบบเครือข่ายโทรศัพท์มือถือ รองรับโดยระบบ GSM (Global System for Mobile Comunication) TDMA (Time Division Multiple Access) และ CDMA (Code Division Multiple Access) เมื่อ SMS ถูกส่งจากโทรศัพท์มือถือเครื่องหนึ่ง ข้อความนั้นจะถูกส่งไปที่ Short Message Service Center (SMSC) จากนั้นจึงจะส่งไปยังโทรศัพท์มือถือเครื่องรับอีกทอดหนึ่ง โดยมีกระบวนการดังนี้

1. SMSC จะส่ง SMS Request ไปยัง Home Location Register (HLR) เพื่อหาตำแหน่งของผู้รับ

2. เมื่อ HLR ได้รับสัญญาณ Request ก็จะส่งสถานะของผู้รับ (Subscriber's status) กลับมายัง SMSC คือ สถานะของเครื่องรับ Inactive หรือ Active ตำแหน่งของเครื่องรับ ถ้าสถานะของเครื่องรับเป็น Inactive แล้ว SMSC จะเก็บข้อความไว้ช่วงเวลาหนึ่ง และเมื่อใดที่เครื่องรับมีสถานะ Active แล้ว HLR จะส่ง SMS Notification ไปยัง SMSC และ SMSC ก็จะตอบรับข้อความ

นั้นไว้ จากนั้น SMSC จะส่งผ่านข้อความในรูปแบบ Short Message Delivery Point-to-Point ไปยังระบบบริการ โดยระบบจะทำการเรียกไปยังเครื่องรับและถ้าเครื่องรับมีการตอบรับกลับมาข้อความก็จะถูกส่งตามไปและ SMSC จะได้รับการตอบยืนยันว่า ข้อความได้ถูกรับโดยปลายทางเรียบร้อยแล้ว หลังจากนั้นข้อความจะมีสถานะเป็น SENT และจะไม่ถูกส่งอีก

กรณีที่โทรศัพท์เคลื่อนที่ของผู้รับปิดอยู่นอกพื้นที่ให้บริการ ข้อความสั้นจะถูกเก็บไว้ใน SMS-C ประมาณ 1 วัน (ระยะเวลาที่เก็บขึ้นอยู่กับผู้ให้บริการแต่ละราย) หากผู้ใช้บริการไม่เปิดเครื่องหรือกลับเข้าสู่พื้นที่ให้บริการข้อความสั้นที่เก็บไว้ก็จะถูกลบออกจากศูนย์ข้อความสั้น เพื่อป้องกันไม่ให้ข้อความที่เก็บในศูนย์ข้อความสั้นล้นจนทำให้ระบบหยุดการทำงานได้



รูปที่ 2.21 หลักการทำงานของ SMS [8]

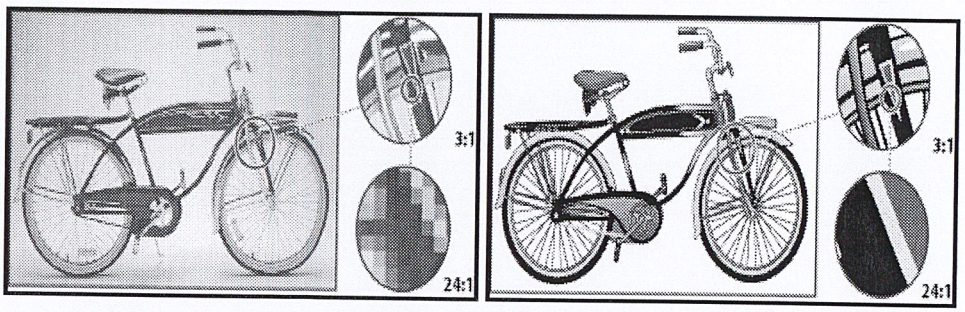
2.6 ระบบการประมวลผลภาพ (Image Processing)

2.6.1 รูปภาพดิจิตอล (Digital Image)

โดยปกติแล้ว ข้อมูลภาพทั่วๆไป นั้นได้มาจาก การที่แสงตกกระทบกับวัตถุแล้วเกิดการสะท้อนผ่านเลนส์เข้าสู่ตัวบันทึกภาพ อาจจะอยู่ในรูปตรวจจับ (Sensor) หรือฟิล์ม (Film) หากเราย้อนนึกถึงเมื่อเวลาเราถ่ายภาพด้วยกล้องดิจิตอล วัตถุหรือภาพที่เรามองเห็นด้วยตานั้นเป็นข้อมูล

สามมิติ (Three-dimension) ที่ประกอบด้วยความลึก ความสูง และความกว้าง แต่เมื่อเราแปลกข้อมูลภาพออกมาเป็นข้อมูลภาพดิจิตอล (Digital Image) ข้อมูลของภาพนั้นจะประกอบไปด้วยความกว้างและความสูงของภาพ (Width and Height) เท่านั้น

โดยทั่วไปแล้วเราสามารถที่จะแบ่งรูปภาพที่ปรากฏและใช้งานบนเครื่องคอมพิวเตอร์ออกเป็น 2 ประเภทคือรูปภาพแบบบิตแมป (Bitmap Image) และรูปภาพแบบเวกเตอร์(Vector Image) ดังรูปที่ 2.22



(ก) ภาพแบบบิตแมป (ข) ภาพแบบเวกเตอร์

รูปที่ 2.22 รูปภาพดิจิตอล [9]

2.6.1.1 ภาพแบบบิตแมป (Bitmap Image)

ภาพแบบ Bitmap หรืออาจจะเรียกว่าภาพแบบราสเตอร์ (Raster) เป็นภาพที่เกิดจากจุดสีที่เรียกว่า pixels ซึ่งประกอบกันเป็นรูปร่างบนพื้นที่ที่มีลักษณะเป็นเส้นตาราง (กริด) แต่ละพิกเซลจะมีค่าของตำแหน่ง และค่าสีของตัวเอง ภาพหนึ่งภาพ จะประกอบด้วยพิกเซลหลายๆ พิกเซลผสมกัน แต่เนื่องจากพิกเซลมีขนาดเล็กมาก จึงเห็นภาพมีความละเอียดสวยงาม ไม่เห็นลักษณะของกรอบสี่เหลี่ยม จึงเป็นภาพที่เหมาะสมต่อการแสดงภาพที่มีเฉด และสีสันจำนวนมาก เช่น ภาพถ่าย หรือภาพวาด ภาพแบบ Bitmap เป็นภาพที่ขึ้นอยู่กับความละเอียด หรือความคมชัด (Resolution) ซึ่งก็คือ จำนวนพิกเซลที่แน่นอนในการแสดงภาพ ดังนั้นเมื่อมีการขยายภาพ จะเกิดปัญหาคือ เห็นเป็นกรอบสี่เหลี่ยมเล็กๆ หลายๆจุดประกอบกันเพราะกริดของภาพมีขนาดที่แน่นอน

2.6.1.2 ภาพแบบเวกเตอร์ (Vector)

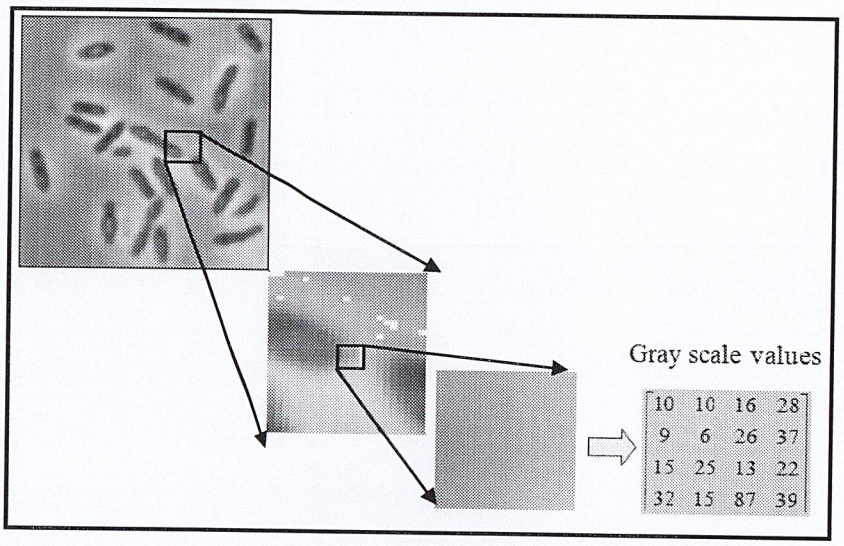
เป็นภาพที่สร้างด้วยส่วนประกอบของเส้นลักษณะต่างๆ และคุณสมบัติเกี่ยวกับสีของเส้นนั้นๆ ซึ่งสร้างจากการคำนวณทางคณิตศาสตร์ เช่น ภาพของคน ก็จะถูกสร้างด้วยจุดของเส้นหลายๆ จุด เป็นลักษณะของโครงร่าง (Outline) และสีของคนก็เกิดจากสีของเส้นโครงร่างนั้นๆ กับพื้นที่ผิวภายในนั่นเอง เมื่อมีการแก้ไขภาพ ก็จะเป็นการแก้ไขคุณสมบัติของเส้น ทำให้ภาพไม่สูญเสียความละเอียด เมื่อมีการขยายภาพ

2.6.2 ประเภทของภาพ (Images)

โดยทั่วไปแล้ว เราสามารถแบ่งประเภทของภาพบิตแมปตามคุณสมบัติการแสดงผลของสีภาพเป็น 4 ประเภทดังนี้คือ

2.6.2.1 ภาพระดับความเข้มเทา (Intensity Image or Gray Scale Image)

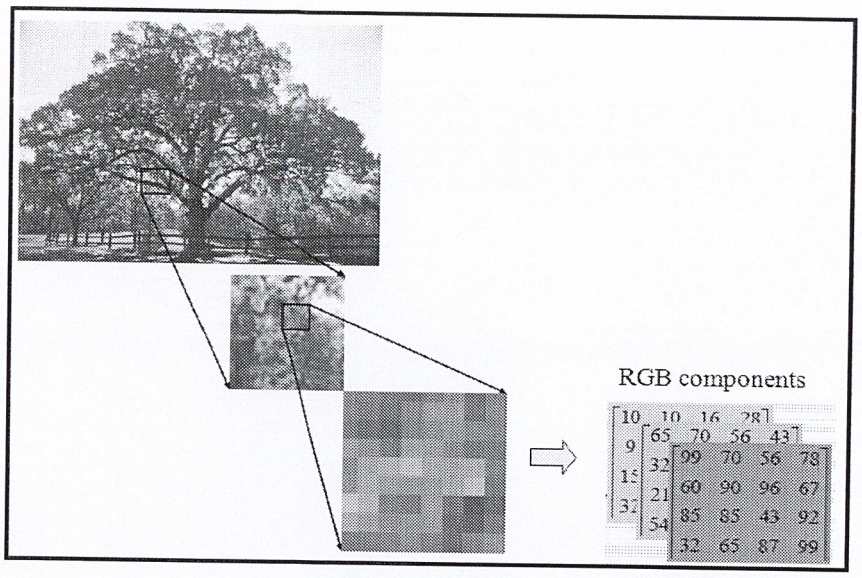
Gray Scale เป็นอัตราส่วนของโทนสีเทา ซึ่งมีการไล่ระดับความอ่อนแก่ ที่อยู่ระหว่างสีขาวกับสีดำ Halftone Image การสร้างภาพให้มีระดับสีต่างๆ อย่างต่อเนื่อง ด้วยการใช้จุดสีที่มีขนาดต่างกัน หรือมีความหนาแน่นของจุดต่างกัน ค่าในแต่ละพิกเซลของ Gray Image คือค่าความเข้มของแสง ณ แต่ละตำแหน่งของพิกเซล ซึ่งจะอยู่ในรูปของ Gray Scale (Gray Level) ค่าที่เป็นไปได้ของ Gray Scale จะขึ้นอยู่กับจำนวนบิตที่ใช้ ดังรูปที่ 2.23



รูปที่ 2.23 แสดงค่าสีใน Gray Scale [10]

2.6.2.2 ภาพสี (Color Image)

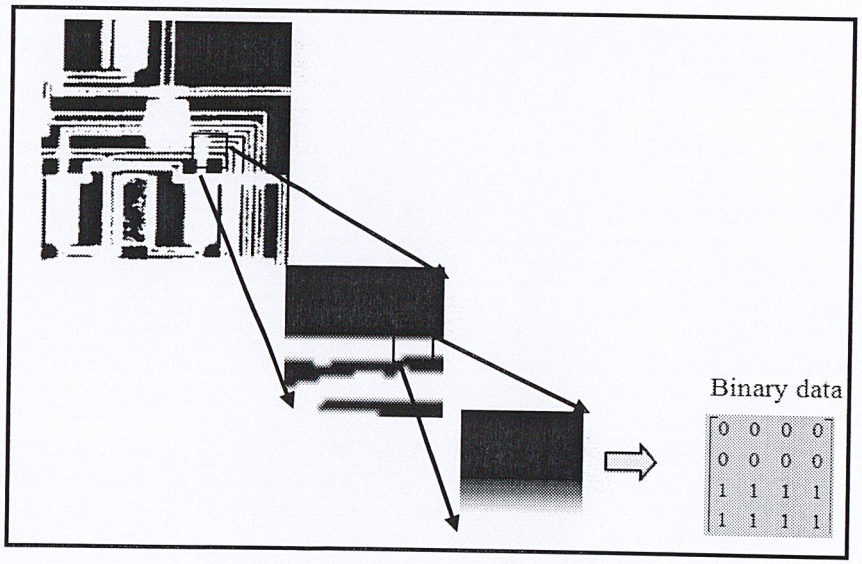
ภาพชนิดนี้ แต่ละจุดภาพหรือพิกเซลของภาพจะเก็บค่าระดับความเข้มเทาของแต่ละแถบแสงของแม่สีหลัก 3 สีที่ซ้อนกันอยู่คือ สีแดง (Red) สีเขียว (Green) สีน้ำเงิน (Blue) ซึ่งในแต่ละพิกเซลนั้นๆ ก็จะแสดงผลของค่าสีของแต่ละพิกเซลตามระดับความเข้มในแต่ละแถบแสงสีนั้น แสดงตัวอย่างดังรูปที่ 2.24



รูปที่ 2.24 แสดงภาพสี [10]

2.6.2.3 ภาพไบนารี (Binary Image)

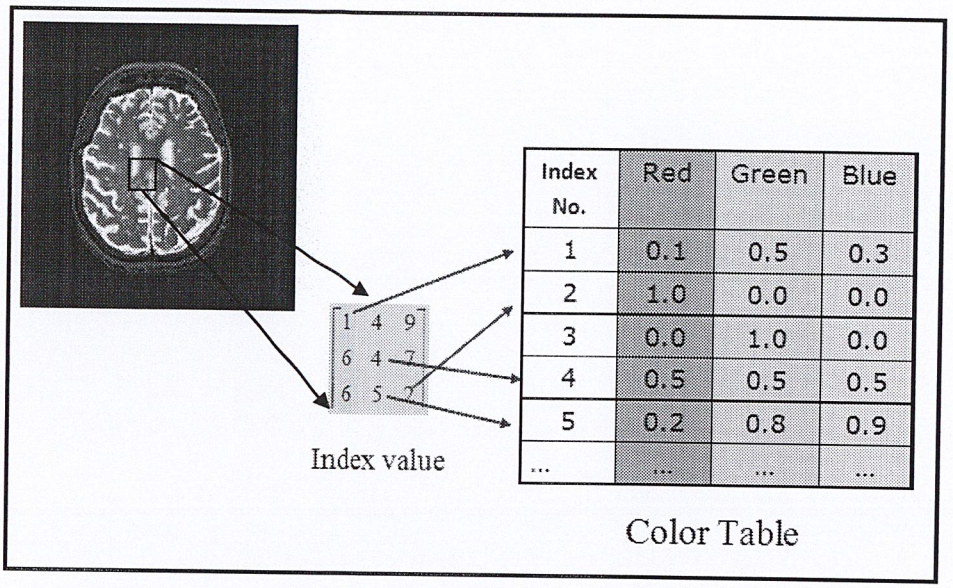
ภาพไบนารีจะแสดงลักษณะของข้อมูลภาพในรูปแบบขาวดำ กล่าวคือในแต่ละพิกเซลของภาพจะถูกแสดง ด้วยค่าแบบไบนารี (Binary) คือ มี 1 บิต ซึ่งประกอบไปด้วยค่า 1 กับ 0 โดยที่ 1 หมายถึง จุดภาพสีขาว และ 0 หมายถึง จุดภาพสีดำ ภาพประเภทนี้เหมาะสำหรับภาพที่เกี่ยวกับตัวอักษร (Text) ภาพลายนิ้วมือ (Finger Print) เป็นต้น ดังรูปที่ 2.25



รูปที่ 2.25 ตัวอย่างแสดงภาพแบบขาวดำ [10]

2.6.2.4 ภาพแบบดัชนี (Index Image)

ภาพประเภทนี้ ในแต่ละพิกเซลของภาพจะเก็บค่าดัชนี (Index Number) ซึ่งเป็นตัวเลขจำนวนเต็มซึ่งจะถูกนำค่าดัชนีดังกล่าวไปเปรียบเทียบกับตารางสี (Color Table) ซึ่งเป็นตารางแสดงค่าสี สีแดง สีเขียว และสีน้ำเงินซึ่งค่าดัชนีนี้จะเป็นตัวบ่งชี้ให้เห็นว่าภาพในตำแหน่งพิกเซลใดๆ มีอัตราส่วนของแม่แสง 3 สีในอัตราส่วนละเท่าไหร่ แสดงตัวอย่างดังรูปที่ 2.26



รูปที่ 2.26 แสดงภาพแบบดัชนี [10]

2.6.2.5 ขนาดของไฟล์ภาพ (Image File Sizes)

ขนาดของไฟล์ภาพขึ้นอยู่กับปัจจัยหลักๆ 2 ส่วนคือ ขนาดจองภาพ (Size) และจำนวนบิตที่ใช้ในการแสดงค่าสีหรือระดับความเข้มของแสงในแต่ละพิกเซลของภาพ เมื่อกำหนดให้ M x N คือขนาดของสัญญาณภาพและ L คือ จำนวนบิตที่ใช้ควอนไทซ์ในแต่ละจุดภาพ ดังนั้นขนาดของไฟล์ภาพ (S) หรือจำนวนบิตทั้งหมดที่ต้องใช้สำหรับหน่วยความจำในการเก็บข้อมูลภาพมีค่าดังสมการ (3)

$$S = M \times N \times L \qquad (3)$$

เมื่อเราพิจารณาภาขาว-ดำ (Binary Image) ขนาด 512 x 512 พิกเซลขนาดของไฟล์ภาพจะสามารถ

$$512 \times 512 \times 1 = 262{,}144 \text{ บิต}$$

$$= 32{,}768 \text{ ไบต์}$$

$$= 0.033 \text{ เมกะไบต์}$$

ในกรณีที่ภาพนั้นเป็นภาพแบบ Gray Scale ซึ่งมีระดับค่าความเข้มเทาอยู่ระหว่าง 0-255 (8 บิต) และมีขนาด 512 x 512 พิกเซลขนาดไฟล์ภาพจะสามารถคำนวณได้จาก

$$512 \times 512 \times 8 = 2{,}097{,}152 \text{ บิต}$$
$$= 262{,}144 \text{ ไบต์}$$
$$= 0.25 \text{ เมกะไบต์}$$

หากเมื่อภาพที่พิจารณาเป็นภาพสี ขนาด 512x512 พิกเซล ความละเอียด 8 บิต ขนาดของไฟล์ภาพจะสามรถทำควณขนาดได้จาก

$$512 \times 512 \times 8 \times 3 = 6{,}291{,}456 \text{ บิต}$$
$$= 786{,}432 \text{ ไบต์}$$
$$= 0.786 \text{ เมกะไบต์}$$

2.6.3 ระบบการมองเห็นภาพ (Vision System)

กลไกระบบการมองเห็นภาพ (Vision System) นั้น จะมีความหมายที่รวมไปถึงทุกสิ่งที่จำเป็นที่สามารถแปลงภาพนั้นๆเป็นรหัสดิจิตอลเพื่อที่จะเอามาใช้กับระบบคอมพิวเตอร์ได้ การปรับปรุงเปลี่ยนแปลงข้อมูลและการนำเสนอภาพที่ได้มาหลังจากการปรับปรุงเปลี่ยนแปลงข้อมูลและการนำเสนอภาพที่ได้มาหลังจากปรับปรุงเปลี่ยนแปลงข้อมูลแล้ว ความยุ่งยากของระบบการมองเห็นภาพนี้จะขึ้นอยู่กับการใช้งาน ซึ่งสามารถแบ่งเป็น 3 ขั้นตอนที่สำคัญได้ดังนี้

1. การได้มาซึ่งภาพ (Image Acquisition)
2. กระบวนการประมวลผลภาพ (Image Processing)
3. ผลที่ได้รับหรือการแสดงผล (Output or Display)

ในปัจจุบันได้มีการประยุกต์ใช้งานระบบการมองเห็นอยู่มากมาย เช่น การใช้บาร์โค๊ด การพิมพ์ สิ่งพิมพ์ต่างๆและการประยุกต์ใช้งานในโรงงาน เป็นต้น

2.6.4 การได้มาซึ่งภาพ (Image Acquisition)

การได้มาซึ่งภาพ หมายถึงการแปลงภาพในลักษณะทางกายภาพให้เป็นเขตของข้อมูลทางดิจิตอลซึ่งเขตของข้อมูลนี้จะถูกส่งไปยังหน่วยประมวลผลต่อไป ฟังก์ชั่นของการได้มาซึ่งภาพนี้จะแบ่งออกเป็น 4 เฟส ได้แก่

1. การส่องสว่าง (Illumination)
2. รูปแบบของภาพ หรือ การทำให้ภาพชัดขึ้น (Image Formation for Focusing)
3. การตรวจจับภาพ หรือ การรับภาพ (Image Detection or Sensing)
4. รูปแบบของผลสัญญาณที่ได้จากกล้อง (Formatting Camera Output Signal)

การส่องสว่างเป็นตัวแปรสำคัญที่มีอิทธิพลต่อสัญญาณอินพุท (Input Signal) ที่จะส่งต่อให้กับระบบการมองเห็นภาพ ดังนั้นเราจึงต้องออกแบบให้มีการส่องสว่างที่เหมาะสมกับการใช้

งานที่แตกต่างกัน โดยที่ชนิดและวิธีการส่องสว่างของแหล่งกำเนิดแสงจะมีผลต่อกำลังงานของแสงที่ส่งออกมา ซึ่งจะมีผลต่อกระบวนการประมวลภาพ และผลของสัญญาณที่ได้รับ

2.6.5 กระบวนการประมวลผลภาพ (Image Processing)

การประมวลผลภาพ คือ การสร้างภาพใหม่โดยการแยกส่วนของข้อมูลที่เราสนใจกับสิ่งรบกวน (Noise) ออกจากกัน โดยการทำงานพื้นฐานของการประมวลผล คือ การกำจัดสิ่งรบกวนของภาพ (Noise Elimination) การปรับแต่งขอบภาพให้ดีขึ้น (Edge Enhancement) การกรองภาพ (Filtering) การปรับปรุงเปลี่ยนแปลงค่าระดับเกรย์ (Gray Scale Modification) โดยทั่วไปแล้วจะใช้ฮาร์ดแวร์และซอฟต์แวร์ ซึ่งความซับซ้อนของการประมวลผลจะขึ้นอยู่กับลักษณะของการใช้งาน และจะมีวิธีการประมวล 3 อย่าง คือ

1. ที่จุดเดียวกันในรูปภาพเดียวกัน (Point by Point in one image) คือ การสร้างภาพใหม่โดยการเปลี่ยนค่าแบบจุดต่อจุด โดยจุดหนึ่ง คือ จุดในรูปภาพเดิม และอีกจุดหนึ่ง คือ จุดในรูปภาพใหม่ที่ได้รับ การปรับปรุวเปลี่ยนแปลงจการูปเดิมแล้ว เช่น การแปลงภาพในระบบเลขฐานสองจากจุดที่มีค่าเป็น 0 ถูกเปลี่ยนเป็น 1 และจากค่า 1 ถูกเปลี่ยนกลับเป็น 0

2. ที่จุดเดียวกันในรูปภาพที่แตกต่างกัน (Using Conrresponding Point In One Image) คือ การสร้างภาพใหม่โดยการหาค่าเฉลี่ยรอบๆจุดนั้นในภาพนั้น ค่าของจุดในภาพใหม่ คือ ค่าเฉลี่ยของจุดในภาพนั้นเป็นอันเดิม

3. ที่บริเวณจุดนั้นในภาพนั้น (Using Regional Point In One Image) คือ การสร้างภาพใหม่โดยการหาค่าเฉลี่ยรอบๆ จุดนั้นในภาพนั้น ค่าของจุดในภาพใหม่ คือ ค่าเฉลี่ยของจุดในภาพนั้นเป็นอันเดิม

2.6.6 เทคโนโลยีไบโอเมทริกซ์

2.6.6.1 ความหมายของไบโอเมทริกซ์

ไบโอเมทริกซ์ (Biometrics) เกิดจากการประสมกันของคำสองคำคือ bio หมายถึง “ชีวิต” และ metrics ซึ่งหมายถึง “ที่สามารถวัดค่าหรือปริมาณได้” ได้มีการบันทึกไว้ว่าชาวอียิปต์โบราณมีการใช้ไบโอเมทริกซ์เป็นกลุ่มแรกเพื่อใช้ตรวจสอบ การใช้อุปกรณ์ไบโอเมทริกซ์สมัยใหม่เมื่อประมาณ 20 ปีมาแล้วเป็นเครื่องมือวัดความยาวของนิ้วมือ เพื่อตรวจสอบเวลาการทำงานแทนเครื่องตอกบัตร หลังจากนั้นจึง มีการพัฒนาอุปกรณ์สำหรับแยกแยะลักษณะมือเป็นจำนวนมากมาช่วยทำงานในระบบรักษาความปลอดภัย

2.6.6.2 ลักษณะการทำงาน

การทำงานจะเป็นการตรวจวัดคุณลักษณะทางกายภาพ (Physical Characteristics) และลักษณะทางพฤติกรรม (Behaviore) ที่เป็นลักษณะเฉพาะตัวของบุคคลนั้นๆ มาเปรียบเทียบกับ

คุณลักษณะที่มีการบันทึกไว้ในฐานข้อมูลก่อนหน้านี้ เพื่อแยกแยะบุคคลนั้นจากบุคคลอื่นๆ ในงานด้านต่างๆ นอกจากนี้ยังสามารถใช้เพื่อตรวจสอบกลุ่มผู้ต้องสงสัย เพื่อหาตัวผู้กระทำผิดได้อีกด้วย

ไบโอเมทริกซ์สามารถนำมาประยุกต์ใช้งานได้หลากหลายประเภท เช่น

-งานควบคุมการเข้าออกสถานที่/หรือการใช้ตรวจสอบเวลาทำงาน

การเข้าออกสถานที่หวงห้ามในปัจจุบัน มักจะใช้บัตรผ่าน หรือแม้แต่การใช้ยามเฝ้า ซึ่งการป้องกันแบบนี้สามารถถูกลักลอบได้ง่าย เช่น บัตรผ่าน หรือรหัสผ่านอาจหาย หรือแม้แต่ให้คนอื่นยืมใช้ได้ ส่วนยามเฝ้าก็ขึ้นอยู่กับความเข้มงวดของยามแต่ละคน ความบกพร่องของระบบที่ใช้กันอยู่ในปัจจุบันจึงมีอยู่มาก การนำเอาไบโอเมทริกซ์มาช่วยเช่น การผ่านเข้าออกโดยใช้ลายนิ้วมือ ใช้การตรวจสอบรูปหน้า หรือแม้แต่การใช้การตรวจสอบลักษณะของเรตินาภายในดวงตา จึงเป็นทางออกที่ดีกว่าการใช้งานที่เป็นอยู่ในปัจจุบัน

ระบบที่มีการใช้งานคล้ายกับการควบคุมการเข้าออกสถานที่ก็คือ การตรวจสอบเวลาการทำงานของพนักงาน ซึ่งระบบที่ใช้กันอยู่ในปัจจุบันคือ การเซ็นชื่อ การใช้บัตรตอกตลอดเวลา ลารใช้บัตรแถบแม่เหล็ก

- ระบบใช้งานเครื่องคอมพิวเตอร์และภายในระบบเครือข่าย

เครื่องคอมพิวเตอร์แบบ Notebook หลายๆรุ่น มีการนำเทคโนโลยี Biometrics เช่น การใช้ลายนิ้วมือมาช่วยในการใช้งานเครื่องคอมพิวเตอร์ ซึ่งมีประโยชน์มากสำหรับบุคคลที่ต้องการความปลอดภัยในการรักษาข้อมูล เพราะถึงแม้ว่าเครื่องคอมพิวเตอร์จะถูกโขมย แต่ผู้ที่ขโมยไปก็ไม่สามารถนำไปใช้งานได้ โดยการใช้ลายนิ้วมือมาช่วยมีอยู่หลักๆ สองประเภท คือ เครื่องคอมพิวเตอร์ Notebook ที่มีตัวตรวจลายนิ้วมืออยู่ในตัวเครื่องอยู่แล้ว และประเภทที่ใช้ PC Card ที่มีตัวตรวจจับลายนิ้วมืออยู่ ใส่เข้าไปในช่อง PC Card ของเครื่องคอมพิวเตอร์ Notebook โดยที่ลายนิ้วมือจะเป็นการใช้ทดแทนการใช้รหัสผ่าน (Password)

นอกจากนี้การใช้งานคอมพิวเตอร์ระบบเครือข่าย จะต้องให้ผู้ใช้ใส่รหัสผ่านก่อนการใช้งานทุกครั้ง แต่เนื่องจากรหัสผ่านสามารถถูกคาดเดา หรือขโมย หรือถูกยืมไปใช้ได้ง่าย ดังนั้นการใช้ Biometrics มาเป็นตัวจัดการเริ่มเข้ามาใช้งานของผู้ใช้ระบบเครือข่าย จึงเป็นสิ่งที่สามารถยืนยันได้อย่างแท้จริงว่า ผู้ที่ใช้งานเครือข่ายอยู่คือผู้ที่มีสิทธิในการใช้งานได้จริง เทคโนโลยีที่ใช้ได้กับด้านนี้นอกจากการใช้ลายนิ้วมือแล้ว วิธีที่เหมาะสมต่อการใช้งานมากอย่างหนึ่งคือ การใช้ Keystoke Dynamics หรือการตรวจสอบบุคคลโดยลักษณะของการพิมพ์ ทั้งนี้เพราะการเข้าไปใช้งานระบบเครือข่าย ผู้ใช้ต้องทำการพิมพ์ชื่อและรหัสอยู่แล้ว การตรวจสอบบุคคลโดยใช้ลักษณะของการพิมพ์จึงเป็นสิ่งที่ไม่ต้องให้ผู้ใช้ทำอะไรเพิ่มเติม อีกทั้งวิธีการตรวจสอบแบบนี้ยังไม่ต้องการอุปกรณ์เพิ่มเติมใดๆ

2.6.6.3 ไบโอเมทริกซ์ประเภทต่างๆ

- **การรู้จำใบหน้า (Facial Recognition)**

ไบโอเมทริกซ์โดยใช้ใบหน้า ได้รับการพิจารณาและยอมรับกันอย่างกว้างขว้าง ว่าเป็นวิธีที่เป็นกลางในการพิสูจน์ตัวบุคคล

เทคโนโลยีนี้มีความสามารถที่น่าสนใจอยู่ 2 อย่าง คือ การรู้จำใบหน้า (Facial Recognition) และการสร้างหน้าใหม่ (Face Reconstruction)

- สามารถใช้กับลักษณะที่ซับซ้อนได้
- ใช้ได้กับรูปร่างลักษณะหลายชนิด
- สามารถทำงานได้อย่างรวดเร็ว แม่นยำและใช้ข้อมูลสำหรับเปรียบเทียบขนาดเล็ก ข้อมูลที่ใช้สามารถทำให้อยู่ในรูปข้อมูลทางสถิติได้

- **การรู้จำม่านตา (Iris Recognition)**

การรู้จำม่านตา ทำงานได้โดยที่ไม่ต้องมีการสัมผัสเครื่องมือ และง่ายต่อการใช้งาน ในขณะที่สามารถทำงานได้อย่างมีประสิทธิภาพในการรักษาความปลอดภัยสูง กลายเป็นเทคโนโลยีที่ได้รับการยอมรับอย่างมาก

- มีการทำงานที่มีประสิทธิภาพและความแม่นยำสูง
- รวดเร็ว มีระบบการตรวจสอบที่ง่าย และไม่ต้องมีการสัมผัสกับอุปกรณ์
- ม่านตาของมนุษย์ไม่มีการเปลี่ยนแปลงไปตามอายุขัย
- ความเหมือนกันของข้อมูลมีน้อย ทำให้มีความสับสนกันน้อย

- **การรู้จำลายนิ้วมือ (Fingerprint Recognition)**

การรู้จำลายนิ้วมือมีการทดลอง ทดสอบ และการทำงานด้านความปลอดภัยในการพิสูจน์บุคคลมีการใช้งานต่างๆกันในหลายจำพวก การรู้จำลายนิ้วมือมีข้อได้เปรียบดังต่อไปนี้

- ทนทาน และสามาถเชื่อถือได้
- ใช้งานง่าย
- ใช้กันอย่างกว้างขวาง และยอมรับกันโดยทั่วไป
- ได้รับการพิสูจน์แล้ว ว่าใช้งานได้จริง
- ความหลากหลายของการประยุกต์ใช้

- **การรู้จำเสียง (Voice Recognition)**

เทคโนโลยี ทำงานได้อย่างมีประสิทธิภาพและความแม่นยำสูง เพื่อการยืนยันตัวบุคคลด้วยเสียงของตัวเอง เสียงพูดเป็นสิ่งที่มีติดตัวกันทุกคน และสะดวกในการใช้งานในสถานที่ต่างๆ โดยเฉพาะการใช้งานแบบไร้สัมผัส

- เป็นการทำงานที่มีประสิทธิภาพ และความถูกต้องมาก

- ยืนยันตัวตน เอกลักษณ์ของบุคคลได้จากเสียงของเขาทั้งหลายเอง
- กระบวนการง่ายๆ สามารถฝังตัวรวมกับระบบต่างๆได้หลากหลาย
- เทคโนโลยีนี้ นำไปใช้กับระบบที่ต้องใช้บัตร หรือไม่ต้องใช้บัตรก็ได้
- มีความยืดหยุ่นสำหรับการนำไปใช้ในระบบจริง

2.6.7 คำจำกัดความและขอบเขตของการรู้จำรูปแบบ

เนื่องจากมีปัจจัยหลายอย่างที่จำกัดการออกแบบ Pattern Recognition จึงทำให้การวิจัยในเรื่องนี้เป็นไปได้ยาก แต่ถ้าเราไม่เข้าใจพฤติกรรมของมนุษย์เราก็ไม่สามารถที่จะทำสำเร็จได้

การรู้จำรูปแบบ (Pattern Recognition) ต้องอาศัยการรับรู้และการจำก่อน รวมทั้งประสบการณ์ในอดีตกับปัจจุบันสัมพันธ์กัน ตัวอย่างเช่น มีรูปสุนัขที่ไม่ชัดเจนและบิดเบือนอยู่รูปหนึ่ง ถ้ามีคนไม่เคยได้รับรู้หรือมีประสบการณ์มาก่อนก็จะสามารถตอบคำถามของรูปนี้ได้ถูกต้อง

ถึงแม้ว่าในปัจจุบันเทคโนโลยีทางคอมพิวเตอร์ และความก้าวหน้าใน Pattern Recognition และ Artificial Intelligence สูง การแยกภาพของมนุษย์ที่สมบูรณ์ยังคงเป็นหนทางที่ยาวไกล อย่างไรก็ตามก็ไม่สามารถขัดขวางความพยายามของนักวิจัยได้

มีเทคนิคพื้นฐานจำนวนมากที่ใช้กับ Pattern Recognition เกือบทั้งหมดไม่ว่าจะเป็นภาพวัตถุ หรือ 1-D Time-Vary Signal เช่น คำพูด เทคนิคพื้นฐานได้แสดงไว้ดังนี้

วิธีการในการรู้จำภาพใบหน้าตั้งแต่อดีตจนถึงปัจจุบัน ได้มีแนวคิดในด้านการพิจารณามองเห็นใบหน้า และวิธีการในการตัดสินใจรู้จำใบหน้าที่แตกต่างกัน ซึ่งสามารถแบ่งได้เป็น 6 กลุ่มการวิจัย คือ

- การเทียบเทมเพลต (Template Matching)
- ลักษณะทางเรขาคณิต (Geometrical Feature)
- การเทียบกราฟ (Graph Matching)
- ไอเกนเฟช (Eigenface)
- โครงข่ายประสาทเทียม (Neural Network)
- ภาพ 3 มิติ

- **การเทียบเทมเพรต (Template Matching)**

วิธีการเทียบเทมเพรตนี้ ทำงานโดยการหาสหสัมพันธ์ของภาพ 2 ภาพ โดยตรงให้ผลอย่างมีประสิทธิภาพโดยมีอัตราในการรับรู้จำเป็น 100% เมื่อภาพมีขนาดเดียวกัน มีการวางอยู่ตรงกันและมีการส่องสว่างของแสงเดียวกัน ถ้าภาพที่เข้ามาทดสอบมีการเปลี่ยนแปลงไปจากเดิม ต้องมีการประมวลผลก่อน (Preprocessing) เพื่อทำให้ภาพเข้าสู่ตำแหน่งหรือการส่องสว่างใกล้เคียงกัน

- **ลักษณะทางเรขาคณิต (Geometrical Features)**

มีนักวิจัยจำนวนมากที่เลือกรู้จำใบหน้าในลักษณะทางเรขาคณิต คืออาศัยอัตราส่วนหรืออัตราส่วนของระยะทางจากตาซ้ายตาขวา จากตาไปจมูก จากจมูกไปปาก รูปร่างของปาก รูปร่างของตา และจากรูปร่างของคาง ซึ่งเป็นลักษณะทางกายภาพของใบหน้า ดังมีรายละเอียดของการวิจัย เช่น

- ใช้อัตราของระยะทาง (Ratios of Distance) โดยมีผลการรู้จำอยู่ระหว่าง 45-75% ของฐานข้อมูลภาพ 20 คน
- ใช้การคำนวณเซตของลักษณะทางเรขาคณิต เช่น ความกว้างของจมูก ตำแหน่งของปากบนใบหน้า และรูปร่างของคาง
- ใช้เทคนิคระยะทางผสม (Mixture Distance)

ระบบการรู้จำใบหน้าแบบที่มีการพิจารณาลักษณะทางเรขาคณิตนี้จะสามารถนำไปใช้เป็นระบบที่มีประโยชน์และเป็นไปได้ในทางปฏิบัติในการค้นหาในฐานข้อมูลขนาดใหญ่ได้ถ้ามีการวัดระยะทางจากจุดที่เป็นลักษณะเด่นได้อย่างถูกต้องเที่ยงตรง ทั้งนี้เพราะข้อมูลที่ได้จะมีจำนวนน้อยมากเมื่อเทียบกับการพิจารณาแบบอื่น จึงใช้เวลาน้อยกว่าแบบอื่นๆ ในการค้นหา ดังนั้นจึงมีการสร้างระบบฐานข้อมูลมาสนับสนุนวิธีการแบบนี้ ซึ่งฐานข้อมูลดังกล่าวเรียกว่าฐานข้อมูลภาพหลายด้าน (Mugshot Database) ทั้งนี้เพราะถ้าเรามีภาพด้านข้างด้วยจะเป็นการช่วยหาจุดที่เป็นลักษณะเด่นได้เที่ยงตรงแม่นยำมากขึ้น แต่ทั้งนี้ความเที่ยงตรงในการวัดยังขึ้นอยู่กับอัลกอริทึมที่ใช้ด้วยดังนั้นในปัจจุบันการทำงานอย่างอัตโนมัติก็ยังไม่ค่อยมีความเที่ยงตรงนัก จึงต้องรอกันต่อไป สำหรับวิธีการแบบนี้

- **การเทียบกราฟ (Graph Matching)**

เป็นการมองใบหน้าในลักษณะที่เป็นเวกเตอร์ของกราฟซึ่งมีจุดและเส้นในการเชื่อมต่อเป็นโครงร่างที่ฟิตไปบนใบหน้าบนลักษณะเด่นที่พิจารณา เช่น รูปร่างของกราฟของตา ปาก คาง กับหู และคิ้ว เป็นต้น

- **ไอเกนเฟซ (Eigenface)**

MIT ได้ริเริ่มและเสนอวิธีการในการรู้จำใบหน้าโดยการทำการฉาย (Projection) ภาพใบหน้าไปยังองค์ประกอบหลัก (Principal Components) โดยเรียกภาพใบหน้าดังกล่าวนั้นว่าไอเกนเฟซ (Eigenface) โดยนำใบหน้าไอเกนดังกล่าวไปทำการค้นหาในฐานข้อมูลใบหน้าไอเกน โดยพวกเขาได้แสดงให้เห็นว่าโดยการทดสอบกับฐานข้อมูลใบหน้าไอเกน 16 คนที่มีการเลื่อนการวางตำแหน่งศรีษะหลายๆลักษณะ มีการย่อขยายและการเปลี่ยนแปลงของแสง โดยการแทนใบหน้าไอเกนที่ใช้เทคนิคของพวกเขาแล้วจะมีการเปลี่ยนแปลงเล็กน้อย โดยระบบยังคงมีความสามารถในการรู้จำ เมื่อมีการเปลี่ยนแปลงของแสงมีความสามารถในการรู้จำ 96% มีการวางตำแหน่งศรีษะเปลี่ยนแปลงจะมีความสามารถในการรู้จำ 85% และมีการย่อขยายภาพมี

ความสามารถในการรู้จำ 64% โดยในการย่อขยายนั้นพวกเขาใช้อัลกอริทึมในการปรับศรีษะให้มีขนาดเดียวกับขนาดใบหน้าไอเกนโดยใช้การประมาณขนาดศรีษะ และนำส่วนกลางของใบหน้ามาใช้เท่านั้นเพื่อลดผลจากการเปลี่ยนแปลงของทรงผม และฉากด้านหลังที่เกิดการเปลี่ยนแปลงได้

- **โครงข่ายประสานเทียม (Neural Network)**

จากอดีตจนถึงปัจจุบันได้มีการเสนอบทความที่ใช้โครงข่ายประสาทเทียมในการรู้จำใบหน้ามากมาย แต่ส่วนใหญ่แล้วน่าเสียดายที่วิธีการต่างๆที่เสนอนั้น มีการทดสอบกับฐานข้อมูลขนาดเล็กได้เท่านั้น (ต่ำว่า 20 ตน) จะมีที่ใช้ฐานข้อมูลขนาดใหญ่ไม่มากนัก

- **ภาพ 3 มิติ**

การมองภาพใบหน้า 3 มิติ เป็นวิธีการชั้นสูงและเป็นวิธีการที่ดีมากในปัจจุบัน และมีการทำเป็นธุรกิจผลิตซอฟต์แวร์เพื่อเป็นการค้าเรียบร้อยแล้ว

Facelt คือ ชื่อซอฟต์แวร์ทางการค้าของบริษัท Visionics Corporation ในการรู้จำใบหน้ารูปแบบ 3 มิติแบบเวลาจริงที่ไม่ต้องการฮาร์ดแวร์พิเศษในโลกแหน่งความเป็นจริง

Facelt ใช้การมองภาพในรูปแบบสเตอริโอของภาพ 3 มิติ ที่ประกอบด้วยบล็อคความสูง โดยเรียกว่า หัวไอเกน (Eigen Head) ที่เป็นตัวแสดงภาพ 3 มิติของศรีษะที่ได้มาจากข้อมูลเฉดสี (Shading Information) ของภาพ 2 มิติ ซึ่งหัวไอเกนนี้จะไม่ขึ้นกับแสงของการส่องสว่างและท่าทางการวางศรีษะ และมีการส่งภาพ 3 มิติที่มีการนอร์มอไลด์แล้วแปลงไปเป็นรหัสด้วยการวิเคราะห์ ลักษณะเด่นแบบท้องถิ่น (Local Feature Analysis) เช่น จมูก ปาก แก้ม กระดูก และแนวขากรรไกรซึ่งจะสร้างสิ่งที่เป็นเอกลัษณ์ของบุคคลคนเดียวกันเรียกว่า พิมพ์ของใบหน้า (Faceprint) พิมพ์ของใบหน้านี้สามารถนำไปค้นหาฐานข้อมูลในแบบ real-time และมีความรวดเร็วในการประมาณสูงมากจนกระทั่งสามารถทำกับภาพนิ่งและกับภาพวิดีโอได้ ซึ่งความสามารถจริงของระบบอยู่ที่ความเร็ว และการแก้ไขปัญหาเรื่องการขมวดคิ้ว การยิ้ม การกระพริบตา การใส่แว่น ปัญหาของแสง การย่อขยาย การวางตำแหน่งศรีษะ และการเอียงได้ทั้งหมด อีกทั้งยังเป็นแนวทางที่ใช้ลักษณะ 3 มิติที่เป็นลักษณะเด่นแบบท้องถิ่น คือ จมูก ปาก แก้ม กระดูก และแนวขากรรไกรที่สามารถจะพัฒนาเป็นการประมาณใบหน้าเมื่ออายุเพิ่มขึ้นหรือลดลงได้อีกด้วย จึงเป็นสุดยอดแนวทางของการรู้จำใบหน้าอย่างแท้จริงที่สามารถใช้ในการค้นหาประวัติของเด็กหลงทางที่ไม่สามารถบอกบ้านหรือพ่อแม่ได้ หรือค้นหาคนที่หายไปหลายปีได้ว่าหน้าตาปัจจุบันเป็นอย่างไร

2.6.7.1 การหาองค์ประกอบสำคัญของภาพใบหน้า

การหาองค์ประกอบสำคัญของภาพใบหน้าสามารถแยกออกเป็น 2 ประเภทใหญ่ๆ ได้แก่

- **Appearance based method**

Appearance based method คือ การมองแต่ละจุดในภาพเป็นตัวแปร และแยกแยะความแตกต่างของภาพจากค่ากระจายตัวทางสถิติของค่าสีแต่ละพิกเซลทั้งหมดในภาพ ในวิธีนี้เราไม่จำเป็นต้องหาตำแหน่งของตา จมูก และปากภาพในภาพ

- **Model based method**

Model based method คือ การมองภาพโดยรวม และแยกแยะใบหน้าของแต่ละคนจากตำแหน่งสำคัญๆ บนใบหน้า เช่น ตา หู จมูก ปาก ให้ได้ก่อน แล้วจึงหาความสัมพันธ์ของตำแหน่งต่างๆ เหล่านี้เพื่อแยกแยะใบหน้าต่อไป

ในโครงงานนี้ได้เลือกกระบวนการ Priciple Component Analysis (PCA) ซึ่งเป็นหนึ่งในกระบวนการแบบ Appearance based method โดยทำการฉายภาพใบหน้าไปยังแกนของความแปรปรวนร่วม (Covariance) ที่มากที่สุด เพื่อให้หาความแตกต่างของภาพแต่ละภาพได้แม่นยำขึ้น และวิธีนี้ยังนำหลักการไอเกนเวกเตอร์ (Eigenvector) ซึ่งจะเรียกว่าไอเกนเฟซ (Eigenface) มาใช้เพื่อลดการคำนวณลง และทำให้การทำงานมีประสิทธิภาพมากยิ่งขึ้น

2.6.7.2 ทฤษฎีและวิธีการใช้ไอเกนเฟซ

2.6.7.2.1 วิธีของไอเกนเฟซ

จากการศึกษาก่อนหน้านี้ ของระบบจดจำใบหน้า โดยส่วนมากแล้วการทำงานของระบบนี้จะจดจำใบหน้าอย่างชี้เฉพาะเจาะจง โดยการวัดค่าจากตัวกำหนดที่สัมพันธ์กันและเหมาะสม จากข้างต้นนี้ได้ให้ข้อมูลกับพวกเราว่าการป้อนรหัสและถอดรหัสรูปใบหน้านั้น จะเน้นที่จุดหลักๆ คือลักษณะหน้าตา โดยทั่วไปแล้วบางทีลักษณะหน้าตาอาจจะไม่ตรงกับลักษณะใบหน้าที่แท้จริงในบางส่วน เช่น ตา จมูก ริมฝีปาก และ ผม

ในทฤษฎีของ Language of Information เราต้องการที่จะคัดเลือกข้อมูลที่สัมพันธ์กันกับรูปหน้าตาเพื่อตั้งให้เป็นรหัสออกมาให้เหมือนมากที่สุดเท่าที่จะเป็นไปได้และเปรียบเทียบกับรูปหน้าที่ตั้งรหัสโดยใช้ฐานข้อมูลของรูปประพรรณสัณฐาน ขั้นตอนแรกที่จะคัดเลือกข้อมูลนี้ต้องประกอบด้วยรูปของใบหน้าที่ได้จากกลุ่มใบหน้าที่ได้ถ่ายมา โดยมีหลายรูปหน้า หน้าตาหลายๆ แบบ และใช้รูปภาพเหล่านี้มาตั้งใส่รหัสหลังจากนั้นมาเปรียบเทียบกับหน้าเป็นรายบุคคลไป

ในระบบทางคณิตศาสตร์นั้น เราต้องการที่จะหาองค์ประกอบที่สำคัญของส่วนประกอบใบหน้า หรือ ไอเกนเวกเตอร์ของโควาเรียนเมทริกซ์ ของรูปแบบใบหน้า ไอเกนเวกเตอร์สามารถคิดแยกรูปแบบลักษณะของรูปหน้าที่มีลักษณะที่คล้ายคลึงกันออกเป็นชุดๆได้ ซึ่งในแต่ละรูปจะมี

ไอเกนเวกเตอร์ที่แตกต่างกันออกไป ดังนั้นเราสามารถแสดงผลของไอเกนเวกเตอร์ออกมาอย่างร่างๆ หยาบๆ ได้ ที่เราเรียกกันว่า ไอเกนเฟซ

ในแต่ละรูปหน้านั้นสามารถแสดงผลออกมาในรูปแบบของการรวมตัวของเส้นตรงต่างๆ ของไอเกนเฟซ จำนวนหมายเลขที่ไอเกนเฟซจะเท่ากันจำนวนรูปของใบหน้าในชุดที่มี อย่างไรก็ตาม ใบหน้าเหล่านี้ก็สามารถประมาณหาไอเกนเฟซที่ดีที่สุดได้ ซึ่งนั่นจะมีค่าไอเกนวาลูร์มากที่สุดดังนั้นจะมีความสัมพันธ์ก็จะมากในรูปชุดนี้ด้วย เหตุผลหลักๆ ที่ใช้ไอเกนเฟซน้อยๆ เพื่อการคำนวณที่มีประสิทธิภาพมากขึ้น

2.6.7.2.2 ขั้นตอนการสร้างไอเกนเฟซและคำนวณค่าน้ำหนัก

ขั้นตอนที่ 1 : เซต S ซึ่งประกอบไปด้วย ข้อมูลภาพจำนวน m ภาพซึ่งได้ทำการแปลงเป็นเวกเตอร์ที่มีขนาดเท่ากับ n

$$S = \{T_1, T_2, T_3, \ldots, T_m\}$$

$$T_k = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{bmatrix} \quad \text{โดยที่} \quad k = 1,2,3,\ldots,n$$

ขั้นตอนที่ 2 : หาค่าเฉลี่ยของข้อมูลภาพชนิดเวกเตอร์ในแต่ละชุด

$$\psi_i = \frac{1}{n}\sum_{k=1}^{n} t_k \quad \text{โดยที่} \quad i = 1,2,3,\ldots,m$$

ขั้นตอนที่ 3 : หาผลต่างระหว่าง ภาพ กับ ค่าเฉลี่ยของภาพๆนั้น จะได้เมตริกซ์ส่วนเบี่ยงเบนมาตรฐาน

$$\phi_i = T_i - \psi_i \quad \text{โดยที่} \quad i = 1,2,3,\ldots,m$$

ขั้นตอนที่ 4 : หาเมตริกซ์ความแปรปรวน

$$C = AA^T$$

$$\text{โดยที่} \quad A = \{\phi_1, \phi_2, \phi_3, \ldots, \phi_m\}$$

ขั้นตอนที่ 5 : หาค่าไอเกนวาลูร์ และไอเกนเวกเตอร์จากเมตริกซ์

ขั้นตอนที่ 6 : นำค่าไอเกนเวกเตอร์มาคำนวณหาค่าไอเกนเฟซ

$$u_i = \sum_{k=1}^{m} v_k \phi_k$$

เมื่อ v_k คือ ไอเกนเวกเตอร์ โดยที่ $i = 1,2,3,\ldots,m$

ขั้นตอนที่ 7 : นำค่าไอเกนเฟซ มาคำนวณหาค่าน้ำหนัก

$$w_i = u_i^T \times (T_i - \psi_i)$$

2.6.7.2.3 ระยะทางแบบยูคลิเดียน (Euclidian Distance Estimation)

การวัดค่าคล้ายคลึงของข้อมูลโดยการใช้ฟังก์ชั่นการวัดค่าระยะทางแบบยูคลิเดียน เป็นการวัดระยะห่างระหว่างข้อมูลที่ต้องเปรียบเทียบความคล้ายคลึงกันโดยระยะห่างระหว่างข้อมูลจะแปรผันตรงกับความคล้ายคลึงกันของข้อมูล โดยผลลัพธ์ที่ได้จากการวัดที่มีค่ามากกว่า แสดงว่าความคล้ายคลึงกันของข้อมูลมีน้อยกว่าหรือค่าที่วัดได้น้อยกว่าจะมีความคล้ายคลึงกันของข้อมูลมากกว่า ฟังก์ชั่นการวัดค่าระยะทางแบบยูคลิเดียนดังสมการ (4)

$$error = \sqrt{\sum_{i=1}^{n} \sum_{j=1}^{n} \left(w_{(i,j)} - w_{(i,j)ref} \right)^2} \qquad (4)$$

เมื่อ $w_{(i,j)}$ คือ ค่าน้ำหนักที่ได้จากการทดสอบ

$w_{(i,j)ref}$ คือ ค่าน้ำหนักที่ได้จากกระบวนการเรียนรู้

การวัดระยะห่างโดยวิธี Euclidian มีปัญหาที่ต้องระมัดระวังในสองประเด็นหลัก คือ ค่าระยะห่างจะมีความไว (Sensitive) กับขนาดของวัตถุที่แตกต่างกันเช่น วัตถุ a วัดค่าเป็นหน่วยเมตร ในขณะที่วัตถุ b วัดค่าออกมาเป็นหน่วย เซนติเมตร ประเด็นที่สองที่เป็นปัญหาของการวัดโดยวิธี Euclidian คือ ค่าความห่างไกลที่คำนวณได้ ไม่ได้สนใจความเกี่ยวข้องสัมพันธ์กัน (Correlation) ของวัตถุต่างๆ อาจมีบางวัตถุมีความเกี่ยวข้องสัมพันธ์กันสูง

2.6.8 การประมวลผลภาพแบบบริเวณ (Local Image Processing)

สำหรับกระบวนการกระทำการกับภาพแบบบริเวณนี้ ค่าระดับความเข้มเทาของพิกเซลในแต่ละจุดในภาพผลลัพธ์จะขึ้นกับค่าระดับความเข้มเทาของกลุ่มพิกเซลที่อยู่ในบริเวณข้างเคียงกัน (Neighborhood Pixels) ของภาพต้นฉบับ แสดงลักษณะการกระทำการกับภาพบริเวณ ตัวอย่าง

ของการประมวลผลภาพทางดิจิตอลแบบนี้ได้แก่การกรองสัญญาณภาพในสเปเชียลโดเมน (Spatial Domain Filtering) หรือที่นิยมเรียกว่า การคอนโวลูชัน (Convolution)

2.6.9 การกรองข้อมูลภาพ (Image Filtering)

การกรองข้อมูลภาพ (Image Filtering) คือ การประมวลภาพแบบบริเวณอย่างหนึ่ง โดยหลักการก็คือ การนำภาพต้นฉบับไปผ่านตัวกรองสัญญาณเพื่อให้ได้ภาพผลลัพธ์ออกมา โดยภาพผลลัพธ์ที่ได้จะมีคุณสมบัติแตกต่างจากภาพต้นฉบับ วัตถุประสงค์หลักของการกรองข้อมูลภาพคือการเน้นหรือลดทอนคุณสมบัติบางประการของภาพต้นฉบับ เพื่อให้ได้ภาพผลลัพธ์ที่มีคุณสมบัติตามต้องการ การกรองข้อมูลภาพเป็นวิธีการที่จำเป็นอย่างยิ่งในกระบวนการประมวลผลภาพดิจิตอล เนื่องจากในการใช้งานจริง ภาพที่ได้มาบางครั้งอาจจะมีสัญญาณรบกวนหรือสัญญาณไม่พึงประสงค์อื่นๆ ปะปนอยู่ด้วย การกรองข้อมูลภาพสามารถปรับปรุงให้ภาพมีคุณภาพที่ดีขึ้น

ในการกรองข้อมูลภาพจะพิจารณาภาพดิจิตอล คือ สัญญาณสองมิติที่ประกอบขึ้นจากสัญญาณสองมิติที่ประกอบขึ้นจากสัญญาณความถี่ต่างๆ ผสมกันอยู่อยู่ในสัดส่วนที่ต่างกัน การออกแบบตัวกรองจึงเป็นการกำหนดว่าต้องการกำจัดสัญญาณความถี่ใดออกไป หรือต้องการเลือกสัญญาณความถี่ใดบ้าง ดังนั้นในการกรองสัญญาณความถี่ใดออกไป หรือต้องการเลือกสัญญาณความถี่ใดบ้าง ดังนั้นในการกรองสัญญาณใดๆต้องทราบความถี่หรือช่วงความถี่ของสัญญาณที่ต้องการและสัญญาณที่ไม่ต้องการ จากนั้นจะเลือกตัวกรองที่เหมาะสมมาใช้เพื่อกำจัดสัญญาณที่ไม่ต้องการออก ตัวอย่างเช่น การลดสัญญาณรบกวนของภาพ หรือในบางครั้งภาพต้นฉบับมีความพร่ามัว ไม่ชัดเจน ซึ่งสามารถที่จะทำให้ภาพมีความคมชัดมากขึ้นได้โดยใช้วิธีการกรองข้อมูลภาพ

2.6.10 การคอนโวลูชันแบบสองมิติ (Two-dimensional Convolution)

การกรองข้อมูลภาพ (Image Filtering) เป็นวิธีการประมวลผลภาพแบบบริเวณ หรือเรียกว่า การคอนโวลูชัน ซึ่งการคอนโวลูชันคือการกระทำกันระหว่างภาพ (Image) กับ มาส์ค (Mask) คือ แมทริกซ์ขนาด $n \times m$ ของชุดตัวเลขที่จะนำไปซ้อนทับภาพที่ตำแหน่งต่างๆเพื่อหาผลลัพธ์ของการคอนโวลูชัน ถ้ากำหนดให้มาส์ค $M(i,j)$ เป็นหน้าต่างขนาด $n \times m$ และภาพ $F\left(x,y\right)$ ต้นฉบับมีขนาดการคอนโวลูชันระหว่างมาร์คกับภาพสามารถแสดงได้ดังสมการ (5)

$$G(x,y) = M * F = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1} M(i,j) \cdot F\left(x-i, y-j\right) \qquad (5)$$

โดยที่ $G(x,y)$ คือภาพผลลัพธ์ที่ได้จากการคอนโวลูชันที่จุดพิกัด (x,y) ใดๆ ของภาพ

จากสมการ (5) จะเห็นว่าระดับความเข้มเทาที่จุดพิกัด (x,y) ในภาพผลลัพธ์สามารถคำนวณได้จากการหาผลรวมของผลคูณระหว่างค่าสัมประสิทธิ์หรือค่าถ่วงน้ำหนักในมาส์คกับค่า

ระดับความเข้มเทาของภาพในบริเวณที่มาส์คซ้อนทับอยู่ หรืออาจกล่าวได้ว่า ค่าระดับความเข้มเทาของพิกเซลแต่ละจุดของภาพผลลัพธ์จะขึ้นอยู่กับค่าระดับความเข้มเทาของกลุ่มพิกเซลท่าอยู่ในบริเวณข้างเคียงกัน (Neighborhood Pixels) โดยการทำคอนโวลูชันนั้น จะต้องทำการเคลื่อนย้ายมาส์คไปทางแนวแกนนอนและแกนตั้ง หรือในแนวแถวและแนวหลักของภาพตลอดทั่วทั้งภาพ

2.6.11 การลดสัญญาณรบกวนภาพ (Image Noise Reduction)

รูปภาพดิจิตอลที่ใช้งานจริง บางครั้งภาพต้นฉบับที่จัดเก็บมาได้อาจจะมีสัญญาณรบกวน (Noise) มาปรากฏทับซ้อนบนค่าระดับความเข้มเทาของจุดเทา ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีวิธีการประมวลภาพที่จะนำมาใช้งานในการลดสัญญาณรบกวนของภาพ โดยทั่วไปแล้วสัญญาณรบกวน คือ ข้อมูลภาพในช่วงความถี่สูงดังนั้นในการขจัดสัญญาณรบกวน สามารถที่จะใช้ตัวกรองความถี่ต่ำผ่าน (Low-pass Filtering) มาทำการลดหรือขจัดสัญญาณรบกวนของภาพได้ วิธีการลดสัญญาณรบกวนแบบเป็นเชิงเส้นโดยอาศัยวิธีการคอนโวลูชันและการลดสัญญาณรบกวนแบบไม่เป็นเชิงเส้น

2.6.12 การลดสัญญาณรบกวนแบบเป็นเชิงเส้น

การขจัดสัญญาณรบกวนออกจากมีวัตถุประสงค์ในการกำจัดสัญญาณรบกวนซึ่งเป็นสัญญาณประเภทความถี่สูง โดยพื้นฐานนั้นอาศัยหลักการทำการเฉลี่ยค่าความเข้มแสงเฉพาะบริเวณ หรืออีกนัยหนึ่งก็คือการกรองสัญญาณความถี่ต่ำผ่าน (Low-pass Filtering) ผลกระทบของการกรองด้วยสัญญาณความถี่ต่ำผ่านจะทำให้สัญญาณรบกวนถูกทำให้ลดลง ในขณะที่ภาพผลลัพธ์จะมีความเรียบ (Smooth) การขจัดสัญญาณรบกวนออกจากภาพในบางกรณีภาพผลลัพธ์จะพร่ามัว (Blurring Effect) มีความคมชัดน้อยลง เนื่องจากขอบของวัตถุในรูปภาพจะเป็นบริเวณที่มีความเปลี่ยนแปลงระดับค่าความเข้มแสง และจัดว่าเป็นสัญญาณความถี่สูงที่ถูกกรองออกไป ดังนั้นเทคนิคการกำจัดสัญญาณส่วนใหญ่จะเน้นที่การกำจัดสัญญาณรบกวนแต่จะไม่ทำลายขอบของวัตถุในภาพเท่าที่จะสามารถทำได้ มาส์คที่ใช้ในการขจัดสัญญาณรบกวนจะมีลักษณะค่าสัมประสิทธ์ของตัวกรองทุกตำแหน่งเป็นบวกทั้งหมด และผลรวมของค่าสัมประสิทธิ์ภายในมาส์คจะมีค้เท่ากับหนึ่ง

2.6.13 ตัวกรองแบบค่าเฉลี่ย (Moving Averaging Filter)

ตัวกรองความถี่แบบค่าค่าเฉลี่ยคือตัวกรองแบบความถี่ต่ำผ่านชนิดหนึ่งซึ่งผลรวมของค่าสัมประสิทธิ์ของตัวกรองชนิดนี้จะมีค่าเป็นหนึ่ง วิ่งมีทั้งข้อดีและข้อเสีย คือ การเพิ่มขนาดของมาส์คมีขนาดใหญ่จะช่วยลดสัญญาณรบกวนได้มากขึ้น หรืออาจกล่าวได้ว่ายิ่งขนาดของมาส์คมี

ขนาดใหญ่ ปริมาณของสัญญาณรบกวนก็จะถูกขจัดไปได้มาก แต่ภาพผลลัพธ์ที่ได้จะมีลักษณะพร่ามัวมากขึ้น

2.6.14 การลดสัญญาณรบกวนแบบไม่เป็นเชิงเส้น

ในบางกรณี สัญญาณรบกวนบางประเภทไม่สามารถที่จะใช้ตัวกรองหรือฟิลเตอร์แบบเป็นเชิงเส้น (Linear Filtering) ในการลดสัญญาณรบกวนเพื่อให้ได้ภาพผลลัพธ์ที่สมบูรณ์ได้ ดังนั้นในส่วนนี้จะกล่าวถึงวิธีการในการขจัดสัญญาณรบกวนแบบ Salt and Pepper Noise ในภาพดิจิตอลด้วยตัวกรองหรือฟิงเตอร์แบบไม่เป็นเชิงเส้น (Nonlinear Filtering) ด้วยวิธีการกรองแบบมัธยฐาน (Median Filter) และตัวกรองแบบ Minimum and Maximum Filer

2.6.15 ตัวกรองแบบมัธยฐาน (Median Filter)

เป็นตัวกรองที่อาศัยการพิจารณาข้อมูลทางสถิติของข้อมูลภาพโดยใช้ค่ามัธยฐาน (Median) การหาค่ามัธยฐานทำได้โดยการนำข้อมูลระดับความเข้มเทาของภาพที่บริเวณมาร์คครอบคลุมอยู่มาทำการเรียงค่าจากน้อยไปมากตามค่าระดับความเข้มเทาของข้อมูลภาพ ซึ่งค่ามัธยฐานจะเป็นค่าตำแหน่งกึ่งกลางของกลุ่มข้อมูลที่พิจารณาจากนั้นนำค่ามัธยฐานที่ได้นั้นแทนค่ากลับลงไปในตำแหน่งตรงกลางของมาส์ค

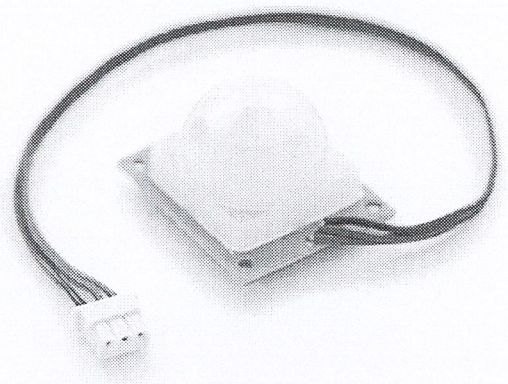
2.6.16 ตัวกรองแบบค่าสูงสุดและค่าต่ำสุด (Minimum and Maximum Filter)

เป็นตัวกรองแบบไม่เป็นเชิงเส้น (Nonlinear Filtering) ที่คล้ายกับตัวกรองแบบมัธยฐาน (Median Filter) กล่าวคือ ตัวกรองแบบมัธยฐานจะแทนค่าตำแหน่งตรงกลางของมาส์คด้วยค่ามัธยฐาน แต่ Minimum Filter และ Maximum Filter จะถูกแทนด้วยค่าต่ำสุดและค่าสูงสุด ตามลำดับ โดยแทนค่าผลลัพธ์ที่ได้ลงในตำแหน่งตรงกลางของมาส์ค

2.6.17 การหาขอบภาพ (Edge Detection)

ขอบของภาพ (Edge) คือส่วนของข้อมูลที่แสดงถึงโครงร่างของวัตถุภายในภาพ ซึ่งประกอบด้วยข้อมูลของภาพที่มีความสำคัญและมีประโยชน์ในการนำไปประยุกต์ใช้งานด้านจ่างๆ เช่น ขอบของภาพ สามารถนำไปใช้ในการระบุถึงขนาดของวัตถุที่อยู่ในภาพ การนำไปประยุกต์ใช้ในการแยกแยะระหว่างวัตถุหรือข้อมูลในภาพกับส่วนของพื้นหลังของภาพ (Background) หรือการนำไปใช้ในการระบุวัตถุที่อยู่ภายในภาพ ขอบต่างๆ ภายในภาพเกิดจากการเปลี่ยนแปลงของค่าระดับความเข้มเทาแบบทันทีทันใด จากค่าระดับต่ำๆ ไปเป็นค่าระดับความเข้มเทาสูงๆ หรือในทางตรงกันข้าม เปลี่ยนจากค่าระดับความเข้มเทาสูงๆ ไปเป็นค่าระดับความเข้มเทาต่ำๆ หรือเกิดจากความไม่ต่อเนื่องของค่าระดับความเข้มเทาของพิกเซลที่อยู่อยู่บริเวณติดกัน (Neighborhood Pixels) กล่าวคือ ค่าระดับความเข้มเทาของพิกเซลที่อยู่ติดกันมีค่าแตกต่างกันมาก

2.7 เซ็นเซอร์ตรวจจับความเคลื่อนไหว PIR (PASSIVE INFRARED)



รูปที่ 2.27 PIR (PASSIVE INFRARED) [11]

เป็นตัวตรวจจับความเคลื่อนไหวของสิ่งมีชีวิต (Motion Sensor) แบบอินฟราเรด ซึ่งใช้หลักการตรวจจับที่เรียกว่า ไพโรอิเล็ตริก (Pyro-Electric) อันเป็นการตรวจจับการแผ่รังสีอินฟราเรด หากระดับของการแผ่รังสีไม่เปลี่ยนแปลง แสดงว่าสิ่งมีชีวิตที่ต้องการตรวจจับนั้นไม่มีการเคลื่อนไหว แต่ถ้าหากมีการเคลื่อนไหวเกิดขึ้น ระดับของการแผ่รังสีจะเปลี่ยนแปลง

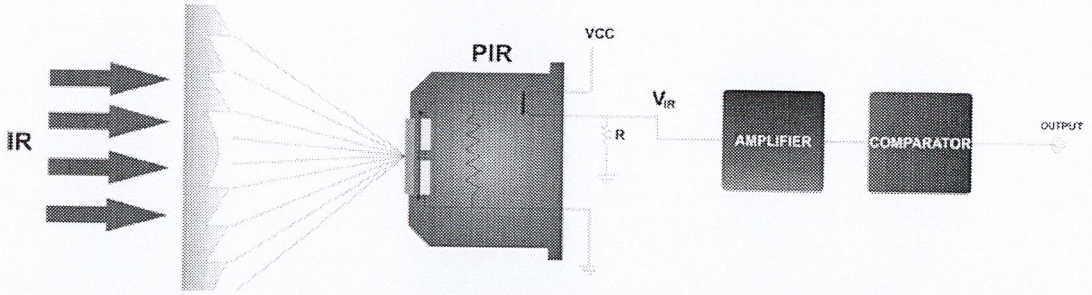
2.7.1 คุณสมบัติที่สำคัญ

- ระยะการตรวจจับสูงสุด 20 ฟุต
- เมื่อตรวจพบความเคลื่อนไหวจะให้ผลการทำงานเป็นสัญญาณลอจิก "1"
- ใช้เวลาในการปรับตัวเพื่อตรวจจับการเปลี่ยนแปลงช่วง 10 ถึง 60 วินาทีหลังจากได้รับไฟเลี้ยง
- สามารถทำงานได้ที่ 3.3 ถึง 12 โวลต์
- ไม่สามารถตรวจจับมนุษย์หรือสัตว์ที่นิ่งเฉยได้

2.7.2 หลักการทำงาน

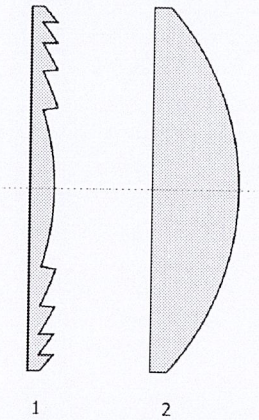
สิ่งมีชีวิตไม่ว่าจะเป็นมนุษย์หรือสัตว์เลือดอุ่นนั้นในภาวะที่ยังมีชีวิตอยู่ จะมีการกระจายพลังงานความร้อนออกมาจากตัวเองในรูปของการแผ่รังสีอินฟราเรดตลอดเวลา ซึ่งเป็นชนิดของพลังงานรังสีซึ่งไม่สามารถมองเห็นได้ด้วยตาของมนุษย์แต่สามารถถูกตรวจจับได้ มันเป็นชนิด

ของเสปคตัมแม่เหล็กไฟฟ้าที่มีความยาวคลื่นมากกว่าแสงที่เราสามารถมองเห็นได้ โดยจะมีปริมาณมากหรือน้อยขึ้นอยู่กับสภาพของร่างกายในขณะนั้น



รูปที่ 2.28 แสดงการทำงานของเซ็นเซอร์ตรวจจับความเคลื่อนไหว [11]

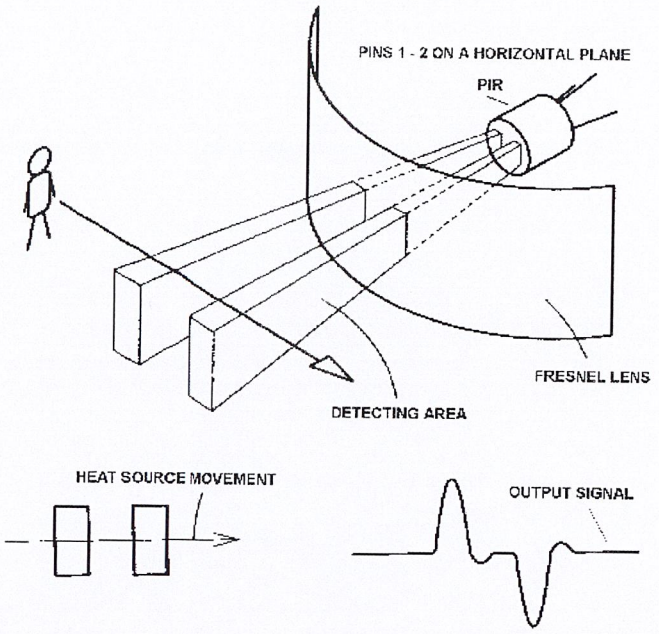
ดังรูปที่ 2.28 เป็นภาพแสดงการทำงานของตัวตรวจจับ PIR โดยพลังงานความร้อนจากมนุษย์หรือสัตว์เลือดอุ่นทำให้เกิดการแผ่รังสีอินฟราเรดขึ้น รังสีจะถูกรวมไปที่ตัวตรวจจับโดยใช้เลนส์แบบพิเศษที่เรียกว่า เลนส์เฟรสเนล (Fresnel lens) ไปยังส่วนที่ใช้ในการรับรู้ทำด้วยวัสดุที่มีโครงสร้างเป็นรูปผลึกซึ่งทำให้พื้นผิวเกิดประจุไฟฟ้าเมื่อมันตรวจพบความแตกต่างของพลังงานความร้อนในช่วงรังสีอินฟราเรดจากนั้นตัวตรวจจับจะทำการขยายสัญญาณแล้วส่งไปยังวงจรเปรียบเทียบเพื่อสร้างสัญญาณเอาต์พุตต่อไป



รูปที่ 2.29 โครงสร้างของเลนส์เฟรสเนล [11]

ดังรูปที่ 2.29 เลนส์เฟรสเนล (Fresnel lens) เป็นเลนส์แบบขั้นบันไดที่ยอมให้แสงผ่านได้มากจากทุกทิศทาง เนื่องจากตัวเลนส์ได้ถูกสร้างขึ้นโดยลดเนื้อวัสดุในส่วนที่ไม่มีผลกับการหักเหของแสงลงไป ทำให้สามารถทำเลนส์ขนาดใหญ่ที่มีน้ำหนักเบาได้ โดย PIR ใช้เลนส์เฟรสเน

ลในการรวมแสงเข้ามาจากทุกทิศทางเพื่อรวมสัญญาณไปยังส่วนตรวจจับแสงอินฟราเรด เพื่อให้การตรวจจับการเปลี่ยนแปลงของรังสีอินฟราเรดมีความเร็วสูง



รูปที่ 2.30 การทำงานของ PIR เมื่อมีมนุษย์เดินผ่าน แหล่งกำเนิดรังสีอินฟราเรด และสัญญาณเอาต์พุต [11]

ดังรูปที่ 2.30 แสดงเหตุการณ์ขณะที่มนุษย์เคลื่อนไหวผ่านระยะตรวจจับของตัวตรวจจับ ซึ่งในเวลาที่มนุษย์เคลื่อนไหวนั้นจะมีการปล่อยพลังงานความร้อนออกมาในรูปของการแผ่รังสีอินฟราเรด ทำให้ตัวตรวจจับ PIR สามารถตรวจจับการแผ่รังสีที่แตกต่างกันได้ จึงปล่อยสัญญาณเอาต์พุตที่เป็นลอจิกสูงออกมาในขณะที่ตรวจพบการเคลื่อนไหว จากนั้นกลับมาเป็นลอจิกต่ำจนกว่าจะพบการเปลี่ยนแปลงของระดับรังสีอินฟราเรดอีกครั้ง

2.8 Winsock

Winsock หรือ Windows Socket API เป็น Dynamic link library ที่จำเป็นในการใช้งานผ่าน Network ด้วย Protocol TCP/IP หรือ UPD เป็นตัวช่วยในการสื่อสารระหว่างคอมพิวเตอร์ ซึ่งมีอยู่ในระบบปฏิบัติการ Windows เวอร์ชั่นต่างๆอยู่แล้วและ Winsock จะมีฟังก์ชั่นต่างๆเพื่อเรียกใช้งานใน Protocol TCP/IP ได้โดยคำว่า Socket เป็นคำศัพท์ที่คุ้นกันสำหรับการเขียน

โปรแกรมที่มีการติดต่อผ่าน Network ปัจจุบัน .Net Framework นั้นได้ทำให้ใช้งานง่ายๆแล้ว มีขั้นตอนการทำงานดังนี้

รูปที่ 2.31 ขั้นตอนการทำงานของ Winsock [11]

2.8.1 หลักการทำงาน

- ทางฝั่งเซิร์ฟเวอร์มีการกำหนดพอร์ตที่ใช้ในการเชื่อมต่อเพื่อรอการติดต่อจากฝั่งไคลเอนต์
- ทางไคลเอนต์ติดต่อมายังเซิร์ฟเวอร์โดยต้องใช้พอร์ตการเชื่อมต่อที่เหมือนกัน
- หลังจากที่ฝั่งเซิร์ฟเวอร์และไคลเอนต์ติดต่อกันได้สำเร็จจึงสามารถรับและส่งข้อมูลถึงกันได้

2.9 บทสรุป

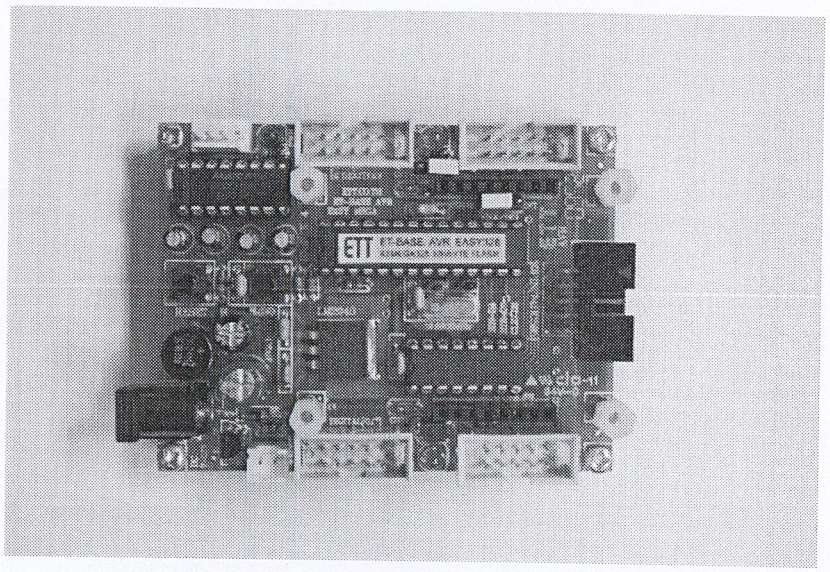
ในบทนี้จะกล่าวถึงทฤษฎีที่เกี่ยวข้องทั้งหมดที่ใช้ในการทำโครงงาน โดยเนื้อหารายละเอียดประกอบไปด้วยทฤษฎีและหลักการทำงานของไมโครคอนโทรลเลอร์ ATmega 328 การติดต่อสื่อสารพอร์ทอนุกรม (Serial Port) เครื่อข่ายอินเตอร์เน็ต การส่งข้อความสั้น การประมวลผลภาพ และ Windows Socket API รวมทั้งรายละเอียดของอุปกรณ์ที่ใช้ในการทำโครงงาน คือ เซอร์โวมอเตอร์ และเซ็นเซอร์ตรวจจับความเคลื่อนไหว

บทที่ 3
การออกแบบ

3.1 ส่วนอุปกรณ์ฮาร์ดแวร์

3.1.1 บอร์ดควบคุม

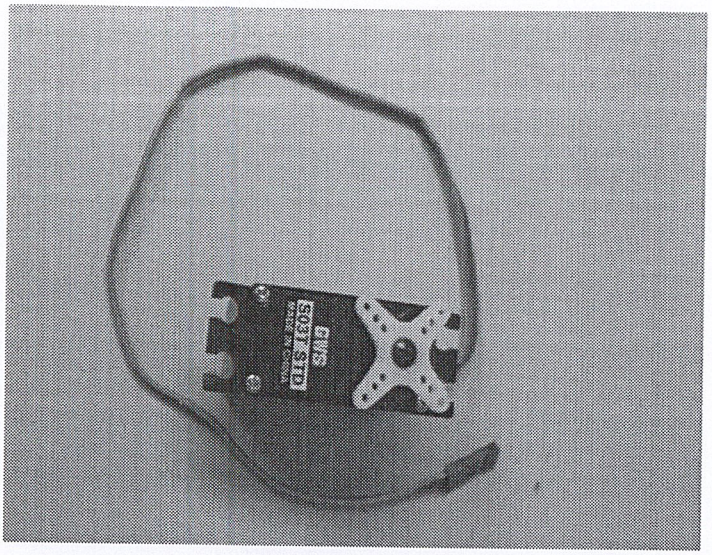
เป็นส่วนของบอร์ดสำหรับควบคุมการหมุนของเซอร์โวมอเตอร์ เป็นตัวที่คอยตรวจสอบตำแหน่งและสร้างสัญญาณพัลส์ (Pulse) เพื่อใช้ในการควบคุมโดยเลือก ไมโครคอลโทรลเลอร์ตระกูล AVR รุ่น ATMEGA328 นี้ เพราะสามารถที่จะรับรู้ค่า อินเตอร์รัพต์ได้โดยบอร์ดมีลักษณะดังรูปที่ 3.1



รูปที่ 3.1 บอร์ดไมโครคอนโทรลเลอร์ ATMEGA 328

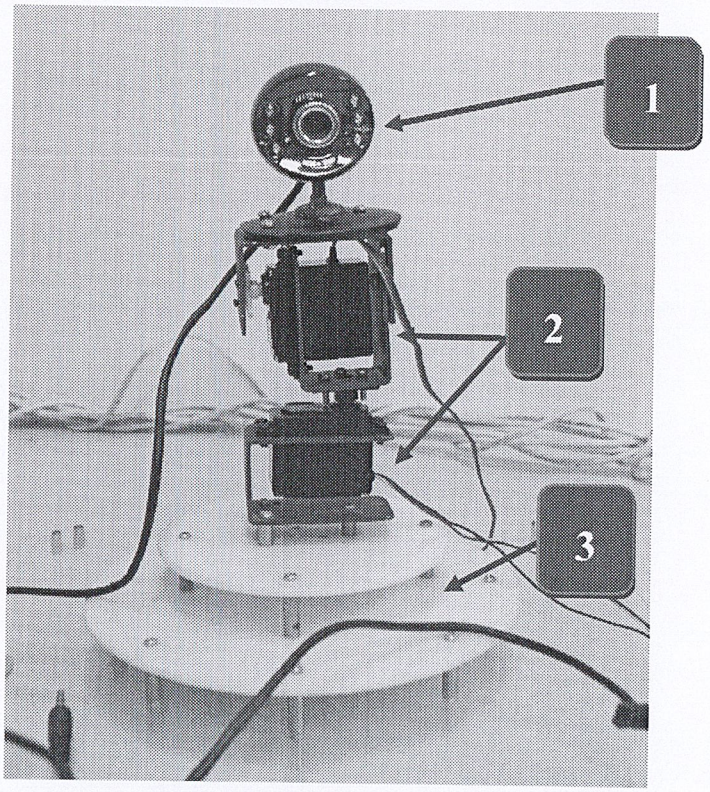
3.1.2 มอเตอร์ควบคุมการหมุนของกล้อง

มอเตอร์ที่ใช้เป็นเซอร์โวมอเตอร์ ซึ่งเป็นมอเตอร์ไฟฟ้ากระแสตรง มีสายแยกจากไฟเลี้ยงและกราวด์ เป็นสายที่ใช้สำหรับการควบคุม ข้อดีในการเลือกใช้มอเตอร์ชนิดนี้ คือ มีขนาดเล็ก น้ำหนักเบา แรงบิดสูง กินพลังงานน้อย ต่อสัญญาณลอจิกที่เป็น TTL เลเวล (Level) ได้โดยตรงไม่ต้องมีการต่อวงจรไดร์ฟ (Drive) ดังรูปที่ 3.2



รูปที่ 3.2 เซอร์โวมอเตอร์

3.1.3 ส่วนการออกแบบโครงสร้างฐานกล้อง

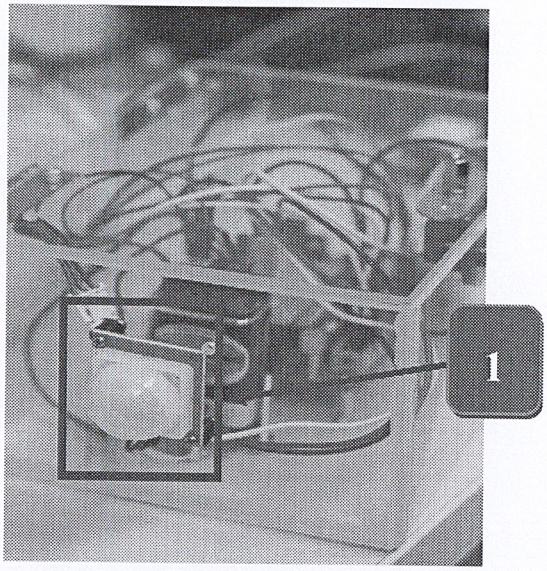


รูปที่ 3.3 ส่วนการออกแบบโครงสร้างฐานกล้อง

จากรูปที่ 3.3 แสดงถึงการออกแบบโครงสร้างฐานกล้อง โดยโครงสร้างฐานกล้องประกอบไปด้วย 3 ส่วน คือ ในส่วนที่ 1 เป็นส่วนของกล้องเว็บแคมที่ใช้ในโครงงาน ซึ่งเป็นกล้องเว็บแคมที่สามารถถ่ายภาพได้ในสถานที่มืด ในส่วนที่ 2 เป็นส่วนของเซอร์โวมอเตอร์ซึ่งใน

โครงงานนี้ใช้เซอร์โวมอเตอร์จำนวน 2 ตัว โดยเซอร์โวมอเตอร์ตัวบนนั้นทำหน้าที่ในการหมุนกล้องเว็บแคมในทิศทางขึ้น-ลง และเซอร์โวมอเตอร์ตัวล่างนั้นบังคับกล้องในทิศทางซ้าย-ขวา และสุดท้ายในส่วนที่ 3 คือส่วนของฐานที่ทำหน้าที่รองรับกล้องและเซอร์โวมอเตอร์

3.1.4 ส่วนของเซนเซอร์ตรวจจับการเคลื่อนไหว

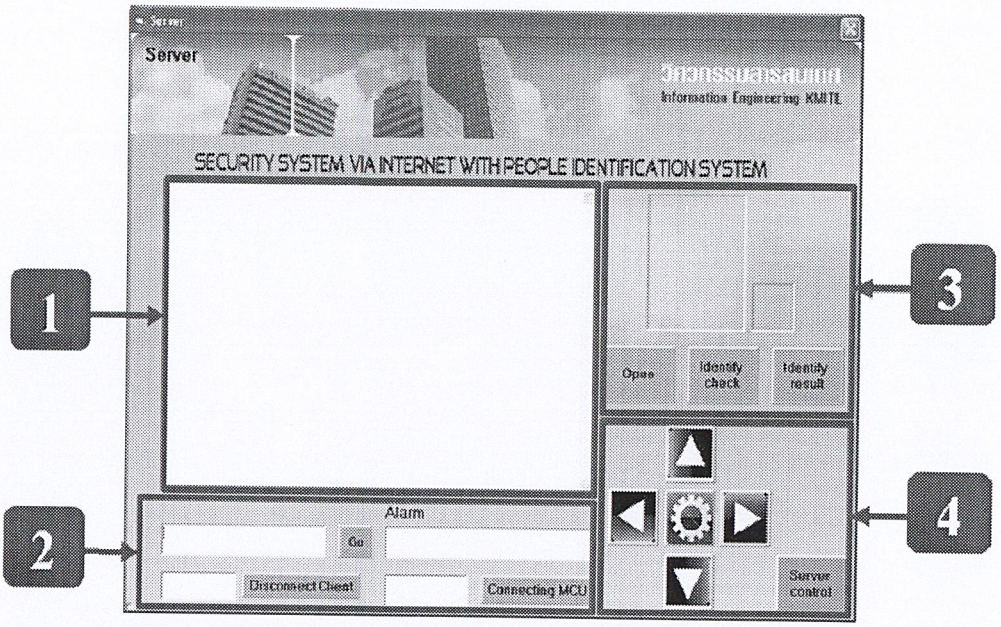


รูปที่ 3.4 เซนเซอร์ตรวจจับการเคลื่อนไหว

จากรูปที่ 3.4 แสดงภาพการออกแบบในส่วนของเซนเซอร์ตรวจจับการเคลื่อนไหว โดยได้นำเซนเซอร์ติดกับกล่องอุปกรณ์ดังส่วนที่ 1 เพื่อทำการตรวจสอบการเคลื่อนไหว เมื่อพบผู้บุกรุกเข้ามาในระบบ เซนเซอร์จะทำการแจ้งเตือนไปยังแอพพลิเคชั่น

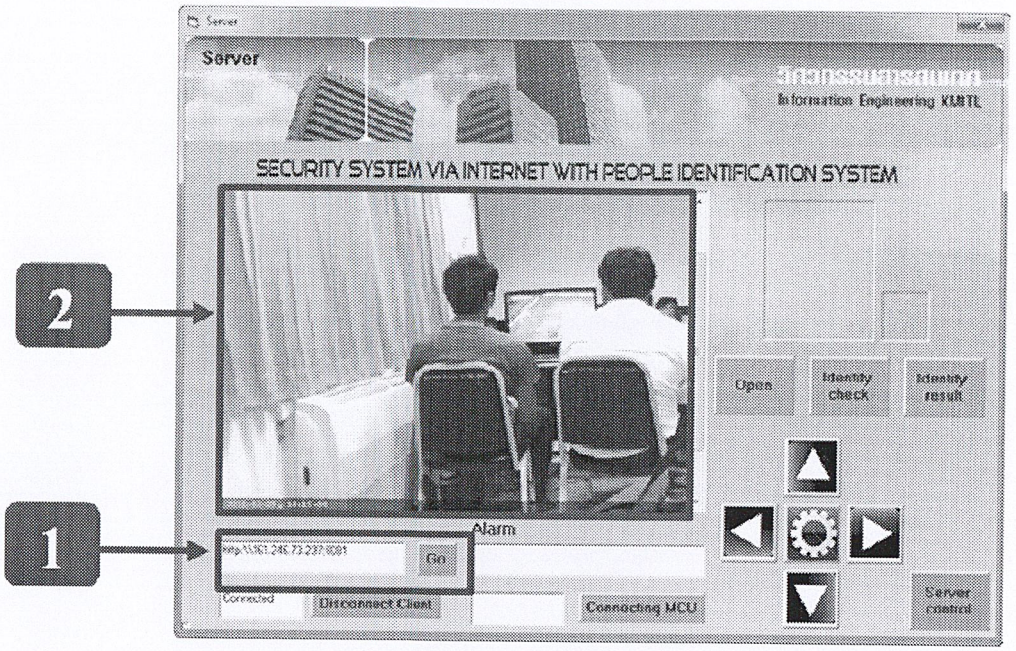
3.2 ส่วนของซอฟต์แวร์

3.2.1 หน้าจอแอพพลิเคชั่นฝั่งเซิร์ฟเวอร์



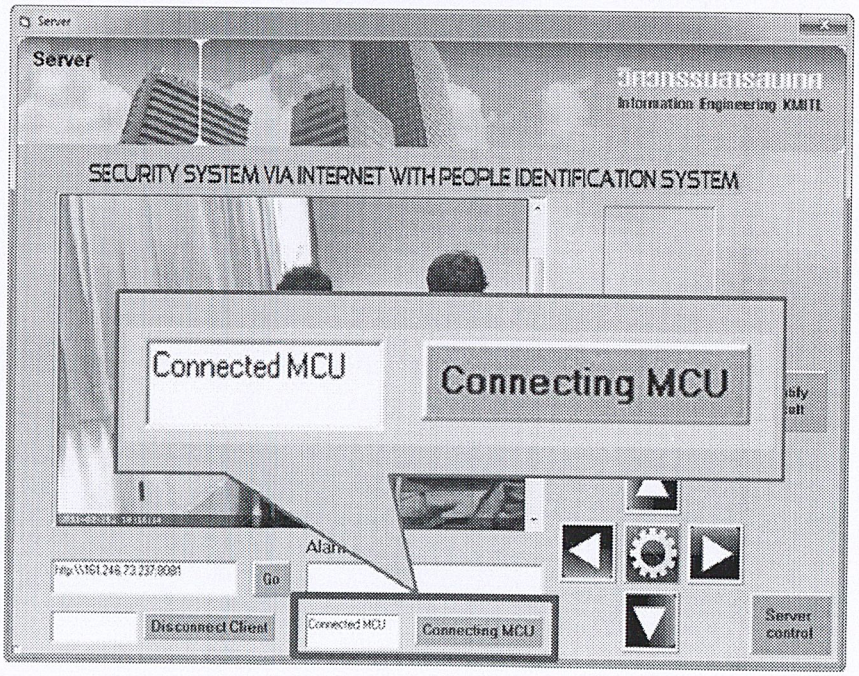
รูปที่ 3.5 แสดงหน้าจอแอพพลิเคชั่นฝั่งเซิร์ฟเวอร์ ขณะรันโปรแกรม

จากรูปที่ 3.5 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการเปิดโปรแกรมในฝั่ง เซิร์ฟเวอร์ ขึ้นมา โดยในส่วนที่ 1 นั้นจะเป็นส่วนของหน้าจอแสดงผลที่ติดต่อรับภาพจากกล้องเว็บแคม ส่วนที่ 2 คือ ส่วนของการเชื่อมระหว่างแอพลิเคชั่นกับฮาร์ดแวร์ ถัดมาสามารถควบคุมฐานกล้องในทิศทางต่างๆได้โดยใช้ปุ่มคำสั่งในส่วนที่ 4 และในส่วนที่ 3 คือหน้าจอสำหรับเรียกดูไฟล์รูปที่ได้ทำการบันทึกไว้หน้านี้ กับ หน้าจอแสดงผลจากการตรวจสอบระบุตัวบุคคล



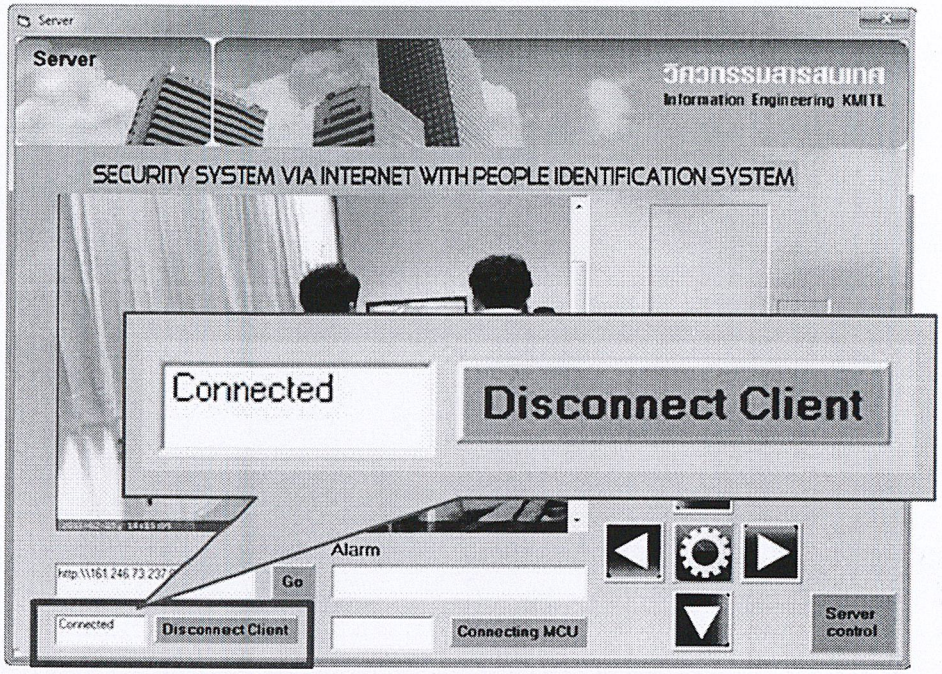
รูปที่ 3.6 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการติดต่อกับกล้องเว็บแคม

จากรูปที่ 3.6 ทำการระบุ Domain name ลงในช่องว่างส่วนที่ 1 เพื่อทำการเชื่อมต่อกับกล้องเว็บแคม เมื่อแอพพลิเคชั่นได้ทำการเชื่อมต่อเป็นที่เรียบร้อยแล้ว หน้าจอแสดงผลในส่วนที่ 2 จะปรากฏภาพที่ได้รับจากกล้องเว็บแคมขึ้นมา



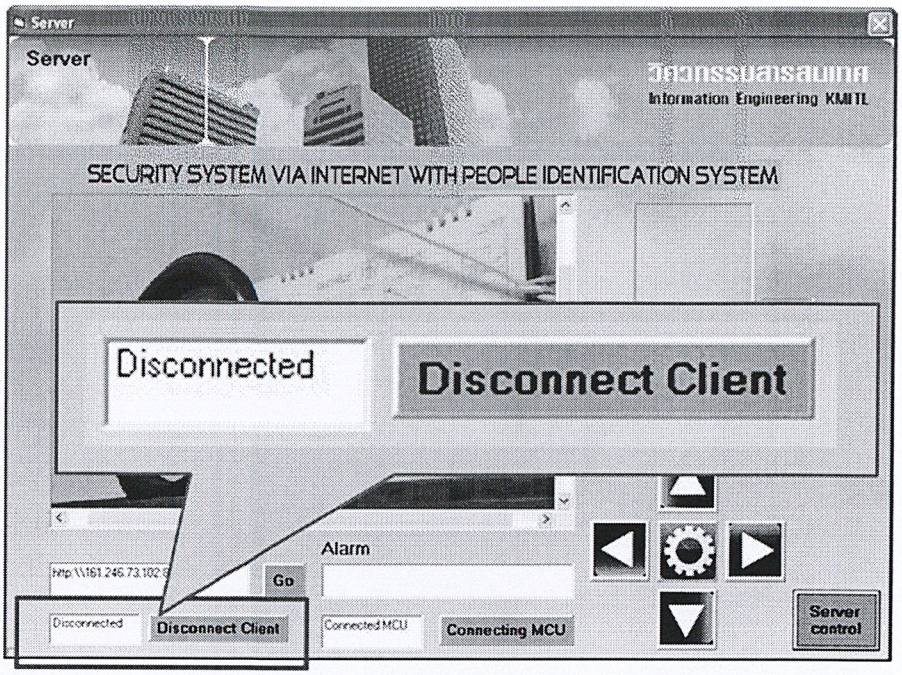
รูปที่ 3.7 แสดงหน้าจอเมื่อทำการเชื่อมต่อแอพพลิเคชั่นกับไมโครคอนโทรลเลอร์

จากรูปที่ 3.7 เมื่อทำกดปุ่ม Connecting MCU เพื่อทำการเชื่อมต่อแอพพลิเคชั่นกับไมโครคอนโทรลเลอร์ให้สามารถควบคุมฐานกล้องพร้อมทั้งรับค่าจากเซนเซอร์ตรวจจับการเคลื่อนไหว แอพพลิเคชั่นจะมีการแสดงข้อความแจ้งสถานะว่าได้ทำการเชื่อมต่อเรียบร้อยแล้ว โดยแสดงข้อความว่า “ Connected MCU ” ดังรูป



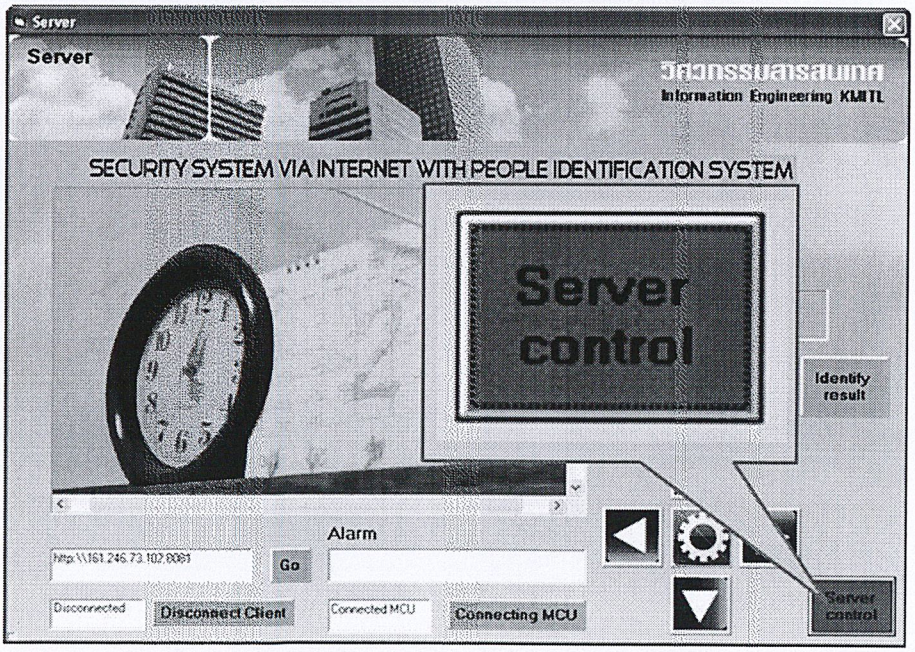
รูปที่ 3.8 แสดงหน้าจอแอพพลิเคชั่นเมื่อ เซิร์ฟเวอร์ เชื่อมต่อกับฝั่งไคลเอนต์

จากรูปที่ 3.8 เมื่อทางฝั่งไคลเอนต์ ได้ทำการเชื่อมต่อมายัง เซิร์ฟเวอร์ และแอพพลิเคชั่นได้ทำการเชื่อมต่อกันเรียบร้อยแล้ว แอพพลิเคชั่นจะมีข้อความแจ้งสถานะว่า “ Connected ” ขึ้นในช่องว่าง ดังรูป



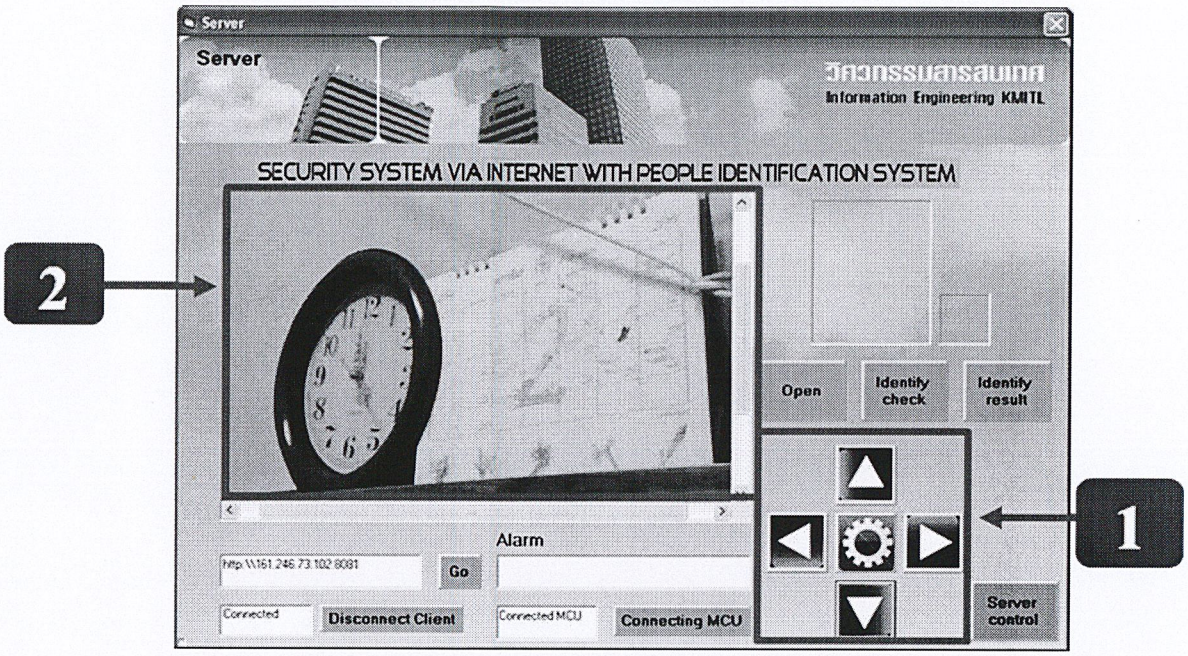
รูปที่ 3.9 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการตัดการเชื่อมต่อกับฝั่งไคลเอนต์

จากรูปที่ 3.9 แสดงหน้าจอแอพพลิเคชั่นเมื่อผู้ควบคุมได้ทำการกดปุ่ม Disconnect Client เพื่อทำการตัดการเชื่อมต่อกับฝั่งไคลเอนต์ จากนั้นเมื่อตัดการเชื่อมต่อกันระหว่างแอพพลิเคชั่นฝั่งเซิร์ฟเวอร์ กับฝั่งไคลเอนต์ เรียบร้อย แอพพลิเคชั่นจะทำการแจ้งสถานะ โดยปรากฏข้อความขึ้นว่า “Disconneted” เพื่อให้ผู้ควบคุมทราบ ดังรูป



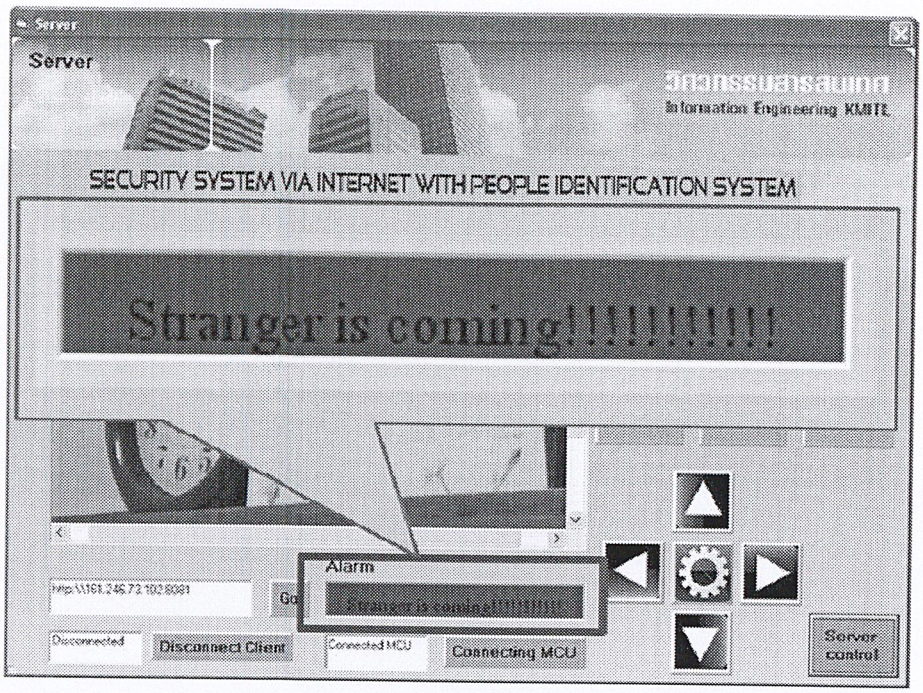
รูปที่ 3.10 แสดงสถานะปุ่ม Server control

จากรูปที่ 3.10 แสดงสถานะของปุ่ม Server control โดยปุ่ม Server control มีหน้าที่ในการกำหนดว่าให้แอพพลิเคชั่นในฝั่งเซิร์ฟเวอร์ หรือทางฝั่งไคลเอนต์ เป็นผู้ควบคุมทิศทางของกล้อง โดยถ้าปุ่ม Server control แสดงสถานะเป็นสีแดง ทางฝั่งเซิร์ฟเวอร์ จะไม่สามารถควบคุมกล้องได้ เป็นทางฝั่งไคลเอนต์ ที่สามารถควบคุมฐานกล้องไปในทิศทางต่างๆ โดยในทางกลับกันหากปุ่ม Server control แสดงสถานะเป็นสีเขียว ก็คือทางฝั่ง เซิร์ฟเวอร์ จะเป็นผู้ควบคุมฐานกล้องและทางฝั่งไคลเอนต์ จะไม่สามารถควบคุมได้



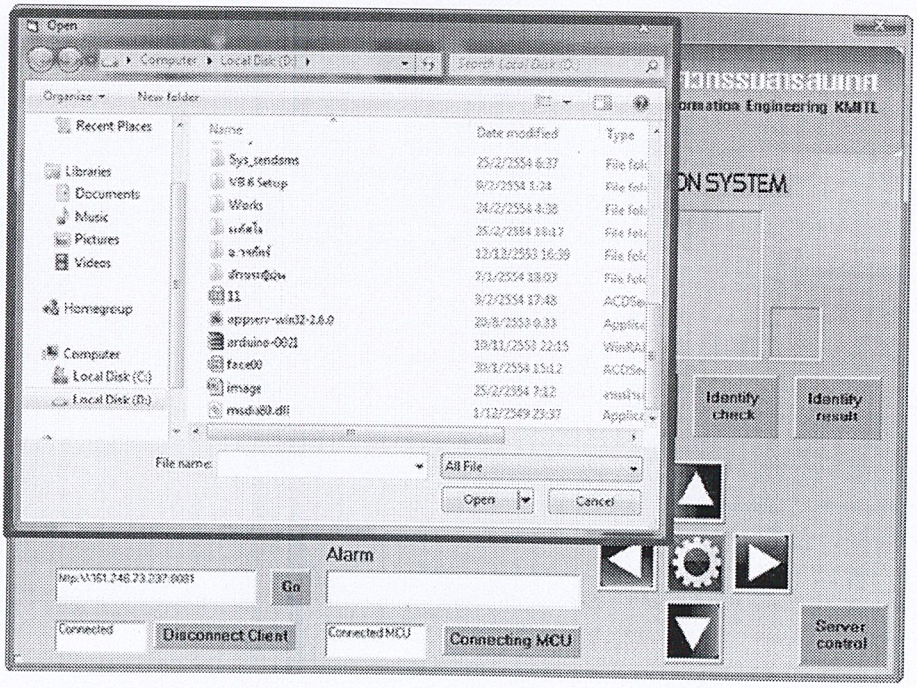
รูปที่ 3.11 แสดงหน้าจอเมื่อได้ทำการควบคุมฐานกล้อง

จากรูปที่ 3.11 หลังจากได้ทำการเชื่อมต่อระหว่างแอพพลิเคชั่นกับไมโครคอนโทรลเลอร์เป็นที่เรียบร้อยแล้ว และปุ่ม Server control แสดงสถานะเป็นสีเขียวแล้ว เมื่อผู้ควบคุมทำการกดปุ่มบังคับทิศทางของฐานกล้องในส่วนที่ 1 นั้น กล้องก็จะทำการหมุนไปยังทิศทางต่างๆที่ผู้ควบคุมต้องการ จะเห็นได้จากตำแหน่งของภาพที่ได้รับจากกล้องมีการเปลี่ยนแปลงไป ดังรูปในส่วนที่ 2



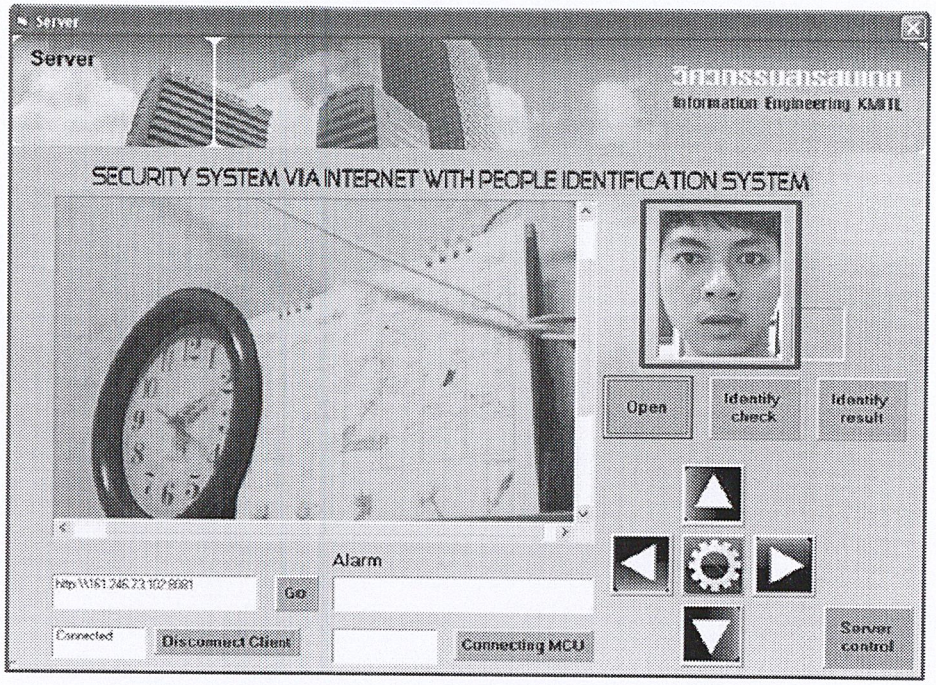
รูปที่ 3.12 แสดงหน้าจอเมื่อเซ็นเซอร์ตรวจพบผู้บุกรุก

จากรูปที่ 3.12 เมื่อเซนเซอร์ตรวจจับการเคลื่อนไหวได้ทำการตรวจพบผู้บุกรุก เซ็นเซอร์จะทำการส่งข้อมูลมายังแอพพลิเคชั่น จากนั้นเมื่อแอพพลิเคชั่นได้รับข้อมูลจะทำการแจ้งเตือนให้ผู้ควบคุมทราบผ่านทางการแสดงข้อความแจ้งเตือนว่า “Stranger is coming!!!!” ดังรูป



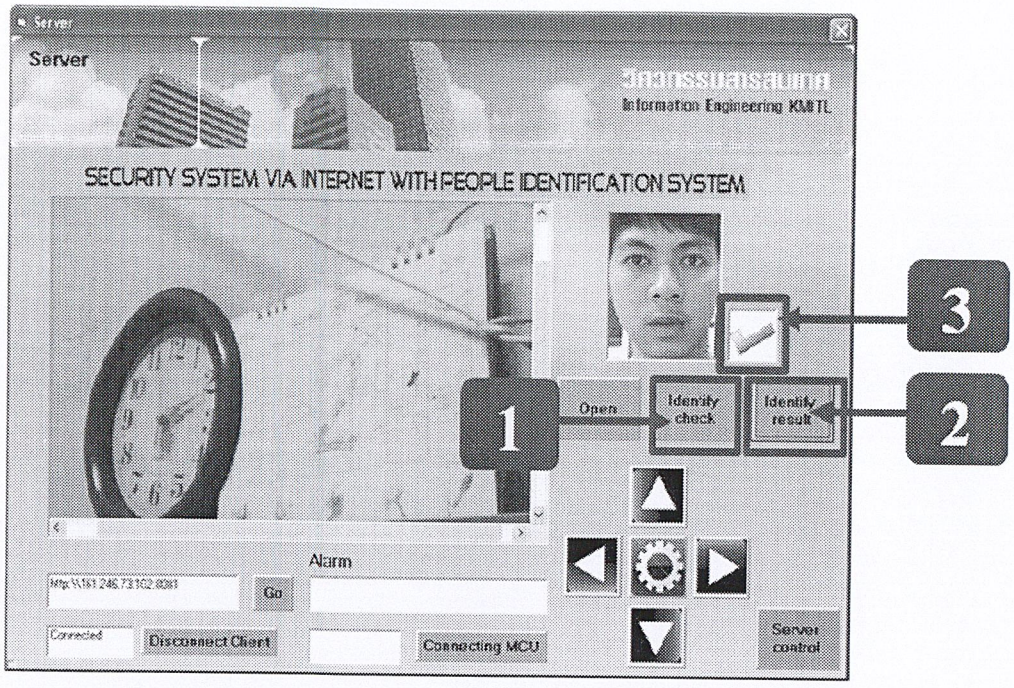
รูปที่ 3.13 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการกดปุ่ม Open

จากรูปที่ 3.13 เมื่อผู้ควบคุมทำการกดปุ่ม Open จะปรากฏหน้าต่าง Open ขึ้นมาดังรูป เพื่อให้ผู้ควบคุมทำการเลือกไฟล์ภาพที่ได้บันทึกไว้ก่อนหน้านี้ โดยการเลือกไฟล์ภาพที่ต้องการ จากนั้นกด Open



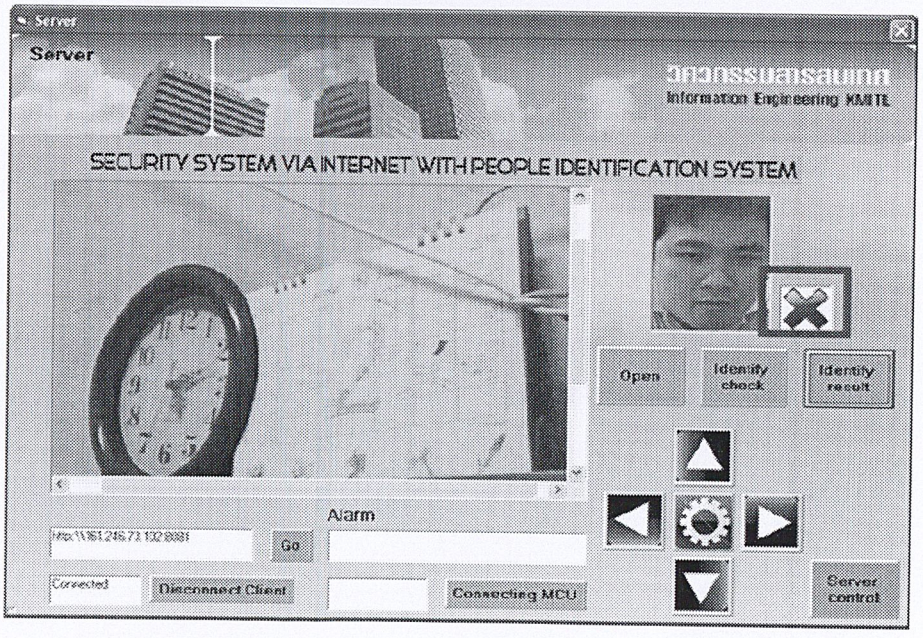
รูปที่ 3.14 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการเลือกไฟล์ภาพขึ้นมา

จากรูปที่ 3.14 เมื่อผู้ควบคุมได้ทำการเลือกไฟล์ภาพที่ได้ทำการบันทึกไว้ก่อนหน้านี้ ขึ้นมานั้น ภาพที่ได้ทำการเลือกจะปรากฏขึ้นบนหน้าจอแอพพลิเคชั่นดังรูป โดยสามารถนำไปทำการประมวลผลเพื่อระบุตัวบุคคลต่อไป



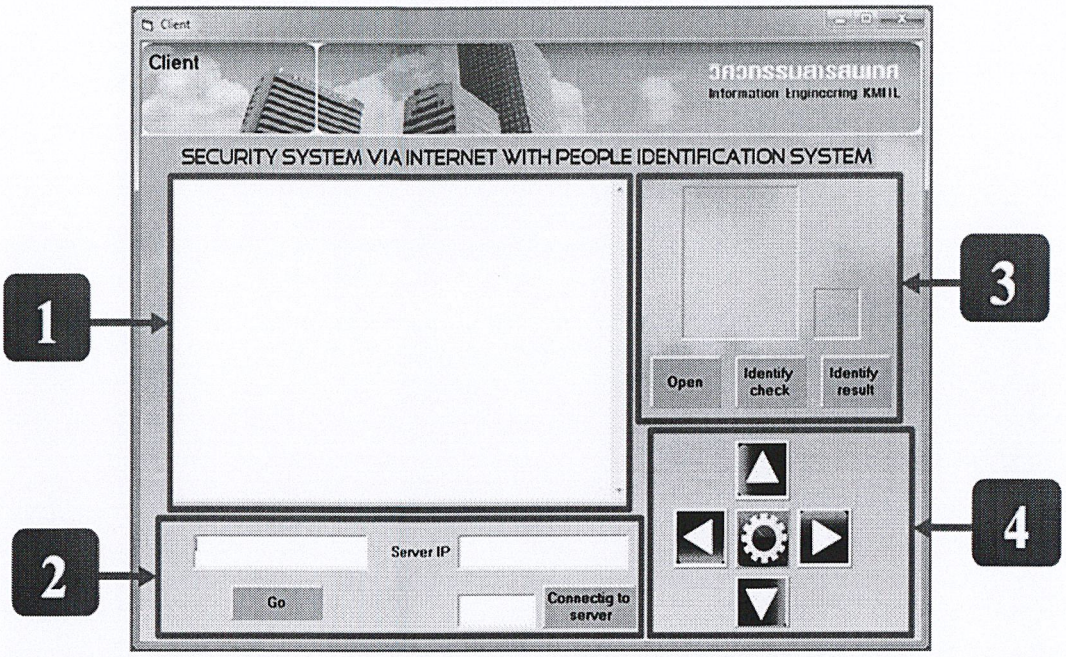
รูปที่ 3.15 แสดงขั้นตอนการประมวลผลภาพเพื่อระบุตัวบุคคล

จากรูปที่ 3.15 เมื่อผู้ควบคุมทำการเลือกไฟล์ภาพที่ทำการบันทึกไว้ก่อนหน้านี้ขึ้นมา จากนั้นผู้ควบคุมสามารถที่จะทำการประมวลผลภาพเพื่อระบุตัวบุคคลโดยทำการกดปุ่ม Identify check เพื่อสั่งการให้ส่วนประมวลผลภาพเริ่มทำงาน จากนั้นกดปุ่ม Identify result ในส่วนที่ 2 เพื่อรับค่าที่ผ่านการประมวลผลกลับมาแล้วแสดงผลในส่วนที่ 3 ว่าเป็นผู้ที่อยู่ในฐานข้อมูล หรือว่าเป็นผู้บุกรุก โดยถ้าเป็นผู้ที่อยู่ในฐานข้อมูลจะแสดงผลด้วยเครื่องหมายถูก และหากเป็นผู้บุกรุกจะแสดงด้วยเครื่องหมายกากบาท ดังรูปที่ 3.16



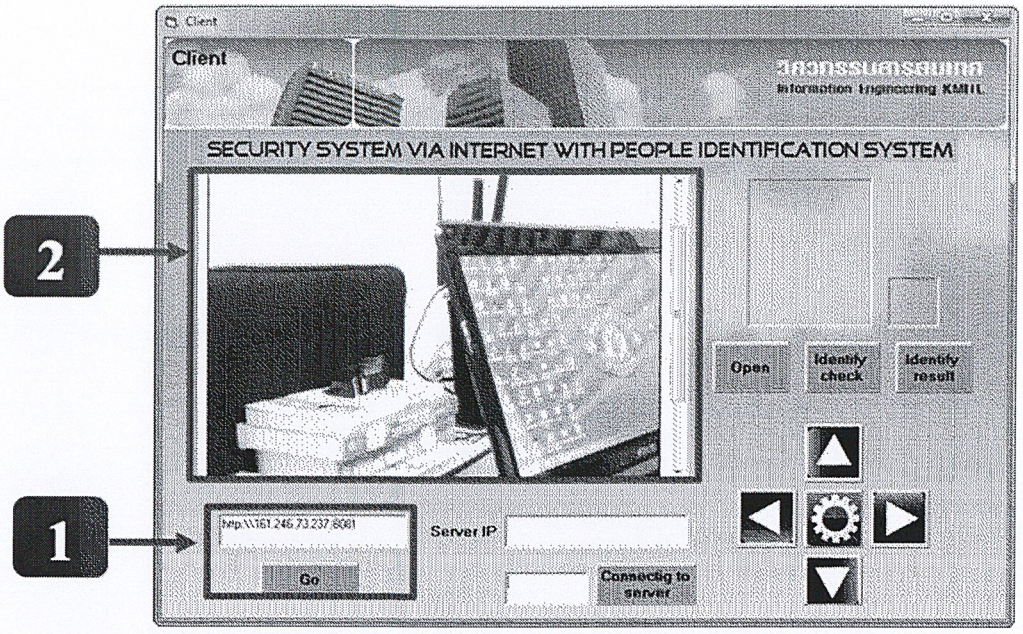
รูปที่ 3.16 แสดงเครื่องหมายกากบาทเมื่อทำการตรวจพบว่าเป็นผู้บุกรุก

3.2.2 หน้าจอแอพพลิเคชั่นฝั่งไคลเอนต์



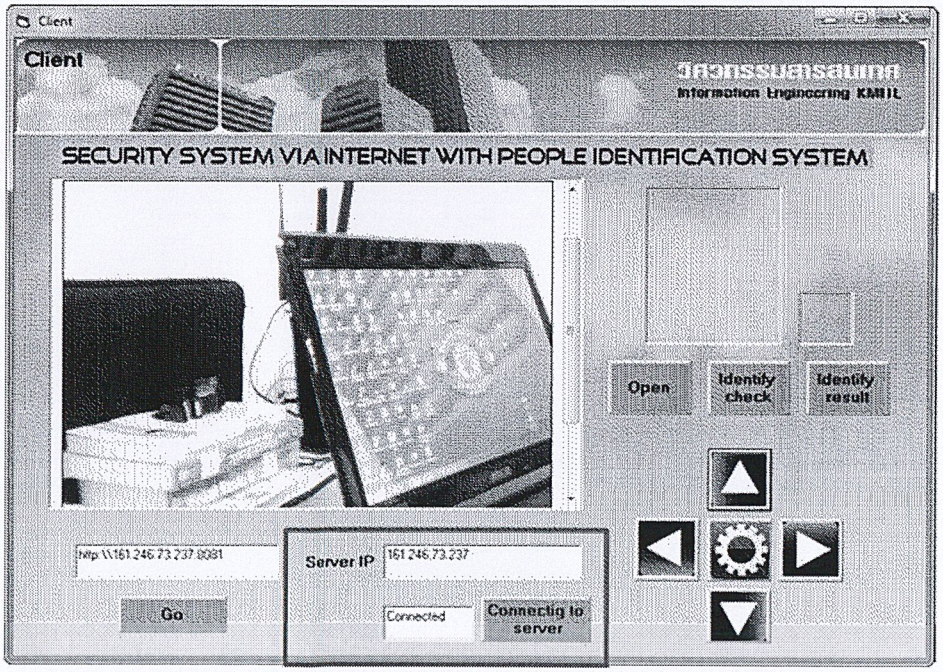
รูปที่ 3.17 แสดงหน้าจอแอพพลิเคชั่นฝั่งไคลเอนต์ ขณะรันโปรแกรม

จากรูปที่ 3.17 แสดงหน้าจอแอพพลิเคชั่นฝั่งไคลเอนต์ เมื่อทำการเปิดโปรแกรม โดยในส่วนที่ 1 เป็นหน้าจอแสดงผลจากกล้องเว็บแคมที่รับภาพมาจากฝั่ง เซิร์ฟเวอร์ ในส่วนที่ 2 คือส่วนที่ทำการตั้งค่าเพื่อเชื่อมต่อระหว่าง ไคลเอนต์ กับ เซิร์ฟเวอร์ และผู้ควบคุมสามารถควบคุมฐานกล้องให้ไปในทิศทางต่างๆ โดยกดปุ่มบังคับในส่วนที่ 4 และสามารถเรียกดูไฟล์ภาพที่ทำการบันทึกไว้ก่อนหน้านี้และประมวลผลภาพเพื่อระบุตัวบุคคลในส่วนที่ 3



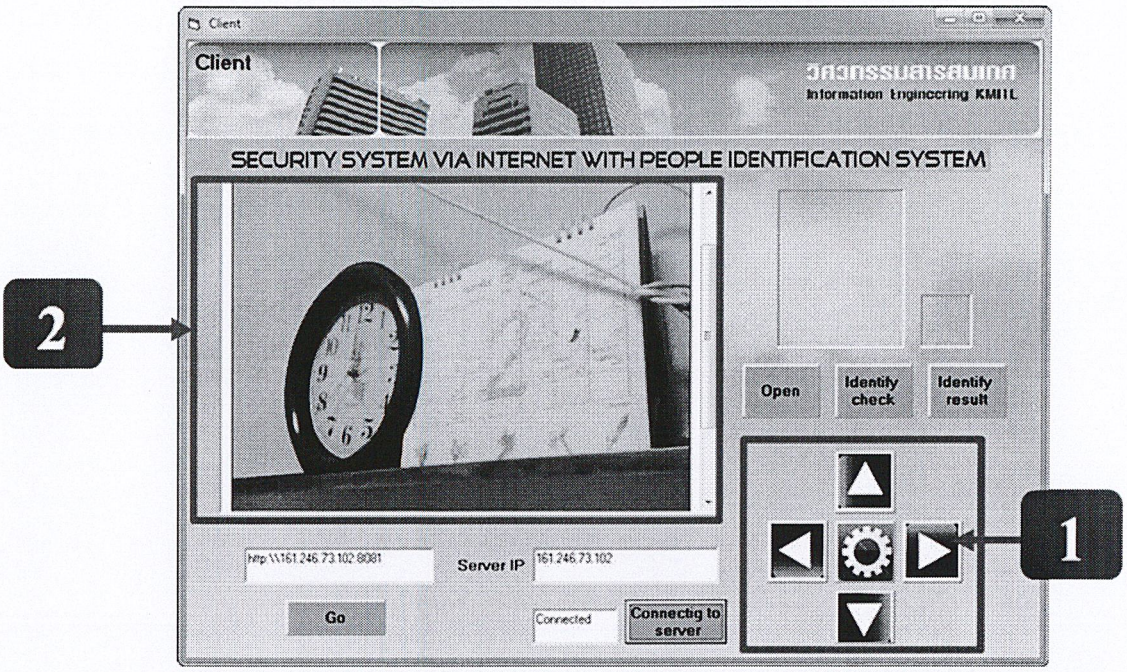
รูปที่ 3.18 แสดงหน้าจอแอพพลิเคชั่นฝั่งไคลเอนต์ เมื่อเชื่อมต่อกล้องกับฝั่ง เซิร์ฟเวอร์

จากรูปที่ 3.18 ผู้ควบคุมสามารถเชื่อมต่อกับฝั่ง เซิร์ฟเวอร์ เพื่อติดต่อกับกล้องเว็บแคม พร้อมทั้งควบคุมกล้อง โดยการระบุ Domain name ในช่องว่างส่วนที่ 1 หลังจากนั้นเมื่อทำการเชื่อมต่อสำเร็จ แอพพลิเคชั่นฝั่งไคลเอนต์ จะสามารถเห็นภาพจากกล้องเว็บแคมได้ โดยแสดงขึ้นที่หน้าจอแสดงผลในส่วนที่ 2



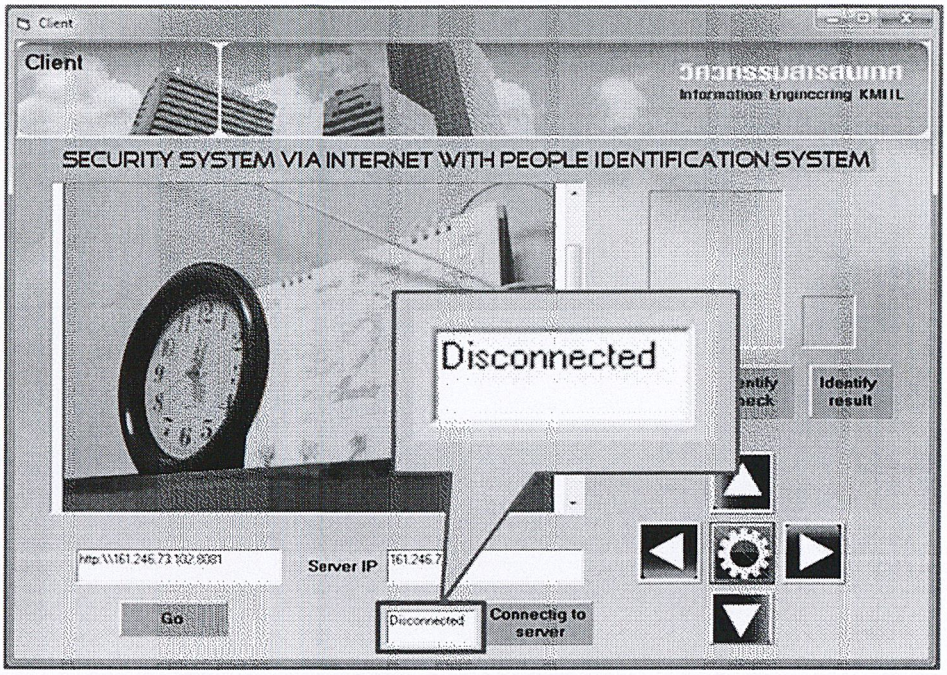
รูปที่ 3.19 แสดงการเชื่อมต่อกับฝั่งเซิร์ฟเวอร์ เพื่อทำการควบคุมฐานกล้อง

จากรูปที่ 3.19 เมื่อผู้ควบคุมต้องการที่จะควบคุมฐานกล้องให้บังคับไปในทิศทางที่ต้องการนั้น ผู้ควบคุมต้องทำการระบุค่า Domain name ลงในช่อง Server IP หลังจากนั้นกดปุ่ม Connect to server เพื่อทำการเชื่อมต่อกับแอพพลิเคชั่นฝั่งเซิร์ฟเวอร์ เพื่อควบคุมฐานกล้อง ดังรูป



รูปที่ 3.20 แสดงภาพเมื่อทำการกดปุ่มบังคับควบคุมฐานกล้อง

จากรูปที่ 3.20 หลังจากที่ผู้ควบคุมได้ทำการเชื่อมต่อแอพพลิเคชั่นฝั่งไคลเอนต์ กับฝั่งเซิร์ฟเวอร์ เป็นที่เรียบร้อยแล้วนั้น ผู้ควบคุมสามารถที่จะควบคุมกล้องให้หมุนตามทิศทางที่ต้องการได้โดยกดปุ่มที่อยู่ในส่วนที่ 1 กล้องจะทำการหมุนไปในทิศทางต่างๆ ดังหน้าจอแสดงผลในส่วนที่ 2 จะเห็นว่าตำแหน่งของภาพที่รับมาจากกล้องมีการเปลี่ยนแปลงไป



รูปที่ 3.21 แสดงข้อความแจ้งสถานะ Disconnected

จากรูปที่ 3.21 เมื่อแอพพลิเคชั่นทางฝั่งไคลเอนต์ และฝั่งเซิร์ฟเวอร์ ได้ทำการตัดการเชื่อมต่อกันเรียบร้อย แอพพลิเคชั่นจะมีการปรากฏข้อความแจ้งสถานะว่า Disconnected ขึ้นในช่องว่าง ดังรูป โดยผู้ควบคุมสามารถทำการเชื่อมต่อหรือตัดการเชื่อมต่อกับฝั่งเซิร์ฟเวอร์ ด้วยการกดปุ่ม Connecting to server

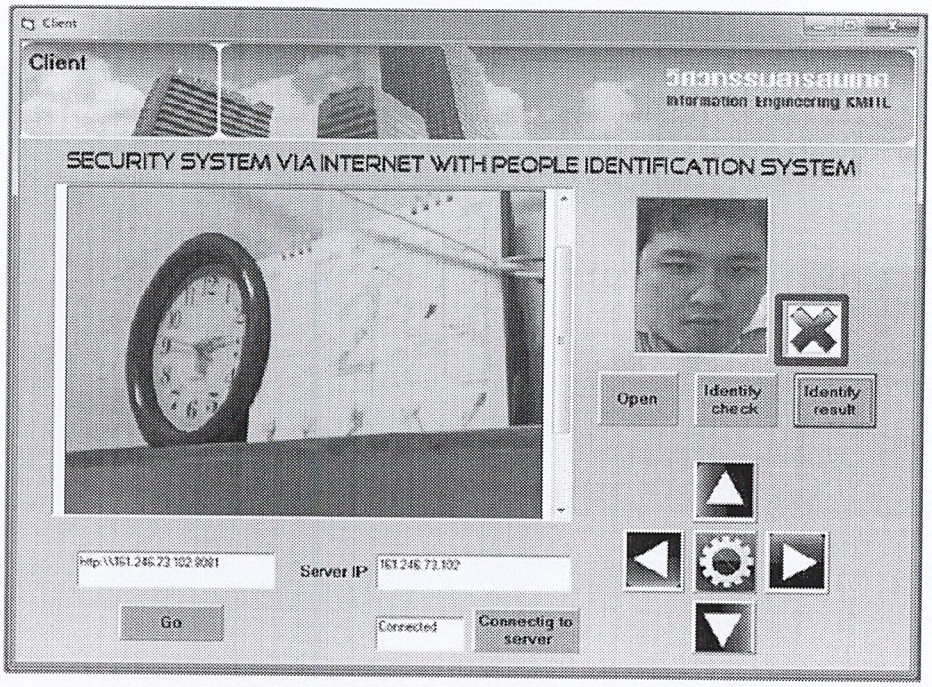
รูปที่ 3.22 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการกดปุ่ม Open

จากรูปที่ 3.22 เมื่อผู้ควบคุมต้องการเรียกดูไฟล์ภาพที่ได้ทำการบันทึกไว้ก่อนหน้านี้ สามารถทำได้โดยกดปุ่ม Open จากนั้นจะปรากฏหน้าต่าง Open ขึ้นมาให้ทำการเลือกไฟล์ภาพที่ต้องการ แล้วไฟล์ภาพที่ทำการเลือกก็จะปรากฏขึ้นดังรูปที่ 3.23

รูปที่ 3.23 แสดงหน้าจอแอพพลิเคชั่นเมื่อทำการเลือกไฟล์ภาพที่ต้องการ

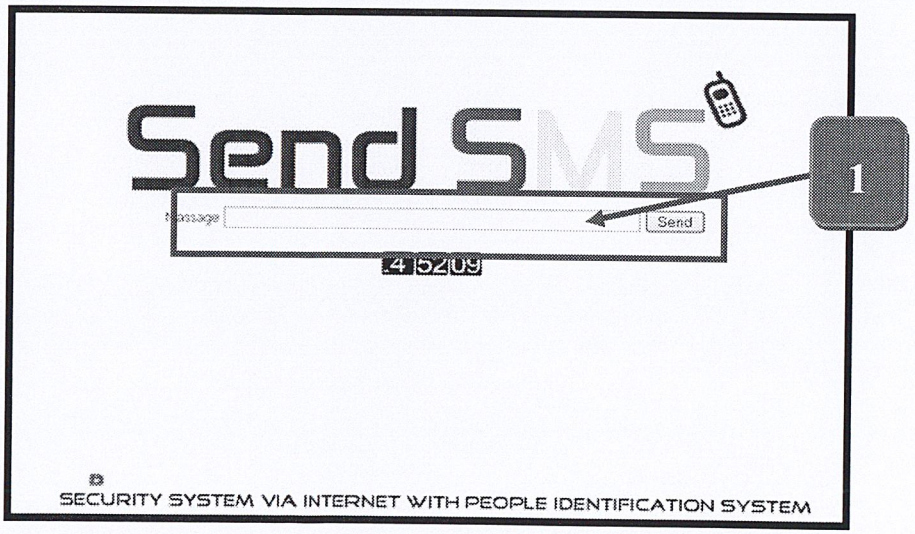
รูปที่ 3.24 แสดงขั้นตอนการประมวลผลภาพเพื่อระบุตัวบุคคลทางฝั่งไคลเอนต์

จากรูปที่ 3.24 ผู้ควบคุมสามารถทำการประมวลผลภาพเพื่อระบุตัวบุคคลจากทางฝั่งไคลเอ็นต์ ได้เช่นเดียวกับฝั่งเซิร์ฟเวอร์ โดยการทำตามขั้นตอนที่เหมือนกันกับทางฝั่งเซิร์ฟเวอร์ คือตามขั้นตอน 1 2 และผลที่ได้จะปรากฏในส่วนที่ 3 ว่าเป็นบุคคลที่มีอยู่ในฐานข้อมูลหรือว่าเป็นผู้บุกรุก โดยถ้าผลปรากฏว่าเป็นผู้บุกรุกจะแสดงเครื่องหมายกากบาท ดังรูปที่ 3.25



รูปที่ 3.25 แสดงเครื่องหมายกากบาทเมื่อตรวจพบว่าเป็นผู้บุกรุก

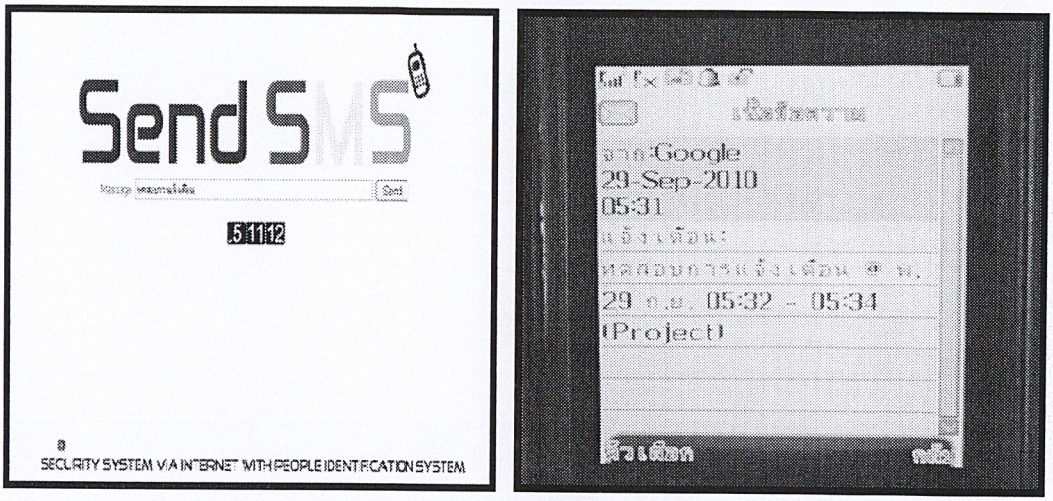
3.3 ส่วนการส่งข้อความแจ้งเตือน



รูปที่ 3.26 แสดงหน้าอินเตอร์เฟสสำหรับการส่งข้อความแจ้งเตือน

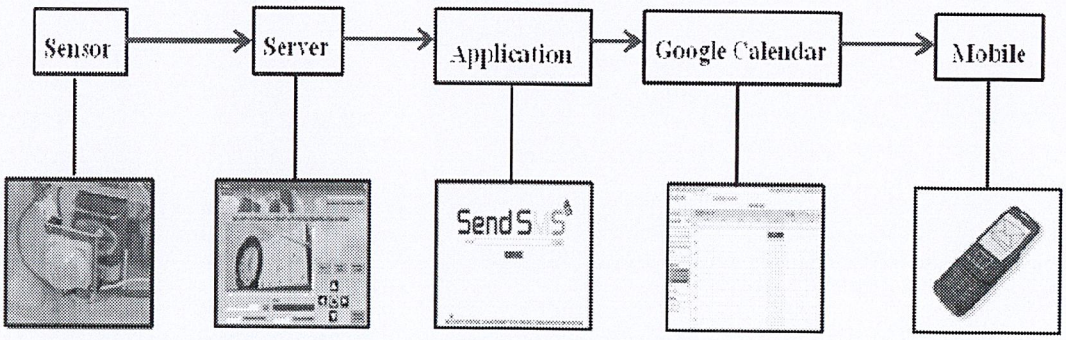
จากรูปที่ 3.26 หน้าจออินเตอร์เฟสเพื่อให้ระบบส่งข้อความแจ้งเตือนโดยการพิมพ์ข้อความลงใน ช่องว่างในส่วนที่ 1 หลังจากนั้นกดปุ่ม Send ข้อความจะถูกส่งไปยัง Google Calendar และ Google Calendar ก็จะส่งข้อความมายังโทรศัพท์มือถืออีกที

Google Calendar คือ ปฏิทินแบบออนไลน์ของ Google ซึ่งเราสามารถเก็บข้อมูลเหตุการณ์ต่างๆ ไม่ว่าจะเป็นการนัดประชุม แจ้งเตือนวันเกิด ซึ่งเราสามามารถกำหนดวัน เวลา เพื่อให้ Google Calendar ส่งข้อความแจ้งเตือนทั้งทาง SMS, E-mail มายังเราได้



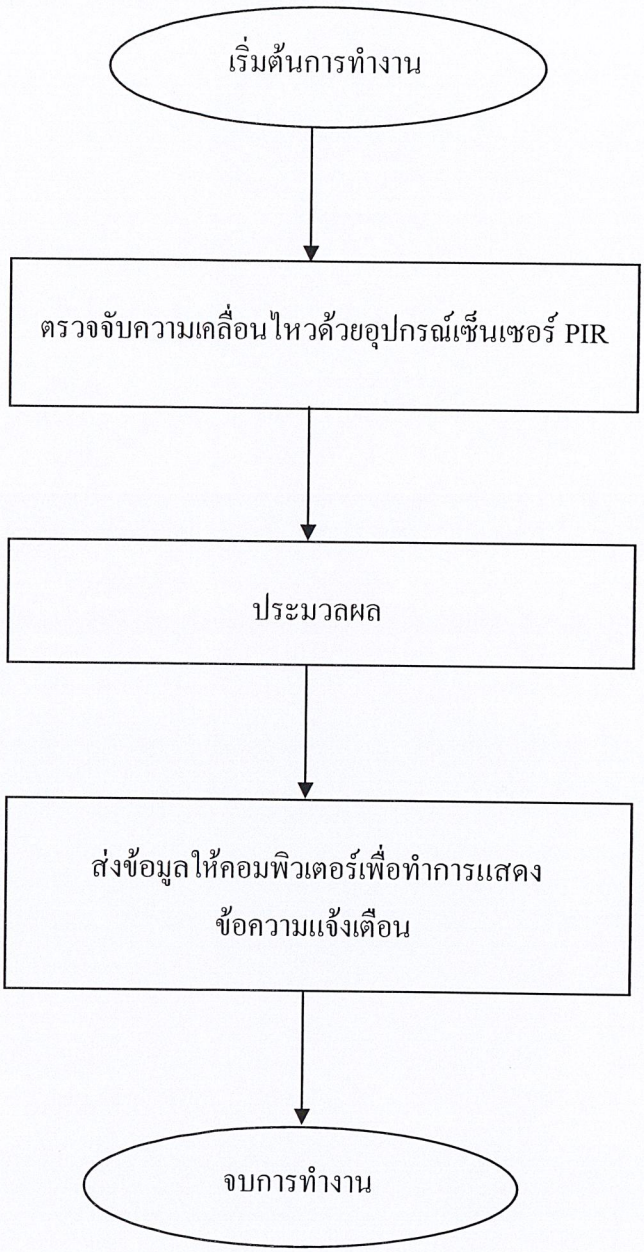
รูปที่ 3.27 แสดงข้อความแจ้งเตือนที่โทรศัพท์มือถือได้รับ

จากรูปที่ 3.27 เมื่อทำการกด Send เพื่อทำการส่งข้อความที่ต้องการแล้ว ระบบก็จะทำการส่งข้อความไปยังโทรศัพท์มือถือ ในเวลาต่อโทรศัพท์มือถือจะได้รับข้อความแจ้งเตือนที่ได้ทำการส่งมา



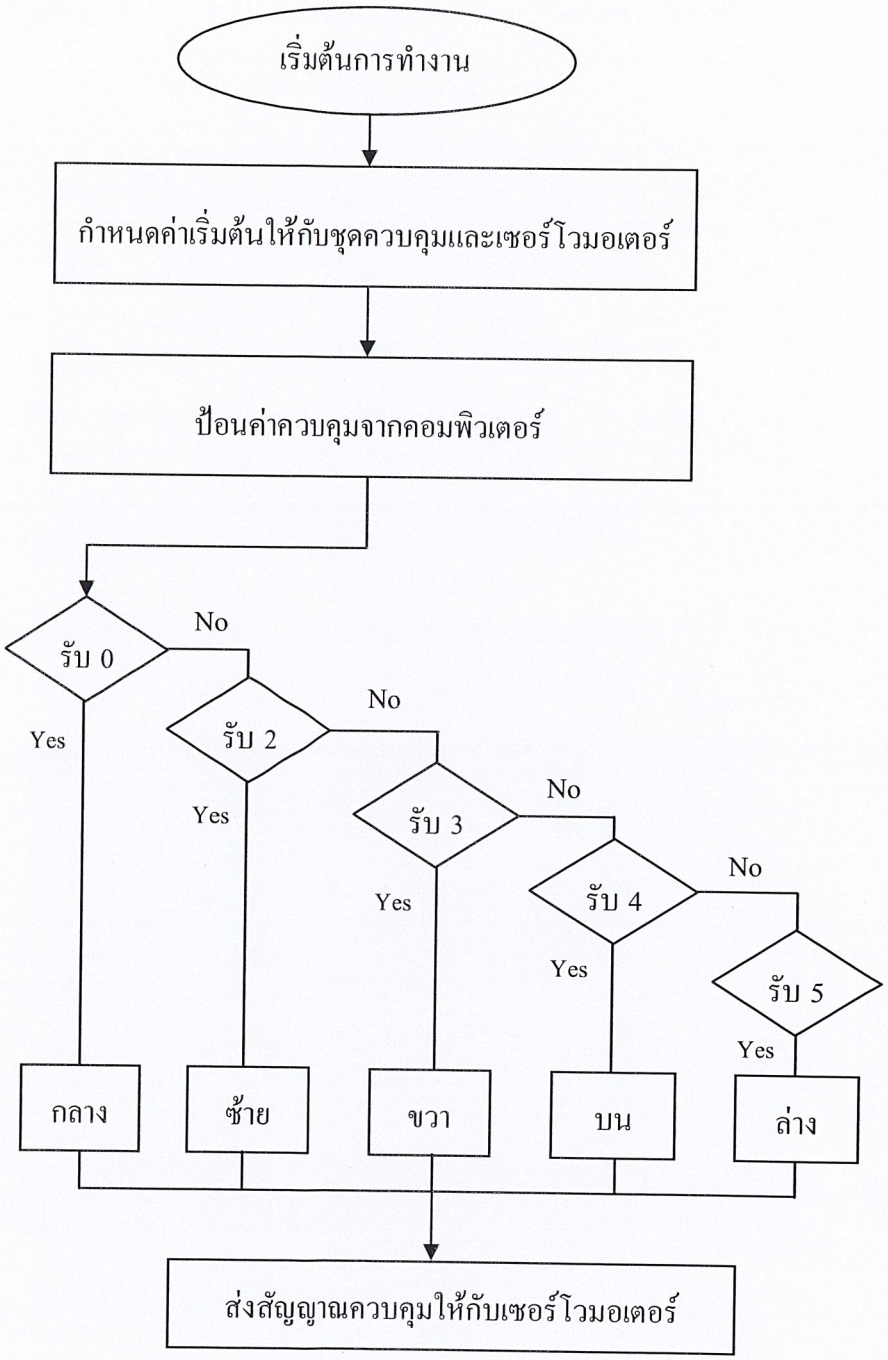
รูปที่ 3.28 แสดงขั้นตอนการส่งข้อความแจ้งเตือนอัตโนมัติ

จากรูปที่ 3.28 แสดงขั้นตอนการส่งข้อความแจ้งเตือนโดยอัตโนมัติ โดยเมื่อเซ็นเซอร์ตรวจพบการเคลื่อนไหวเข้ามาในระบบจะทำการส่งสัญญาณข้อมูลมายังแอพพลิเคชั่นเพื่อทำการแสดงข้อความแจ้งเตือนบนหน้าจอแอพพลิเคชั่น จากนั้นแอพพลิเคชั่นจะทำการเชื่อมต่อไปยังแอพพลิเคชั่นที่ใช้ในการส่งข้อความเพื่อเชื่อมต่อกับ Google Calendar แล้วทำการส่งข้อความต่อไป



รูปที่ 3.29 Flow Chart แสดงขั้นตอนการทำงานของอุปกรณ์เซ็นเซอร์ PIR

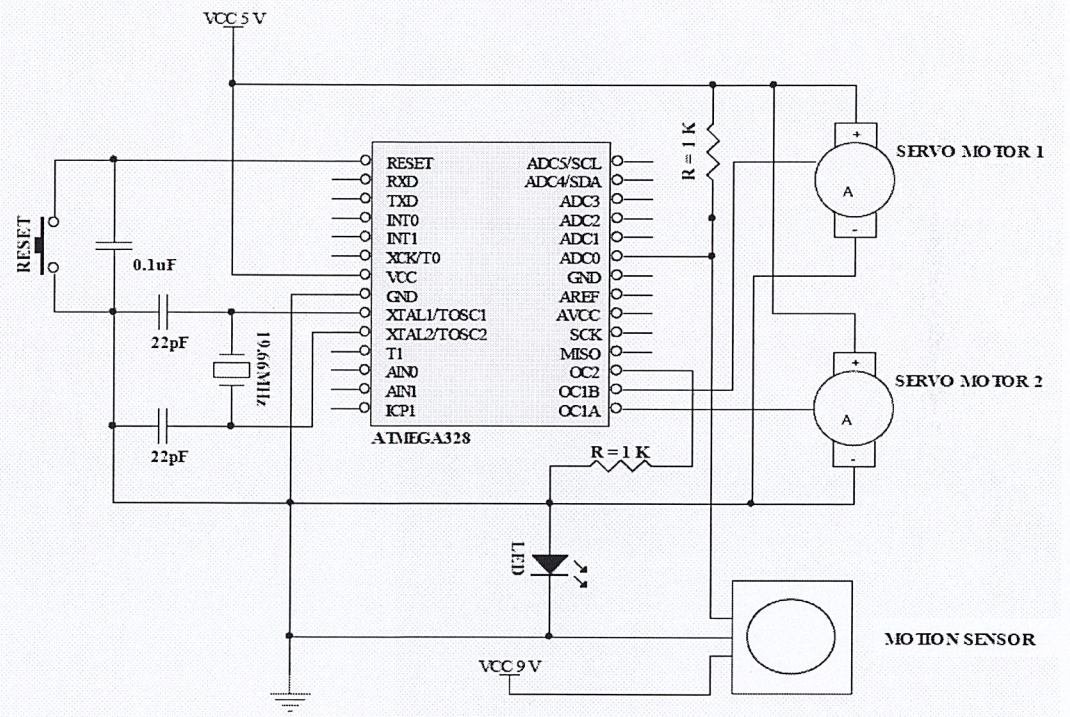
จากรูปที่ 3.29 แสดงขั้นตอนการทำงานของอุปกรณ์เซ็นเซอร์ PIR โดยเมื่อเริ่มต้นการทำงานของอุปกรณ์เซ็นเซอร์นั้น เมื่อเซ็นเซอร์ตรวจจับพบการเคลื่อนไหวแล้ว เซ็นเซอร์จะทำการส่งข้อมูลให้กับไมโครคอนโทรลเลอร์เพื่อทำการประมวลผล จากนั้นไมโครคอนโทรลเลอร์จะทำการส่งค่าไปยังแอพพลิเคชั่น เพื่อให้แอพพลิเคชั่นทำการแจ้งเตือนไปยังผู้ควบคุมผ่านทางข้อความแจ้งเตือนต่อไป



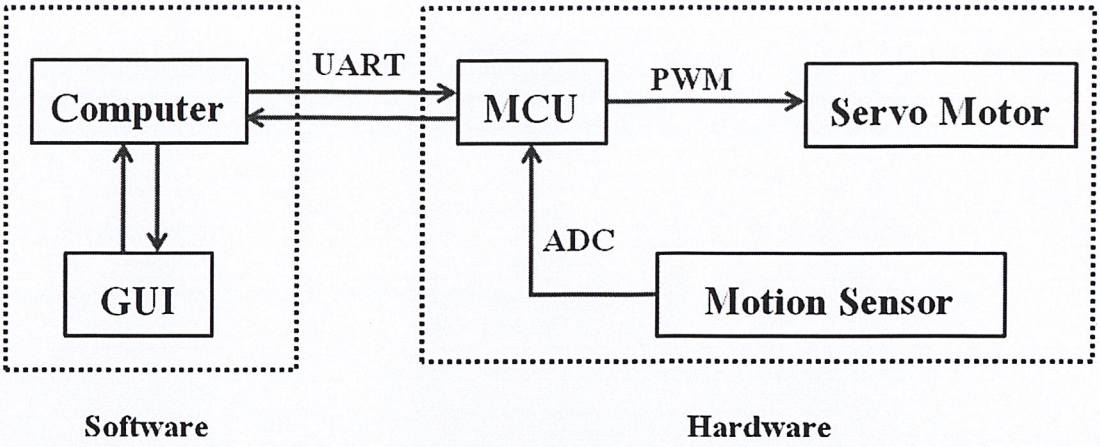
รูปที่ 3.30 Flow Chart แสดงขั้นตอนการทำงานของเซอร์โวมอเตอร์

จากรูปที่ 3.30 แสดงขั้นตอนการทำงานของเซอร์โวมอเตอร์ เมื่อบอร์ดควบคุมเริ่มต้นการทำงานจะทำการกำหนดค่าเริ่มต้นให้กับไมโครคอนโทรลเลอร์เพื่อใช้ในการควบคุมเซอร์โวมอเตอร์ เช่น อัตราบอร์ด เป็นต้น จากนั้นตั้งค่าให้เซอร์โวมอเตอร์ทำการหมุนไปสู่จุดศูนย์กลางเพื่อรอรับการทำงานต่อไป ต่อมาเมื่อผู้ควบคุมทำการกดปุ่มบังคับทิศทางผ่านทางแอพพลิเคชั่นคอมพิวเตอร์จะทำการส่งค่าไปยังบอร์ดควบคุมผ่านทางพอร์ตอนุกรม เพื่อควบคุมให้เซอร์โวมอเตอร์หมุนไปยังทิศทางที่ต้องการคือ ตรงกลาง ซ้าย ขวา บน และล่าง โดยค่าที่คอมพิวเตอร์ทำการส่งไปนั้นคือ 0 2 3 4 5 ตามลำดับ เมื่อบอร์ดควบคุมได้รับค่าที่ส่งมานั้น ก็จะทำการประมวลผลและส่งสัญญาณควบคุมไปยังเซอร์โวมอเตอร์ต่อไป

จากรูปที่ 3.31 และรูปที่ 3.32 แสดงวงจรไฟฟ้าทั้งระบบและ Block Diagram แสดงการทำงานของระบบตามลำดับ



รูปที่ 3.31 แสดงวงจรไฟฟ้าทั้งระบบ



รูปที่ 3.32 Block Diagram แสดงการทำงานของระบบ

3.4 บทสรุป

เนื้อหาในบทนี้จะกล่าวถึงส่วนต่างๆของระบบ ได้แก่ ส่วนของอุปกรณ์ฮาร์ดแวร์ซึ่งประกอบไปด้วย บอร์ดควบคุมการหมุนของเซอร์โวมอเตอร์ เซอร์โวมอเตอร์ ส่วนของฐานกล้อง เป็นต้น และส่วนถัดไปคือส่วนของซอฟต์แวร์ ในส่วนนี้จะประกอบไปด้วย แอพพลิเคชั่นในฝั่งเซิร์ฟเวอร์และแอพพลิเคชั่นในฝั่งไคลเอนต์ ซึ่งจะแสดงการทำงานของแอพพลิเคชั่นในส่วนต่างๆ และส่วนสุดท้ายคือส่วนของการส่งข้อความแจ้งเตือน

บทที่ 4

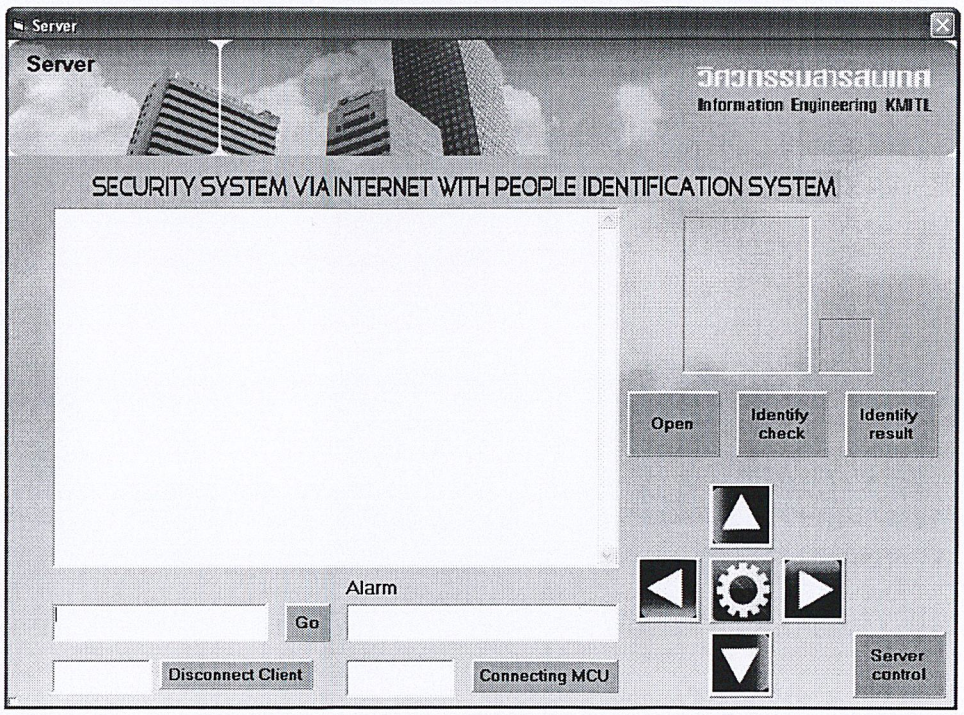
ผลการทดลอง

4.1 ขั้นตอนการทดลอง แบ่งออกเป็น 2 ส่วน คือ

4.1.1 ส่วนการควบคุมอุปกรณ์ผ่านทางเครือข่ายอินเตอร์เน็ต

เมื่อผู้ใช้ต้องการควบคุมกล้องเว็บแคมผ่านเครือข่ายสามารถทำโดยการเรียกผ่านโปรแกรมแอพลิเคชันซึ่งแบ่งออกเป็น 2 ส่วน คือ เซิร์ฟเวอร์ และ ไคลเอนต์

4.1.1.1 โปรแกรมแอพพลิชันส่วนเซิร์ฟเวอร์



รูปที่ 4.1 แสดงหน้าจอแอพพลิเคชั่นฝั่งเซิร์ฟเวอร์

จากรูปที่ 4.1 แสดงหน้าจอแอพพลิเคชั่นในฝั่ง เซิร์ฟเวอร์ เมื่อผู้ควบคุมทำการเรียกโปรแกรมขึ้นมาใช้งานโดยประกอบไปด้วยหน้าจอแสดงผล และปุ่มควบคุมต่างๆ โดยปุ่มสั่งการไปยัง เซอร์โวมอเตอร์เพื่อทำการควบคุมการหมุนของกล้องผ่านทาง Serial Port มีดังนี้

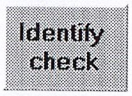
คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนไปทางขวาครั้งละ 1 องศา

คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนไปทางซ้ายครั้งละ 1 องศา

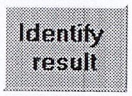
คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนลงล่างครั้งละ 1 องศา

คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนขึ้นบนครั้งละ 1 องศา

คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนเข้าสู่ตำแหน่งจุดศูนย์กลาง



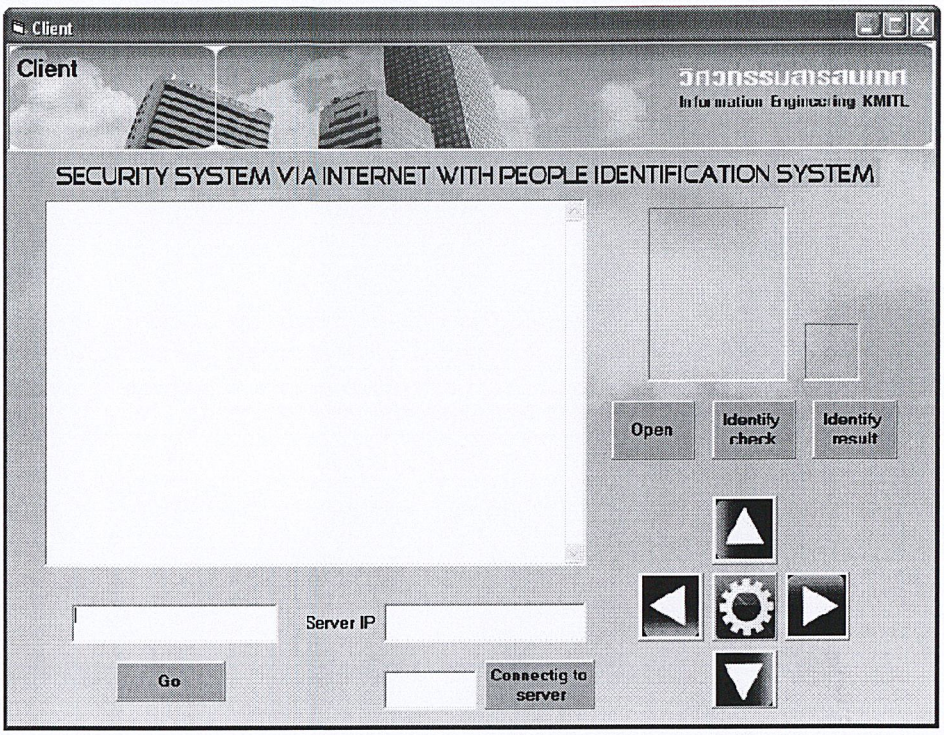
คือ ปุ่มคำสั่งเพื่อใช้ในการตรวจสอบบุคคลที่กล้องจับภาพได้ โดยจะตรวจสอบกับภายในฐานข้อมูล



คือ ปุ่มคำสั่งเพื่อแสดงผลการตรวจสอบ

คือ ปุ่มคำสั่งเปิดภาพถ่ายที่ได้ทำการบันทึกไว้ก่อนหน้านี้

4.1.1.2 โปรแกรมแอพพลิชันส่วนไคลเอนต์



รูปที่ 4.2 แสดงหน้าจอแอพพลิเคชั่นฝั่งไคลเอนต์

จากรูปที่ 4.2 แสดงหน้าจอแอพพลิเคชั่นในฝั่งไคลเอนต์ เมื่อผู้ควบคุมทำการเรียกเปิดโปรแกรมขึ้นมาโดยรายละเอียดของปุ่มสั่งการไปยังเซอร์โวมอเตอร์เพื่อทำการควบคุมการหมุนของกล้องผ่านอินเตอร์เน็ต มีดังนี้

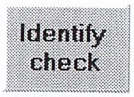

คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนไปทางขวาครั้งละ 1 องศา


คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนไปทางซ้ายครั้งละ 1 องศา

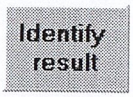

คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนลงล่างครั้งละ 1 องศา


คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนขึ้นบนครั้งละ 1 องศา


คือ ปุ่มคำสั่งในการสั่งการให้เซอร์โวมอเตอร์หมุนเข้าสู่ตำแหน่งจุดศูนย์กลาง



คือ ปุ่มคำสั่งเพื่อใช้ในการตรวจสอบบุคคลที่กล้องจับภาพได้ โดยจะตรวจสอบกับภายในฐานข้อมูล



คือ ปุ่มคำสั่งเพื่อแสดงผลการตรวจสอบ

คือ ปุ่มคำสั่งเปิดภาพถ่ายที่ได้ทำการบันทึกไว้ก่อนหน้านี้

กรณีมีผู้ควบคุม

ผู้ใช้งานสามารถกดปุ่มควบคุมฐานกล้องให้หมุนไปทางซ้าย-ขวา และขึ้น-ลงได้ ปุ่มใช้งานสำหรับใช้ตรวจสอบภาพบุคคลต้องสงสัยแล้วแสดงผลออกมาเป็นภาพเครื่องหมายถูก ในกรณีที่ตรงกับภาพในฐานข้อมูล และแสดงผลออกเป็นภาพเครื่องหมายผิด ในกรณีที่ไม่ตรงกับภาพในฐานข้อมูล เมื่อ Motion Sensor ตรวจจับความเคลื่อนไหวได้ Motion Sensor จะส่งข้อมูลมาให้กับโปรแกรมแอพพลิเคชั่น แสดงเป็นข้อความว่า Stranger is coming!!!!

กรณีไม่มีผู้ควบคุม

Motion Sensor จะทำหน้าที่ตรวจจับความเคลื่อนไหว เมื่อมีการเคลื่อนไหวเกิดขึ้นแล้ว Motion Sensor จะส่งค่าให้กับโปรแกรมแอพพลิเคชั่นแล้วบันทึกภาพแล้วนำภาพที่บันทึกไว้ไปทำการตรวจสอบเพื่อยืนยันว่าใช้บุคคลในฐานข้อมูลหรือไม่ ถ้าผลออกมาว่า ไม่ใช่ จะดำเนินการส่งข้อความแจ้งเตือน SMS ไปยังผู้ทำหน้าที่ดูแลอยู่ เพื่อแจ้งเตือนให้ทราบ และดำเนินการควบคุมกล้องผ่านทางเครือข่ายอินเตอร์เน็ต เพื่อที่จะดูสถานการณ์ภายในห้องนั้นได้ทันท่วงที

4.1.2 ส่วนของการประมวลผลภาพเพื่อระบุตัวบุคคล

4.1.2.1 การทดลองระบุบุคคลโดยใช้ภาพใบหน้าที่มีลักษณะต่างๆที่มีความคล้ายคลึงกับภาพในฐานข้อมูล

วิธีการทดลอง

จากการเก็บข้อมูลภาพบุคคลลงในฐานข้อมูล หลายๆมุมมอง เพื่อนำมาเปรียบเทียบกับภาพใหม่จะใช้เพื่อทดสอบการระบุตัวตน โดยเป็นภาพที่ถ่ายคนละครั้ง ที่มีความแตกต่างเพียงเล็กน้อยจำนวน 25 ครั้ง เพื่อนำไปหาเปอร์เซ็นต์ความผิดพลาดโดนในที่นี้ จะทำการทดลองทั้งหมด 5 ครั้งจะแบ่งออกเป็น 5 รูปแบบคือ

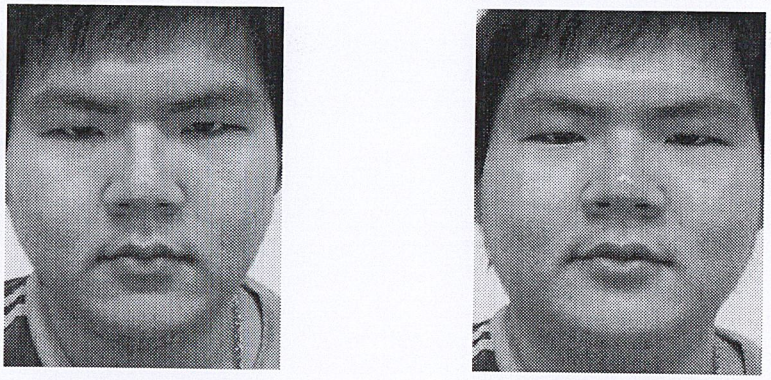
เมื่อทดสอบกับภาพใบหน้าตรง

ผลการทดลอง

ตารางที่ 4.1 แสดงผลการทดลองการระบุบุคคลโดยใช้ภาพหน้าตรงที่ต่างจากภาพในฐานข้อมูล

ครั้งที่	จำนวนภาพที่ทดลอง	จำนวนภาพที่ระบุบุคคลได้ถูกต้อง	ความถูกต้อง (%)	ความถูกต้องเฉลี่ย (%)
1	25	20	72	
2	25	19	76	
3	25	17	68	73
4	25	18	73	
5	25	19	76	

จากผลการทดลอง จะเห็นได้ว่า เมื่อนำภาพหน้าตรงที่ต่างจากภาพในฐานข้อมูลมาทดสอบการระบุตัวบุคคลนั้นจะสามารถระบุได้ค่อนข้างดี แต่สภาวะแวดล้อมของภาพต้องไม่แตกต่างไปจากภาพในฐานข้อมูลมากนัก ซึ่งค่าไอเกนวาลูร์ (Eigenvalue) ของภาพจะเปลี่ยนไปจากเดิมเล็กน้อย จึงสามารถระบุตัวบุคคลได้ถูกต้อง ภาพตัวอย่างที่นำมาทดสอบแล้วสามารถระบุได้ถูกต้องจะแสดงดังรูปที่ 4.3



(ก) ภาพหน้าตรงที่นำมา (ข) ภาพในฐานข้อมูล

รูปที่ 4.3 ภาพตัวอย่างของใบหน้าตรงที่นำมาทดสอบแล้วสามารถระบุตัวบุคคลได้ถูกต้อง

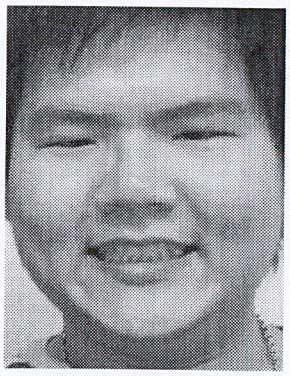
เมื่อทดสอบกับภาพใบหน้ายิ้ม

ผลการทดลอง

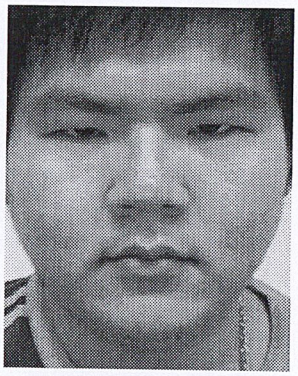
ตารางที่ 4.2 แสดงผลการทดลองการระบุบุคคลโดยใช้ภาพใบหน้ายิ้ม

ครั้งที่	จำนวนภาพที่ทดลอง	จำนวนภาพที่ระบุบุคคลได้ถูกต้อง	ความถูกต้อง (%)	ความถูกต้องเฉลี่ย (%)
1	25	17	68	
2	25	18	72	
3	25	17	68	67.2
4	25	17	68	
5	25	15	60	

จากผลการทดลอง จะเห็นได้ว่า เมื่อนำภาพใบหน้ายิ้มมาทดสอบ การระบุตัวบุคคลนั้นจะสามารถระบุได้ค่อนข้างดี แต่ต้องเป็นใบหน้าตรง และขึ้นกับลักษณะที่ยิ้มด้วย สภาวะแวดล้อมของภาพต้องไม่แตกต่างไปจากภาพในฐานข้อมูลมากนัก ซึ่งค่าไอแกนวาลูร์ (Eigenvalue) ของภาพจะเปลี่ยนไปจากเดิมเล็กน้อย จึงสามารถระบุตัวบุคคลได้ถูกต้อง ภาพตัวอย่างที่นำมาทดสอบแล้วสามารถระบุได้ถูกต้องจะแสดงดังรูปที่ 4.4



(ก) ภาพหน้ายิ้มที่นำมาทดสอบ



(ข) ภาพในฐานข้อมูล

รูปที่ 4.4 ภาพตัวอย่างของใบหน้ายิ้มที่นำมาทดสอบแล้วสามารถระบุตัวบุคคลได้ถูกต้อง

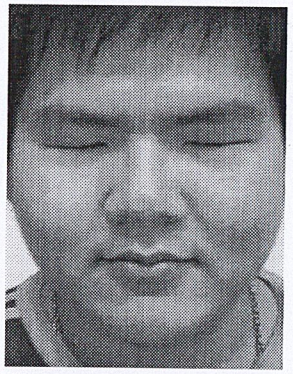
เมื่อทดสอบกับภาพใบหน้าหลับตา

ผลการทดลอง

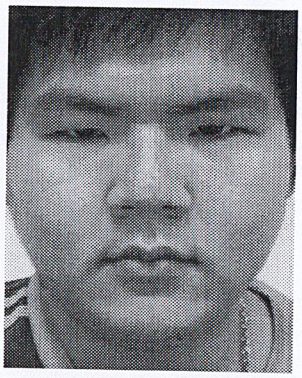
ตารางที่ 4.3 แสดงผลการทดลองการระบุตัวบุคคลโดยใช้ภาพหลับตา

ครั้งที่	จำนวนภาพที่ทดลอง	จำนวนภาพที่ระบุบุคคลได้ถูกต้อง	ความถูกต้อง (%)	ความถูกต้องเฉลี่ย (%)
1	25	19	76	
2	25	18	72	
3	25	17	68	72.8
4	25	19	76	
5	25	18	72	

จากผลการทดลอง จะเห็นได้ว่า เมื่อนำภาพใบหน้าหลับตามาทดสอบ การระบุตัวบุคคลนั้นจะสามารถระบุได้ค่อนข้างดี แต่ต้องเป็นใบหน้าตรง สภาวะแวดล้อมของภาพต้องไม่แตกต่างไปจากภาพในฐานข้อมูลมากนัก ซึ่งค่าไอแกนวาลูร์ (Eigenvalue) ของภาพจะเปลี่ยนไปจากเดิมเล็กน้อย จึงสามารถระบุตัวบุคคลได้ถูกต้อง ภาพตัวอย่างที่นำมาทดสอบแล้วสามารถระบุได้ถูกต้องจะแสดงดังรูปที่ 4.5



(ก) ภาพหลับตาที่นำมาทดสอบ



(ข) ภาพในฐานข้อมูล

รูปที่ 4.5 ภาพตัวอย่างของใบหน้าหลับตาที่นำมาทดสอบแล้วสามารถระบุตัวบุคคลได้ถูกต้อง

4.2 บทสรุป

จากการทดลองซึ่งแยกออกเป็นสองกรณี ประกอบไปด้วย กรณีที่มีผู้ควบคุม กับกรณีที่ไม่มีผู้ควบคุม ผลที่ได้รับคือในกรณีที่มีผู้ควบคุม ผู้ควบคุมสามารถที่จะควบคุมกล้องเว็บแคมให้หมุนไปยังทิศทางต่างๆได้ และในกรณีที่ไม่มีผู้ควบคุมแอพพลิเคชั่นก็สามารถที่จะส่งข้อความแจ้งเตือนไปยังผู้ควบคุมเมื่อเซ็นเซอร์ตรวจพบผู้บุกรุกเข้ามาในระบบ พร้อมทั้งในส่วนการประมวลผลภาพก็สามารถที่จะทำการตรวจสอบรูปภาพที่ต้องการว่าเป็นผู้ที่อยู่ในฐานข้อมูลหรือเป็นผู้บุกรุกได้

บทที่ 5

บทสรุปและวิจารณ์

5.1 สรุปผลการดำเนินงาน

ปริญญานิพนธ์นี้เกี่ยวกับระบบรักษาความปลอดภัย ที่สามารถป้องกันภัยจากผู้บุกรุกและเพื่อป้องกันเหตุการณ์ที่ไม่คาดฝัน เกิดขึ้นแล้วสามารถป้องกันได้ทันที โดยการตรวจสอบการบุกรุกผ่านทางคอมพิวเตอร์ และทำการติดตั้งกล้องไว้ที่สถานที่ที่ต้องการตรวจสอบ จึงทำให้สามารถเข้าตรวจสอบสถานที่นั้นได้ตลอดเวลา พร้อมทั้งมีการระบุตัวบุคคลของผู้ที่สามารถเข้าถึงสถานที่นั้นๆได้ จากการทดสอบระบบทั้งหมดการแบ่งออกได้เป็น 2 ส่วนหลักๆ ดังนี้

ส่วนของการแจ้งเตือนข้อความ (SMS) โดยใช้ Motion Sensor เป็นตัวตรวจจับความเคลื่อนไหว เมื่อตรวจพบว่ามีบุคคลเคลื่อนไหวเกิดขึ้น Motion Sensor จะสั่งให้ระบบทำการบันทึกภาพแล้วตรวจสอบภาพที่บันทึกไว้เพื่อยืนยันระบุตัวบุคคล ถ้าไม่ใช่ภาพบุคคลในฐานข้อมูล ระบบจะทำการส่งข้อความแจ้งเตือน (SMS) ผ่านทาง Google Calendar เพื่อแจ้งผู้ที่ดูแลรับทราบ ว่าขณะนี้มีบุคคลต้องสงสัยบุกรุก

ส่วนของการควบคุมกล้อง เพื่อให้สามารถเลื่อนดูภาพและบันทึกภาพ ซึ่งในการควบคุมฐานกล้องนั้นจะใช้บอร์ดไมโครคอนโทรลเลอร์เชื่อมต่อกับเซอร์โวมอเตอร์เพื่อใช้บอร์ดส่งค่าให้กับเซอร์โวมอเตอร์ ซึ่งสามารถควบคุมฐานกล้องโดยตรง และสามารถควบคุมผ่านทางอินเตอร์เน็ตได้

5.2 ปัญหาที่พบและแนวทางแก้ไขในการพัฒนาโครงงาน

5.2.1 ปัญหาที่พบ

ในส่วนของการทำงาน ด้านการประมวลผลภาพเพื่อระบุตัวบุคคลนั้น ปัญหาหลักๆนั้นจะเป็นปัญหาเกี่ยวกับความไม่ชำนาญในด้านคำสั่งที่ใช้เขียนการประมวลผล และส่วนของการนำแอพพลิเคชั่นที่พัฒนาขึ้นมานั้นให้สามารถติดต่อควบคุมผ่านเครือข่ายอินเตอร์เน็ตได้ ก็พบว่าปัญญาที่เกิดขึ้นในการทำคือ ไม่มีความรู้และความชำนาญในการทำ เนื่องด้วยโครงงานประกอบ

ไปด้วยงานหลายส่วนพร้อมทั้งเรื่องของระยะเวลา แต่โครงงานชิ้นนี้ก็สำเร็จลุล่วงไปได้แต่ก็ยังสามารถนำไปดำเนินการพัฒนาต่อให้สมบูรณ์ในอนาคตข้างหน้าต่อไปได้

5.2.2 แนวทางแก้ไข

- ปรึกษาผู้รู้สอบถามหาแนวทางแก้ไข แล้วนำคำตอบที่ได้มา ไปแก้ไขปัญหาที่เกิดขึ้น
- แบ่งงานออกเป็นส่วนๆ แล้วแบ่งกันรับผิดชอบในแต่ละส่วน เพื่อที่เมื่อเกิดปัญหาในส่วนใดส่วนหนึ่ง งานส่วนอื่นก็ยังดำเนินต่อไป

5.3 แนวทางการพัฒนาโครงงานในอนาคต

โครงงานชิ้นนี้ เป็นโครงงานที่มีการวางแผนของระบบมาดีในระดับหนึ่งแต่ก็ยังมี ข้อด้อยในหลายๆประการ ซึ่งควรที่จะนำไปศึกษาต่อและพัฒนาต่อ เช่น การประมวลผลภาพแบบ real-time ก็คือ สามารถที่จะประมวลผลภาพได้ในขณะที่กล้องกำลังจับภาพอยู่ในเวลานั้นๆได้ และการพัฒนาแอพพลิเคชั่นเพื่อให้รองรับระบบปฏิบัติการอื่นๆ เช่น ระบบปฏิบัติการของมือถือ IOS, Android เป็นต้น

บรรณานุกรม

[1] วัชรินทร์ เดารพ, คู่มือการใช้ servo moter, กรุงเทพฯ: อีทีที จำกัด, 2546

[2] อดิศักดิ์ ชิณะวงศ์, Microcontroller[Online].Availabel: http://www.adisak51.com/page21.html

[3] เริ่มต้น AVR Microcontroller [Online].Availabel : http://www.technicnan.ac.th/nan_ntc/adisak51/avr2.html

[4] บทความ AVR Studio กับ Atmega1281[Online] http://cid-c0a6064779796550.office.live.com/browse.aspx/.Public

[5] อภิชาต ภู่พลับ, เริ่มต้นเขียนโปรแกรมติดต่อ และควบคุมฮาร์ดแวร์ด้วย Visual Basic, นนทบุรี, : อินโฟเพรส, 2546

[6] http://www.ce.kmitl.ac.th/download.php?DOWNLOAD_ID=93&database=subject_download [Online]

[7] วุฒิพร ฉลวยศร และคนอื่นๆ, การควบคุมอุปกรณ์ไฟฟ้าผ่านอินเตอร์เน็ต. ปริญญานิพนธ์ วศ.บ กรุงเทพฯ : สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2548

[8] http://web.agri.cmu.ac.th/extens/Course_all/Course/352792/PDF/520831106.pdf [Online]

[9] http://stks.or.th/wiki/doku.php?id=graphics:vector-bitmap [Online]

[10] http://www.cs.su.ac.th/~tasanawa/510670/DIPandCV.pdf [Online]

[11] สันติสุข ช่างนาค และคนอื่นๆ, ระบบรักษาความปลอดภัยภายในบ้านแบบออนไลน์. ปริญญานิพนธ์ วศ.บ กรุงเทพฯ : สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2552

[12] ประจิน พลังสันติกุล, การเขียนโปรแกรมควบคุมไมโครคอนโทรลเลอร์ AVR ด้วยภาษา C กับ Win AVR (C Compiler), กรุงเทพฯ: บริษัท แอพซอฟต์เทค จำกัด

[13] สุทธิพล พันธุธาดาพร และคนอื่นๆ, ระบบควบคุมกล้องวิดีโอผ่านอินเตอร์เน็ต. ปริญญานิพนธ์ วศ.บ กรุงเทพฯ : สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2542