การสร้างเครื่องกำเนิดค่าสุ่มจริงโดยใช้สัญญาณอลวน

Construction of True Random Number Generator Using Chaotic Signal

ได้รับทุนสนับสนุนงานวิจัยจากงบประมาณเงินรายได้คณะวิศวกรรมศาสตร์
ประจำปี 2553 จำนวนเงิน 59,000 บาท
ระยะเวลาทำงานวิจัยตั้งแต่ 1 ตุลาคม 2552 - 30 กรกฎาคม 2553

ผู้วิจัย ผศ.กฤดากร กล่อมการ
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

บทคัดย่อ

งานวิจัยเสนอการสร้างค่าสุ่มจริงจากสัญญาณอลวน โดยงานวิจัยเสนอการสร้างสัญญาณอลวนรูปแบบใหม่ที่ไม่เคยปรากฏมาก่อนคือรูปผีเสื้อหลายปีก รูปหลุมวน 4 ขนาดสกอร์ รูปแบบอลวนแบบผสม 2 รูปแบบ จากนั้นจึงนำสัญญาณอลวนที่ค้นพบทำการผ่านขบวนการกรองค่าเพื่อให้ได้เป็นค่าสุ่มโดยค่าที่ได้สามารถผ่านการทดสอบทางสถิติเพื่อใช้งานจริงได้

Abstract

The construction of truely random numbers generator from chaotic attractor presented in this report. In this report, the four of new attractor such as a multi-wing butterfly attractor, four scrolls attractor, and two mixed mode chaotic attractor have been discovered. The random number which extracted form each attractor passed standard test suited for grantee the random number can be used in practically.

บทที่ 1

แนวคิดและที่มาของปัญหา

ค่าสุ่มจริงเป็นค่าที่เกิดขึ้นโดยไม่สามารถทำนายได้ มีประโยชน์สำหรับการจำลองทางสถิติ,การทดสอบวงจรอิเลคทรอนิคส์ การออกฉลากกินแบ่ง, การใช้สำหรับขบวนการเข้ารหัสลับ โดยเป็นที่ทราบกันดีว่าหลังจากการบังคับใช้กฎหมายอาญากรรมคอมพิวเตอร์ พ.ศ. 2550 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้กำหนดแผ่นแม่บท สำหรับการรักษาความมั่นคงปลอดภัยข่าวสารขององค์กรในด้านต่างๆ ซึ่งวิธีการสร้างความมั่นคงปลอดภัยข่าวสารส่วนใหญ่จะอยู่บนพื้นฐานของประยุกต์การเข้ารหัสลับ ซึ่งต้องอาศัยค่าสุ่มจริงเป็นอุปกรณ์พื้นฐานหรือ primitive tool ในขบวนการเช่น การสร้างค่าสุ่มสำหรับเป็นค่าเริ่มต้นของการเข้ารหัสลับแบบ Block ใน mode แบบ CBC, ค่าสุ่มสำหรับการสร้าง password, การสร้างกุญแจในการเข้ารหัส, การ PAD ลงใน Block ข้อมูล, การสร้างค่าสุ่มของ protocol สำหรับการพิสูจน์ตน โดยในการพัฒนาระบบสร้างความมั่นคงปลอดภัยข่าวสารขึ้นนั้น จำเป็นอย่างยิ่งที่ต้องมีอุปกรณ์สร้างค่าสุ่มจริงเสมอ ซึ่งค่าที่สร้างขึ้นนี้จะต้องมีเป็นค่าที่คาดเดาหรือทำนายไม่ได้(unpredictable) เพราะสามารถทำการคาดเดาได้แล้วขบวนการสร้างความมั่นคงข่าวสารอาจล้มเหลวโดยสิ้นเชิง

ดังนั้นอุปกรณ์สร้างค่าสุ่มจริงที่ออกแบบให้ทำงานร่วมกับระบบความมั่นคงข่าวสาร จึงต้องมีความน่าเชื่อถือสูง ทำให้ผลิตภัณฑ์ที่จำหน่ายมีราคาสูงพร้อมกับผลิตภัณฑ์มีการปกป้องการลอกเลียนด้วยสิทธิบัตรการสร้างด้วยเช่นกัน สำหรับงานวิจัยนี้เสนอวิธีการสร้างอุปกรณ์กำเนิดค่าสุ่มจริงโดยใช้สัญญาณอลวนซึ่งผู้วิจัยได้มีประสบการณ์ในการสร้างขึ้นมาในรูปแบบต่างๆ โดยคุณสมบัติที่เด่นชัดของสัญญาณก็คือมีลักษณะคล้ายสัญญาณสุ่ม (Random like) และเนื่องการสร้างสัญญาณสุ่มจริงขึ้นจากสัญญาณอลวน ยังมีสิทธิบัตรคลอบคลุมอยู่น้อยชิ้น ดังนั้นนอกจากที่สามารถพัฒนาเทคโนโลยีหลัก สำหรับการรักษาความมั่นคงข่าวสารแล้ว ความรู้จากงานวิจัยยังสามารถที่จะสร้างสิทธิบัตรของอุปกรณ์สร้างค่าสุ่มจริงรวมทั้งเป็นต้นแบบเพื่อผลิตในเชิงพาณิชย์อีกด้วย

1.1 วัตถุประสงค์ของโครงการวิจัย

1.1สร้างองค์ความรู้การสร้างค่าสุ่มจริงจากสัญญาณอลวน

1.2 สร้างเครื่องต้นแบบเครื่องกำเนิดค่าสุ่มจริงด้วยสัญญาณอลวนที่ผ่านการทดสอบคุณสมบัติทางสถิติเพื่อใช้งานจริง

1.2 ขอบเขตของโครงการวิจัย

สร้างเครื่องต้นแบบของการกำเนิดค่าสุ่มจริงด้วยสัญญาณอลวนแบบใหม่ที่ผ่านการทดสอบทางสถิติที่สามารถต่อใช้งานร่วมกับคอมพิวเตอร์โดยผ่านพอร์ตอนุกรมหรือพอร์ต USB ภายในเครื่องกำเนิดค่าสุ่มจริงประกอบด้วย

1.2.1 ส่วนสร้างสัญญาณจากวงจรสร้างสัญญาณอลวน

1.2.2 ส่วนแยกสัญญาณสุ่มออกจากสัญญาณอลวน

1.2.3 ส่วนเชื่อมต่อกับคอมพิวเตอร์

1.3 ขอบเขตของงานวิจัย

1.3.1 ทำการออกแบบวงจรกำเนิดสัญญาณอลวน

1.3.2 ทำการสร้างวงจรกำเนิดค่า Truly random number ในรูปแบบต่าง ๆ

1.3.3 จำลองและแสดงคุณสมบัติของวงจรกำเนิดค่า Truly random number

1.3.4 นำไปทดสอบเพื่อให้เป็นไปตามมาตรฐาน FIPS 140-1

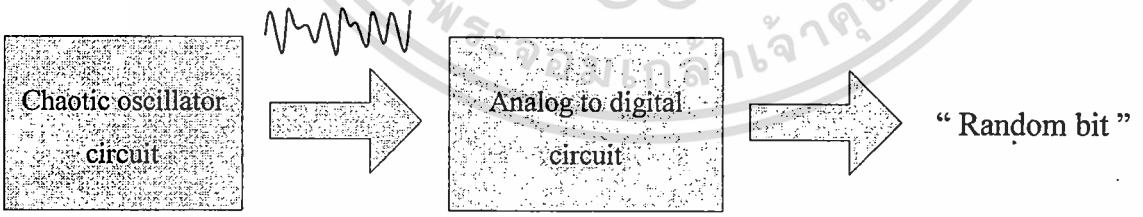
1.4 ผลที่คาดว่าจะได้รับ

1.4.1 สามารถนำวงจรที่ได้ผ่านการทดสอบแล้ว ไปประยุกต์ใช้แทนวงจร หรือ อัลกอลิทึมที่สร้างค่าแรนดัม แบบเดิมได้

1.4.2 สามารถสร้างวงจรกำเนิดค่า Truly random number ได้ในหลาย ๆรูปแบบ

1.4.3 ทราบวงจรกำเนิดค่า Truly random number ที่ได้ผลลัพธ์ที่ดีที่สุด

1.5 ภาพโดยรวมของงานวิจัย



รูปที่ 1-1 Block Diagram แสดงโครงสร้างการทำงานทั้งหมดในงานวิจัยอย่างคร่าว ๆ

1.5.1 Chaotic oscillator circuit เป็นส่วนในการสร้างวงจรเพื่อสร้างสัญญาณอลวนหลาย ๆ รูปแบบเพื่อหาวงจรที่ดีที่สุดที่เมื่อแปลงค่าจากอนาล็อกเป็นดิจิตอลทำให้เกิด ค่าแรนดัมจริง

1.5.2 Analog to digital circuit เป็นส่วนในการแปลงจากสัญญาณ Chaotic ซึ่งเป็นสัญญาณอนาล็อกให้เป็นสัญญาณดิจิตอลเพื่อทำการทดสอบให้ผ่านตามมาตรฐาน FIPS 140

บทที่ 2
ทฤษฎีและหลักการที่ใช้ในงานวิจัย

การประยุกต์ทฤษฎีอลวนกับงานวิศวกรรม

2.1 ทฤษฎีอลวน

เป็นปรากฏการณ์ที่เกิดจากระบบพลวัตแบบไม่เป็นเชิงเส้น(Nonlinear Dynamics System) เข้าใจง่ายๆ หมายถึงระบบแปรค่าตามเวลาแต่ไม่เป็นเชิงเส้นคือ โดยระบบเชิงเส้นนั้น เมื่อเราให้อินพุตเข้า 1 ค่าจะได้เอาท์พุทเป็นจำนวนมากกว่าหรือน้อยกว่าเป็น n เท่าแต่ระบบที่ไม่เป็นเชิงเส้นนั้นค่าอินพุทจะไม่แปรผกผันตรงกับค่าอินพุทแต่จะแปรตามฟังก์ชัน คณิตศาสตร์ที่ แบบง่ายๆ จนไปถึงแบบที่ซับซ้อน ซึ่งค้นพบโดยบังเอิญโดย ศาสตรจารย์ Edward N. Lorenz นักอุตินิยมวิทยาแห่งสถาบันเทคโนโลยีแห่งรัฐแมซซาซูเซท ในปี พ.ศ. 2506 โดยเวลานั้น Lorenz ได้พยายามสร้างแบบจำลองทางอุตุนิยมวิทยาด้วยสมการอนุพันธ์แบบไม่เป็นเชิงเส้นขนาดลำดับ 3 ตัว x, y, z ของความสัมพันธ์ระหว่าง อุณหภูมิ ความกดอากาศ ความเร็วลม และให้ประมวลผลบนคอมพิวเตอร์โดยเริ่มประมวณผลด้วยทศนิยม 6 หลัก แต่เนื่องจากขณะนั้นคอมพิวเตอร์มีประสิทธิภาพต่ำ Lorenz จึงได้ลดหลักทศนิยมของค่าเริ่มต้นของการคำนวณด้วยเลขทศนิยมจาก 6 หลักเหลือ 3 หลัก โดยคิดว่าเลขทศนิยมที่ตัดทิ้งจะไม่มีนัยสำคัญแต่ผลของการคำนวณ แต่เมื่อเวลาผ่านไปช่วงเวลาหนึ่งพบว่าผลของการคำนวณด้วยค่าเริ่มต้นด้วยทศนิยม 3 หลัก ได้เปลี่ยนแปลงจากการคำนวณครั้งก่อนไปอย่างมากมายหรือเพียงกำหนดค่าเริ่มต้นต่างกันเล็กน้อยผลของสมการอนุพันธ์ ที่ Lorenz จำลองขึ้นนี้จะให้ผลแตกต่างกันอย่างสิ้นเชิง กล่าวได้ว่าระบบที่จำลองขึ้นนี้ไวต่อค่าเริ่มต้นและเมื่อทำการพล็อต ความสัมพันธ์ระหว่างตัวแปร x ต่อ y และx ต่อ z จะมีลักษณะรูปร่างที่แปลกประหลาดมีลักษณะเป็นหลุมวน(attractor)โดยภายหลังมีผู้เรียกว่าหลุมวนแบบ Lorenz และ Lorenz เรียกปรากฏการณ์ที่ค้นพบโดยบังเอิญนี้ว่าผลกระทบของผีเสื้อ (Butterfly effect) โดยความหมายในระบบอุตุนิยมวิทยาเป็นระบบที่อ่อนไหวมากเพียงผีเสื้อขยับปีกที่ Hong Kong ก็อาจเกิดปรากฏการณ์ Tornado หรือสภาวะสับสนอลหม่านที่ California ได้

หลังจากที่ Lorenz ได้เผยแพร่งานวิจัยชิ้นนี้ก็เพียงแต่ได้รับความสนใจในงานทางวิทยาศาสตร์เท่านั้น ซึ่งต่อมาอีกเกือบ 30 ปี ทฤษฎีอลวนได้รับความสนใจจากวงการวิศวกรรม โดยวิศวกรมีความพยายามควบคุมระบบที่เกิดสภาวะอลวนซึ่งเป็นระบบที่ไร้เสถียรภาพขึ้น จึงได้มีแนวคิดที่จะนำเอาสภาวะอลวนหรือไร้ระเบียบนี้นำไปใช้ประโยชน์

2.1.1 ตัวดึงดูด Lorenz (Lorenz attractor)

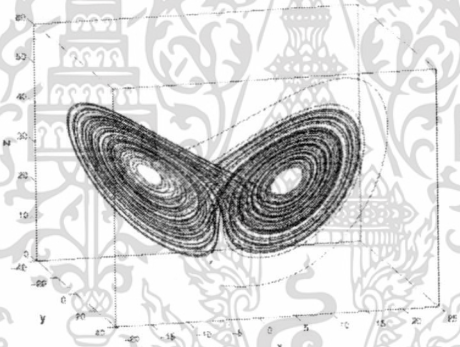
คิดขึ้นโดย เอ็ดเวิร์ด ลอเรนซ์ (Edward Lorenz) ในปี ค.ศ1963 เป็นระบบพลวัตไม่เป็นเชิงเส้น 3 มิติ ทฤษฎีดังกล่าวใช้อธิบายการเคลื่อนตัวของก๊าซและของเหลว สมการที่ใช้อธิบายปรากฏการณ์ Lorenz Attractor นี้คือ

ตัวดึงดูด Lorenz เขียนในรูปสมการทางคณิตศาสตร์เชิงอนุพันธ์ได้ดังต่อไปนี้ :

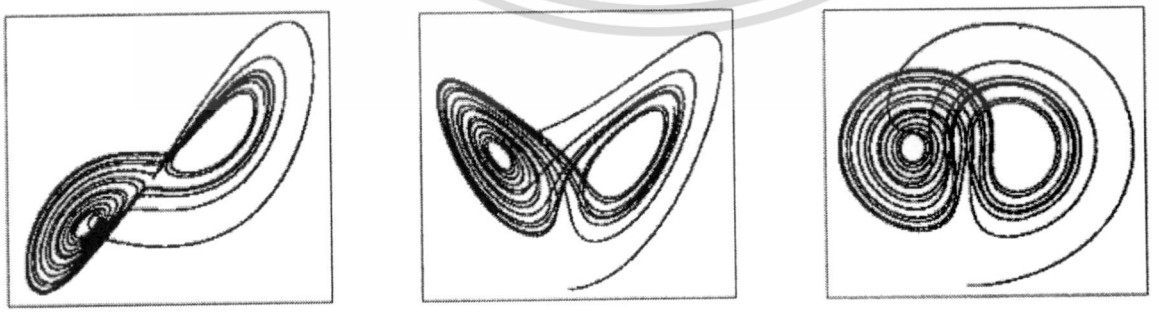
$$\frac{dx}{dt} = \sigma(y - x)$$
$$\frac{dy}{dt} = rx - y - xz \qquad (1)$$
$$\frac{dz}{dt} = xy - bz$$

σ คือค่าอัตราส่วนระหว่างแรงต้านของของเหลวและแรงดันของก๊าซหรือของเหลว, ρ คือค่าความต่างของอุณหภูมิระหว่างช่วงบนสุดกับล่างสุดของตัวกลาง และ β คืออัตราส่วนระหว่างความกว้างกับความยาวของภาชนะที่ใช้บรรจุ เราเรียกปรากฏการณ์นี้ว่า The Butterfly Effect เนื่องด้วยลักษณะการกระจายตัวของค่าที่ได้มีลักษณะคล้ายกับปีกผีเสื้อ ถ้าเราเปลี่ยนแปลงค่า σ, ρ หรือ β เพียงตัวเดียว ถึงแม้ว่าจะเป็นเพียงเล็กน้อยก็ตาม ผลลัพธ์ที่ได้จะเปลี่ยนแปลงไปจากเดิมโดยสิ้นเชิง

จากสมการของ Lorenz เมื่อพล็อตความสัมพันธ์ลงบนแกน x,y,z จะได้ดังรูปที่ 2.1



รูปที่ 2.1 สัญญาณอลวนจากตัวดึงดูด Lorenz ในลักษณะ 3 มิติ



(a) (b) (c)

รูปที่ 2.2 สัญญาณอลวนจากตัวดึงดูด Lorenz ในลักษณะ 2 มิติระหว่างระนาบต่างๆ

(a)ระนาบ x ,y (b) ระนาบ x,z (c) ระนาบ y,z

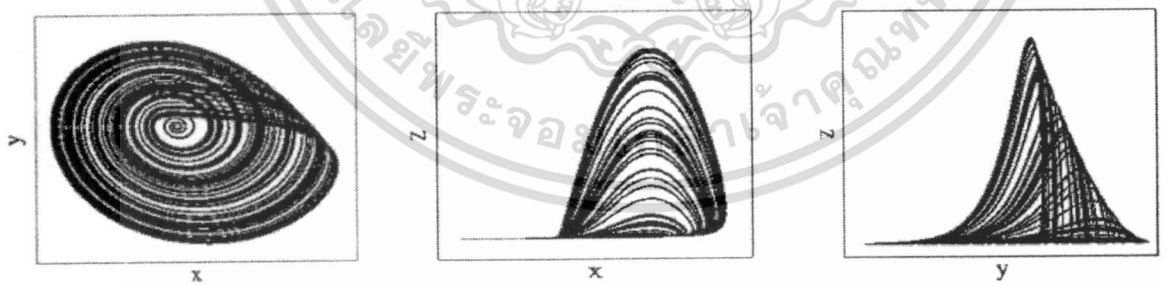
2.1.2 ตัวดึงดูด Rossler (Rossler attractor)

ตัวดึงดูด Rossler นี้คิดขึ้นโดย Otto Rossler ซึ่งสร้างจากชุดของสมการอนุพันธ์ปกติ เขียนในรูปสมการทางคณิตศาสตร์ได้ดังต่อไปนี้ :

$$\frac{dx}{dt} = -y - z$$
$$\frac{dy}{dt} = x - ay \qquad (2)$$
$$\frac{dz}{dt} = a + z(x - c)$$

จากสมการของ Rossler จะเห็นได้ว่าสมการของ Rossler จะมีเทอมผลคูณ 2 ตัวแปรเพียงเทอมเดียวซึ่งน้อยกว่ารูปแบบสมการของ Lorenz ทำให้การใช้วงจร multiplex ลดลง และเมื่อพล็อตความสัมพันธ์ลงบนแกน x,y,z จะได้ดังรูปที่ 2.3

รูปที่ 2.3 สัญญาณอลวนจากตัวดึงดูด Rossler ในลักษณะ 3 มิติ



(a) (b) (c)

รูปที่ 2.4 สัญญาณอลวนจากตัวดึงดูด Lorenz ในลักษณะ 2 มิติระหว่างระนาบต่างๆ

(a) ระนาบ x ,y (b) ระนาบ x,z (c) ระนาบ y,z

2.2 คุณสมบัติของตัวเลขค่าสุ่มและมาตรฐานการทดสอบ

ลักษณะของค่าสุ่ม

- ค่าที่ได้ไม่สามารถระบุตำแหน่งการเกิดได้อย่างเฉพาะเจาะจง
- ค่าที่ได้ต้องกระจายตัวกันไม่มีการซ้ำค่าเดิมจนมากเกินไป
- ค่าทุกค่าควรมีความน่าจะเป็นในการเกิดที่ใกล้เคียงกันเมื่อความยาวเป็นอนันต์
- ไม่มีรอบการเกิดซ้ำ
- ค่าที่ได้เป็นอิสระต่อกัน

มาตรฐานการทดสอบ

โดยมาตรฐานที่เราจะใช้ในงานวิจัยนี้เป็นมาตรฐานที่นิยมใช้งานกันมากที่สุดคือมาตรฐาน FIPS 140-1 tests การที่จะได้ผลลัพธ์ที่เชื่อถือได้นั้น ค่าจำนวนบิตจะต้องมีความยาวมากพอที่จะทำการวัด โดยมาตรฐานนี้ใช้จำนวนบิต 20,000 บิต และมีคุณสมบัติอยู่ภายใต้กฎทั้ง 4 ข้อ ไม่ผ่านข้อใดข้อหนึ่งก็ถือว่าไม่ผ่านมาตรฐาน คือ

2.2.1 Monobit Test คือ การทดสอบในการนับจำนวนบิตที่เป็น '1' ให้อยู่ภายใต้เงื่อนไข

$9{,}654 < N < 10{,}346$ เมื่อ N คือจำนวนบิตที่เป็น '1'

2.2.2 Poker Test คือ การทดสอบการกระจายตัวของบิตตามสมการนี้

$$X_1 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^{\,2}\right) - k \qquad (3)$$

m = ความยาวของจำนวนบิตที่ทำการแบ่งเป็นกลุ่ม

k = จำนวนของกลุ่ม [k = n/m]

i = ลำดับของกลุ่ม$(1,2,3,\ldots,2^m)$

n_i = ค่าตัวเลขฐานสิบของกลุ่มนั้นๆ ที่ทำการแปลงมาจากตัวเลขฐานสอง

ถ้าเรากำหนดความยาวของกลุ่มเป็น 4 บิตจะได้(m = 4)

$$X_1 = \frac{16}{5{,}000}\left(\sum_{i=1}^{16} n_i^{\,2}\right) - 5{,}000 \qquad (4)$$

ค่าจะต้องอยู่ในช่วง $1.03 < X < 57.4$ จึงจะผ่านการทดสอบ

2.2.3 Runs Test คือ การทดสอบเพื่อหาความถี่ในการเกิดบิตติดกัน โดยจะใช้สมการต่อไปนี้ทำการนับ

$$X_2 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(G_i - e_i)^2}{e_i} \qquad (5)$$

$e_i = (n-m+3)/2^{m+2}$

B_i = จำนวนครั้งที่เกิดบิต '1' ติดกัน

G_i = จำนวนครั้งที่เกิดบิต '0' ติดกัน

k = จำนวนของกลุ่ม [k = n/m]

m = จำนวนบิต '1'หรือ บิต '0' ที่ติดกัน

$X_2 \approx 2^k - k$

ค่าที่เป็นมาตรฐานจะต้องเป็นไปตามตารางที่ 2-1

จำนวนบิตที่ติดกัน	จำนวนครั้งที่เกิด
1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
≥ 6	90-223

ตารางที่ 2-1 ตารางแสดงค่ามาตรฐานที่ใช้ใน Runs Test

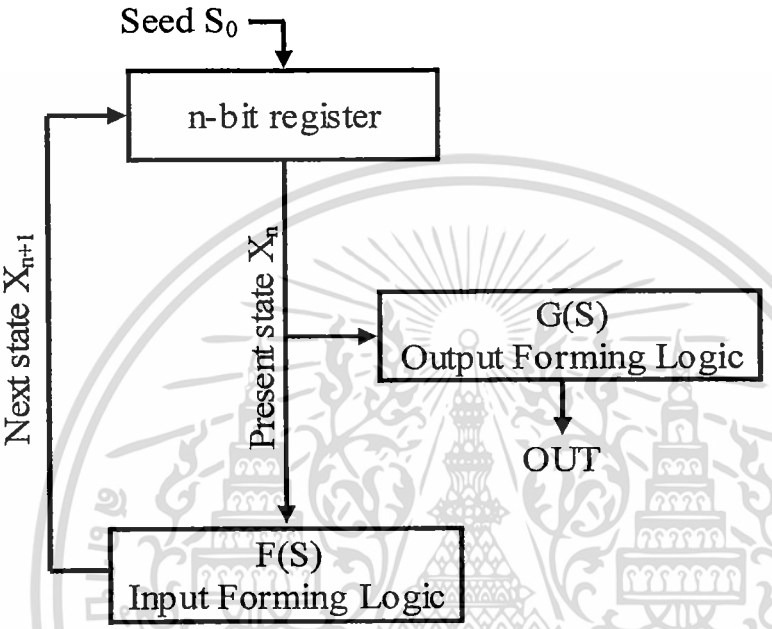
2.2.4 Long-run Test เป็นการตรวจสอบว่าบิตมีการติดกันมากจนเกินไปหรือไม่ โดยมาตรฐานนี้จะกำหนดไว้ที่ความยาว 34 บิตคือถ้ามีบิต '0' หรือ '1' ติดกันเป็นจำนวนมากกว่าหรือเท่ากับ 34 บิต ก็จะไม่ผ่านการทดสอบนี้

2.3 ประเภทของแหล่งกำเนิดค่าค่าสุ่ม

2.3.1 Pseudo random number generators เป็นอัลกอลิทึมที่สร้างค่าค่าสุ่ม ขึ้นมาอย่างอัตโนมัติแต่ในที่สุดจะมีรอบการเกิดซ้ำ เพื่อให้เข้าใจได้ง่ายขึ้นจะทำการยกตัวอย่างอัลกอลิทึมพื้นฐานของแหล่งกำเนิดแบบนี้ เช่น Linear congruence generator แสดงสมการดังนี้

$$X_{n+1} = aX_n + b \pmod{m} \qquad (6)$$

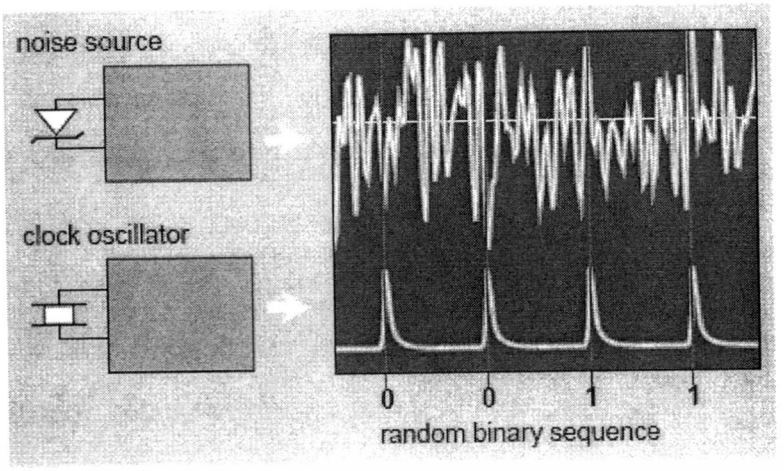
โดยค่า a และ b จะเป็นค่าคงที่หรืออาจเรียกว่ากุญแจของอัลกอลิทึมเพราะถ้าทราบค่าก็จะสามารถสร้างค่าค่าสุ่ม ที่มีลำดับเหมือนกันได้ และเมื่อเราใส่ค่าเริ่มต้น X_n อัลกอลิทึมก็จะทำการสร้างค่าค่าสุ่มมาเป็นจำนวนเท่ากับค่า m ซึ่งจะวนมาได้ค่า X_n ค่าเดิม ซึ่งจะเห็นว่าการสร้างค่าค่าสุ่มแบบนี้จะมีการสร้างค่าที่เป็นค่าค่าสุ่มในช่วงหนึ่งเท่านั้นแล้วจะมีการวนมาครบรอบใช้ค่าเริ่มต้นค่าเดิมอีก ค่าที่ได้ถัดมาก็จะเป็นไปตามอัลกอลิทึมเดิม



รูปที่ 2-5 Pseudo random number generator

จากรูปที่ 2-5 เป็นตัวอย่างบล็อกไดอะแกรมของอัลกอลิทึมที่สร้างบิตค่าสุ่มแบบ Pseudo random โดยโครงสร้างของบล็อกไดอะแกรมจะมีลักษณะเป็นวงจร Sequential ซึ่งค่า Next state จะขึ้นอยู่กับค่า Present state ทำให้ค่าที่ได้ไม่เป็นอิสระต่อกัน

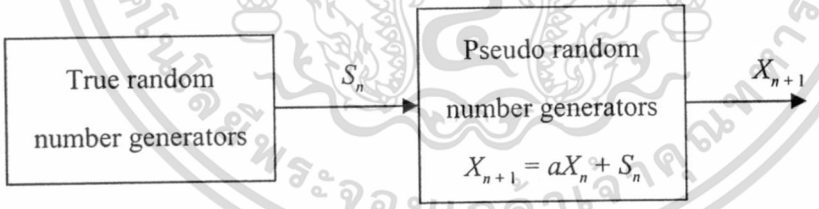
2.3.2 True random number generators จะสร้างค่าค่าสุ่มจากปรากฏการณ์ทางกายภาพของอุปกรณ์ทำให้ไม่สามารถทำนายผลได้ของค่าต่อไปได้ ตัวอย่างการเกิดสัญญาณนี้ เช่น ช่วงเวลาในการอ่อนกำลังลงของวัตถุกัมมันตรังสี สัญญาณรบกวนที่เกิดจากความร้อนที่ตัวอุปกรณ์อิเล็กทรอนิกส์ประเภทสารกึ่งตัวนำ วงจรกำเนิดสัญญาณChaotic เป็นต้น จึงมีชื่อเรียกอีกชื่อว่า hardware-based generators เพราะค่าค่าสุ่มเกิดจากอุปกรณ์ฮาร์ดแวร์ ที่สร้างสัญญาณที่ไม่สามารถทำนายได้อย่างต่อเนื่อง ตัวเลขที่สามารถสร้างมาจะเป็นไปตาม Physical noise



รูปที่ 2-6 True random number generator

จากรูป 2-6 เป็นตัวอย่างของ True random number generator จะเห็นว่าค่าที่ได้ไม่สามารถคาดเดาล่วงหน้าได้ ไม่มีรอบการวนซ้ำและค่าที่ได้เป็นอิสระต่อกัน การนำสัญญาณรบกวนมาใช้ในการสร้างค่าค่าสุ่มเป็นที่รู้จักกันดี แต่ในงานวิจัยจะทำการศึกษาเกี่ยวกับสัญญาณอลวนมาเป็นสัญญาณในการเกิดค่าค่าสุ่มแทน

2.3.3 Hybrid random number generators เป็นการนำ random generator แบบTrue random มา เป็นค่าเริ่มต้นให้กับอัลกอลิทึมของ Pseudo Random generator เพื่อคุณภาพของเอาท์พุตที่ดีขึ้น เนื่องจากจะไม่เกิดการวนรอบซ้ำ และจะมีการกระจายของข้อมูลได้ดีอีกด้วย



รูปที่ 2-7 Hybrid random number generators

2.4 แหล่งกำเนิดบิตค่าสุ่ม

การสร้างแหล่งกำเนิดบิตค่าสุ่มจากสัญญาณอลวนเราจะใช้ฟังก์ชันเทรสโฮล(Threshold function) ในการตัดสัญญาณอลวน โดยจะเป็นไปตามสมการดังนี้

$$s_c(x) = \begin{cases} 0, & if\ x < V_{ref} \\ 1, & if\ x \geq V_{ref} \end{cases} \qquad (7)$$

X = ค่าระดับแรงดันของวงจรอลวน

V_{ref} = ค่าระดับแรงดันของวงจรเปรียบเทียบแรงดัน

เราจะทำการกำหนดระดับแรงดันเปรียบเทียบ ถ้ามากกว่าค่าที่กำหนดจะมีค่าเป็นหนึ่งถ้าน้อยกว่าก็จะมีค่าเป็นศูนย์ เมื่อนำมาใช้กับวงจรอลวนคือเราจะใช้วงจรเปรียบเทียบแรงดัน(Comparator) โดยจะใช้ออปแอมป์เบอร์ LM311ซึ่งเป็นไอซีที่ใช้ในการเปรียบเทียบแรงดันที่รองรับความถี่สูง และระดับแรงดันเปรียบเทียบที่นำมาใช้ในวงจรอลวนอาจเป็นค่าเดียวหรือหลายค่าขึ้นอยู่กับวงจรอลวนที่เรานำมาใช้

รูปที่ 2-8 การใช้ฟังก์ชันเทรสโฮลตัดสัญญาณอลวน

2.4.1 การเลือกระดับแรงดันไฟในการตัดสัญญาณอลวน

การเลือกแรงดันเปรียบเทียบที่ใช้ในการตัดสัญญาณอลวนในช่วงที่เกิดคุณสมบัติค่าสุ่มที่แท้จริง จะต้องคำนึงถึงค่าเอ็นโทรปี(Entropy) ที่มีค่าสูงสุด เนื่องจากค่าเอ็นโทรปียิ่งสูงการบีบอัดข้อมูลก็ยิ่งทำได้ยาก นั่นหมายความว่าข้อมูลที่ได้มีคุณสมบัติค่าสุ่มมากขึ้นตามไปด้วย โดยการหาค่าเอ็นโทรปีควรหาจากข้อมูลที่มีจำนวนมาก ๆ และเลือกระดับของแรงดันที่อยู่ในช่วงการเกิดการค่าสุ่มมา 17 ระดับเพื่อที่จะได้ค่าที่เที่ยงตรง ซึ่งในแต่ละระดับจะมีการหาค่าเอ็นโทรปี ที่ n = 3 ถึง 10 และหาค่าเอ็นโทรปีได้จากสมการต่อไปนี้

$$H(x) = \frac{-\sum_{B^n} p(B^n)\ln P(B^n)}{n} \qquad (8)$$

n = จำนวนบิตที่ทำการแบ่งโดยจะไม่มีการทับซ้อนกัน

B^n = บิตจำนวน n ที่เรียงติดกันหรือเรียกว่าเวิร์ด (words)

$P(B^n)$ = ค่าความน่าจะเป็นของแต่ละเวิร์ด

โดยการแบ่งเวิร์ดเป็นไปตามสมการนี้

$$\{..., \{b(i), b(i+1),..., b(i+n-1)\}, \{b(i+n),..., b(i+2n-1)\},.... \} \quad (9)$$

2.4.2 การแบ่งช่วงของสัญญาณอลวน

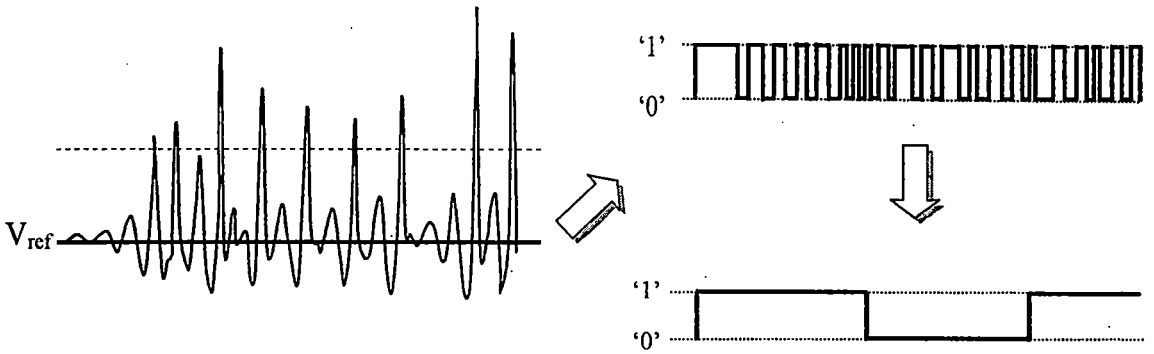
การแบ่งช่วงของสัญญาณอลวน เพื่อกำหนดค่าของบิตที่ได้จากการตัดสัญญาณในช่วงที่เกิดคุณสมบัติค่าสุ่มขึ้นว่าจะมีค่าเป็นบิต '0' หรือบิต '1' จากนั้นจึงทำการเลือกค่าค่าสุ่ม โดยค่าค่าสุ่มที่ได้จะขึ้นอยู่กับจำนวนบิตของแต่ละช่วง

วงจรอลวนมีอยู่หลากหลายรูปแบบ การแบ่งช่วงของอลวนจึงต้องดูลักษณะของสัญญาณแต่ละวงจรก่อน เช่นในงานวิจัยนี้ วงจร Double scroll in a simple '2D' chaotic oscillator [4] จะมีการแบ่งช่วงโดยสัญญาณอยู่แล้ว โดยการนำช่วงนั้นมาใช้ก็เพียงแต่ใช้วงจรเปรียบเทียบแรงดันเปรียบเทียบที่ 0 V ก็จะได้ช่วงของการเกิดสัญญาณค่าสุ่มอลวน

รูปที่ 2-9 การแบ่งช่วงสัญญาณอลวนที่มีการแบ่งช่วง

จากรูปที่ 2-9 เมื่อนำค่าไปรวมกับบิตค่าสุ่มที่ทำการตัดสัญญาณในช่วงที่เกิดคุณสมบัติค่าสุ่มขึ้น โดยนำค่าจากการแบ่งช่วงเป็นData และพัลส์ที่เกิดจากบิตค่าสุ่มเป็นClock จะได้บิต Bit sequence ดังนี้ '1111100000000111100000...'

ส่วนวงจรอื่นที่ไม่มีการแบ่งช่วงของสัญญาณ เราจะทำการแบ่งช่วงของสัญญาณ โดยการขยายช่วงในการกำหนดค่าบิตของบิตค่าสุ่ม ทำให้จำนวนของบิตที่เกิดขึ้นในแต่ละช่วงมีความหลากหลาย ซึ่งในงานวิจัยนี้จะใช้วิธีนำพัลส์ที่เกิดจากการเปรียบเทียบแรงดันในระดับที่เกิดลูกคลื่นมากที่สุดไปผ่านวงจรนับ



รูปที่ 2-10 การแบ่งช่วงสัญญาณอลวนที่ไม่มีการแบ่งช่วง

จากรูปที่ 2.10 เป็นการแบ่งช่วงโดยกำหนดให้พัลส์ 8 ลูกเท่ากับช่วงหนึ่งช่วง เมื่อนำค่าไปรวมกับบิตค่าสุ่มที่ทำการตัดสัญญาณในช่วงที่เกิดคุณสมบัติค่าสุ่มขึ้น โดยนำค่าจากการแบ่งช่วงเป็นData และพัลส์ที่เกิดจากบิตค่าสุ่มเป็นClock จะได้บิต Bit sequence ดังนี้ '11100011...'

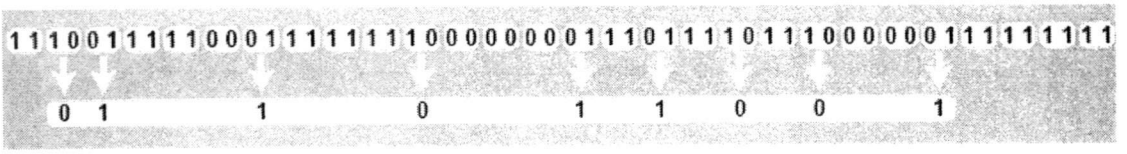
2.4.3 เทคนิควอนนูแมน (Von Neumann's technique)

ถึงแม้ว่าสัญญาณอลวนจะสร้างสัญญาณที่คาดเดาไม่ได้ แต่สัญญาณอลวนเป็นสัญญาณที่เกิดขึ้นต่อเนื่องไม่มีคาบเวลาที่แน่นอน ดังนั้นถ้านำข้อมูลที่ตัดมาใช้โดยตรง จะไม่แสดงความเป็นคุณสมบัติค่าสุ่มของ Bit sequence ที่ตัดมาจากสัญญาณอลวนที่แท้จริง เนื่องจากข้อมูลที่อยู่ติดกันจะมีความสัมพันธ์กัน เราจึงต้องหาวิธีในการเลือกข้อมูลที่แสดงความเป็นคุณสมบัติค่าสุ่มโดยทำการแบ่งข้อมูลเป็นชุด จากนั้นจึงกำหนดค่าของข้อมูลชุดนั้น ๆ ว่าเป็นบิตศูนย์ บิตหนึ่ง หรือจะไม่กำหนดค่าของข้อมูลชุดนั้น ซึ่งในงานวิจัยนี้จะใช้การกำหนดค่าตาม เทคนิคของวอนนูแมน(Von Neumann's technique) โดยวอนนูแมนได้เสนอว่าให้ทำการจับคู่ของข้อมูลโดยที่ไม่มีการซ้อนทับกัน และให้คู่ที่เป็น 01 มีผลลัพธ์เป็น 1 คู่ที่เป็น 10 มีผลลัพธ์เป็น 0 ส่วนคู่ที่เป็น 00 และ11 จะไม่ทำการกำหนดค่าของข้อมูล ก็จะได้ค่าค่าสุ่มมา โดยสามารถดูได้จากสมการที่ 10

$$b_i(s_i, s_{i-1}) = \begin{cases} 0, \; if \; s_i = 0 \wedge s_{i-1} = 1 \\ 1, \; if \; s_i = 1 \wedge s_{i-1} = 0 \\ Undefine, \quad Other \end{cases} \tag{10}$$

S_i = บิตที่อยู่ในสถานะปัจจุบัน

S_{i-1} = บิตก่อนหน้าบิต S_i หนึ่งบิต



รูปที่ 2.11 ภาพการเลือกบิตค่าสุ่มโดยใช้เทคนิคของวอนนูแมน

โดยจะสังเกตเห็นว่าเทคนิคของวอนนูแมนนั้น ค่าที่ได้จะขึ้นอยู่กับการแบ่งช่วงของ อลวน ถ้าจำนวนบิตในช่วงนั้นเป็นจำนวนคู่ จะไม่ทำการกำหนดค่าในข้อมูลชุดนั้นแต่ถ้าจำนวนบิตเป็นจำนวนคี่ จะใช้ข้อมูลจากชุดถัดไป และให้ผลลัพธ์เป็นข้อมูลที่ได้ดึงมาใช้

ดังนั้นค่าที่ได้เป็นอิสระต่อกันไม่ขึ้นอยู่กับค่าที่ได้รับการเลือกก่อนหน้า แต่จะขึ้นอยู่กับระยะการแบ่งช่วงของอลวนที่ทำให้เกิดจำนวนบิตในแต่ละช่วงแตกต่างกัน จำนวนบิตที่แตกต่างกันนี้เอง คือคุณสมบัติค่าสุ่มของสัญญาณอลวน

บทที่ 3
การสร้างวงจรกำเนิดสัญญาณอลวน

ในงานวิจัยจะทำการสร้างสัญญาณอลวนเพื่อนำไปเป็นแหล่งกำเนิดค่าสุ่มโดยการสร้างในหัวข้อ 3.2 -3.8 เป็นการทบทวนการสร้างจากงานวิจัยที่มีอยู่แล้วและในหัวข้อ 3.9-3.11 เป็นการค้นพบใหม่

3.1 ตัวดึงดูด Sprott (Sprott attractor)

หลังจากที่ Lorenz และ Rossler ได้ค้นพบสมการเกี่ยวกับการสร้างตัวดึงดูดสัญญาณ อลวน ต่อมามีผู้ได้ศึกษาเกี่ยวกับการสร้างสัญญาณอลวนแบบใหม่ คือ J.C. Sprott ซึ่งได้ใช้คอมพิวเตอร์หาสมการอลวนทั้งหมดที่เป็นไปได้โดยอยู่ในรูป Jerk function ($\dddot{x} = J(\ddot{x}, \dot{x}, x)$) พร้อมด้วยฟังก์ชันแบบไม่เป็นเชิงเส้นแบบง่ายๆ 1 ตัว โดยสมการที่ Sprott ค้นพบมีดังนี้

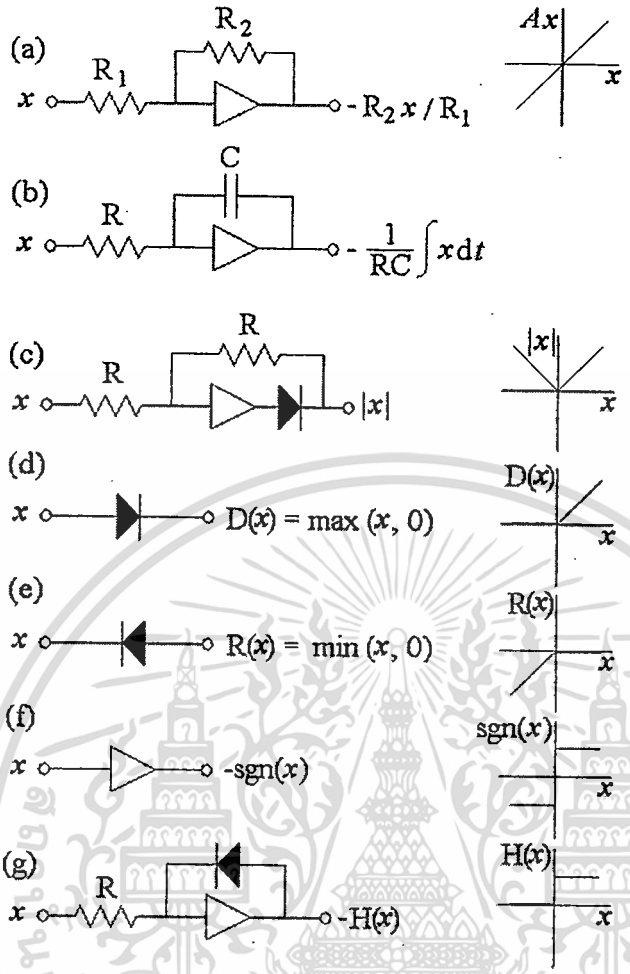
ตารางที่ 3.1 แสดงการสร้างสัญญาณอลวน third-order ODE systemsและ Lyapunov exponents

System	Initial conditions $(x, \dot{x}, \ddot{x})$	Lyapunov exponents (base e)
$\dddot{x} = -2.017\ddot{x} \pm \dot{x}^2 - x$	(0, 0, ±1)	0.055, 0, −2.072
$\dddot{x} = -2.8\ddot{x} \pm \dot{x} + x^2$	(∓0.5, −1, 1)	0.002, 0, −0.002
$\dddot{x} = -0.44\ddot{x} - 2\dot{x} \pm (x^2 - 1)$	(0, 0, 0)	0.105, 0, −0.545
$\dddot{x} = -0.5\ddot{x} - \dot{x} \pm x \pm x^2$	(0, ±1, 0)	0.094, 0, −0.594
$\dddot{x} = -2\ddot{x} \pm (\lvert\dot{x}\rvert - 1)$	±(−1, −1, 1)	0.003, 0, −0.003
$\dddot{x} = -0.6\ddot{x} - \dot{x} \pm (\lvert x\rvert - 1)$	(0, 0, 0)	0.036, 0, −0.636
$\dddot{x} = -0.3\ddot{x} - 0.3\dot{x} - D(x) + 1$	(0, 0, 0)	0.042, 0, −0.342
$\dddot{x} = -0.3\ddot{x} - 0.3\dot{x} - R(x) - 1$	(0, 0, 0)	0.042, 0, −0.342
$\dddot{x} = -2.9\ddot{x} \pm (0.7x - D(x) + 1)$	±(0, −0.5, 0.5)	0.003, 0, −0.003
$\dddot{x} = -2.9\ddot{x} \pm (0.7x - R(x) - 1)$	±(0, 0.5, −0.5)	0.003, 0, −0.003
$\dddot{x} = -0.5\ddot{x} - \dot{x} - x + \mathrm{sgn}(x)$	(0, 1, 0)	0.152, 0, −0.652
$\dddot{x} = -0.5\ddot{x} - \dot{x} + x - \mathrm{sgn}(x)$	(0, 1, 0)	0.601, 0, −1.101
$\dddot{x} = -0.7\ddot{x} - \dot{x} - x + H(x)$	(0, 1, 0)	0.085, 0, −0.785
$\dddot{x} = -0.4\ddot{x} - \dot{x} - x + 2S(x)$	(0, 1, 0)	0.072, 0, −0.472
$\dddot{x} = -0.4\ddot{x} - \dot{x} + x - 2S(x)$	(0, 1, 0)	0.091, 0, −0.491
$\dddot{x} = -0.19\ddot{x} - \dot{x} - x + 2\tanh(x)$	(0, 1, 0)	0.128, 0, −0.318
$\dddot{x} = -0.19\ddot{x} - \dot{x} + x - 2\tanh(x)$	(0, 1, 0)	0.067, 0, −0.257
$\dddot{x} = -3.7\ddot{x} \pm (x - x^3)$	(0, ±0.5, 1)	0.002, 0, −0.002
$\dddot{x} = -0.6\ddot{x} + 2.8\dot{x} - x^3 - x$	(0, 1, 0)	0.034, 0, −0.634
$\dddot{x} = -0.7\ddot{x} - \dot{x} + x - x^3$	(0, 1, 0)	0.138, 0, −0.838
$\dddot{x} = -0.35\ddot{x} - \dot{x} - x + x^3$	(0, 1, 0)	0.082, 0, −0.432
$\dddot{x} = -0.2\ddot{x} - \dot{x} \pm \sin(x)$	(0, 1, 0)	0.123, 0, −0.323

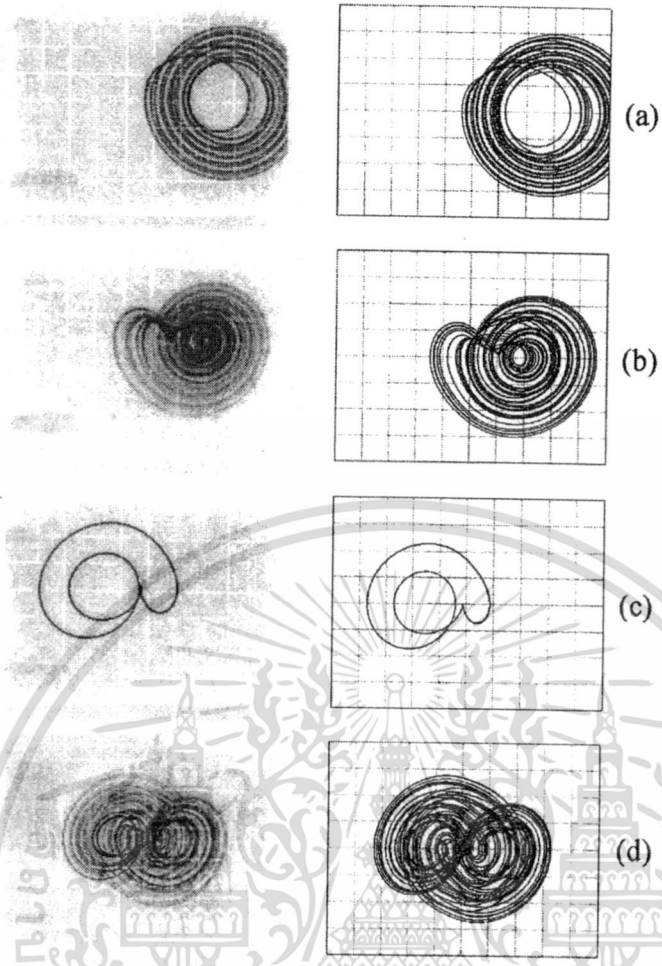
จากตารางที่ 3.1 แสดงสมการอลวนที่อยู่ในรูปแบบของสมการคณิตศาสตร์ พร้อมกับค่าเริ่มต้นและค่า Lyapunov exponents ที่ J.C. Sprott ค้นพบ

ในการสร้างวงจรในทางปฏิบัติจากสมการคณิตศาสตร์เราใช้วงจรอินทิเกรเตอร์ วงจรขยาย และวงจรไม่เป็นเชิงเส้นแบบต่างๆ ซึ่งสร้างโดยอาศัยออปแอมป์และไดโอดแสดงได้ดังรูปที่ 3.1

จากรูปจะเห็นได้ว่าเราสามารถสร้างวงจรขยายสัญญาณ วงจรอินทิเกรเตอร์ และวงจรแบบไม่เป็นเชิงเส้นได้ด้วยการใช้ออปแอมป์และไดโอด ซึ่งในแต่ละกรณีอินพุตจะต่อเข้ากับขา inverting(-) ของออปแอมป์และสำหรับขา noninverting(+)จะต่อลงกราวด์



รูปที่ 3.1 แสดงการดำเนินการทางคณิตศาสตร์ที่แทนด้วยวงจรทางอิเล็กทรอนิกส์



รูปที่ 3.2 สัญญาณอลวนจากตัวดึงดูด Sprott ในลักษณะ 2 มิติระหว่างระนาบ x กับ x'

3.2 การสร้างอลวนแบบวงจรอนาล็อก

ในการออกแบบวงจรสำหรับสร้างสัญญาณอลวนแบบอนาล็อกสามารถสร้างได้ง่ายโดยอาศัยรูปแบบสมการของ J.C.Sprott ซึ่งสมการมีความซับซ้อนไม่มากอีกทั้งฟังก์ชันแบบไม่เป็นเชิงเส้นในสมการบางสมการสามารถสร้างได้โดยใช้วงจรทางไฟฟ้า

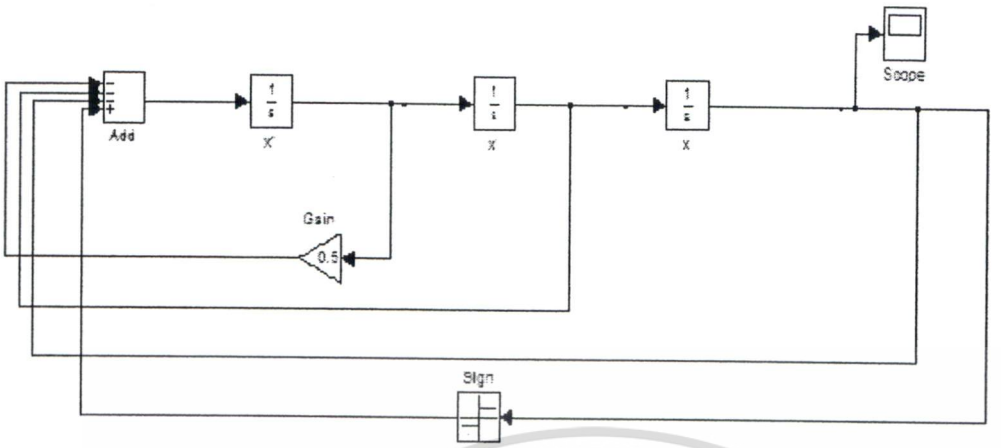
จากสมการทางคณิตศาสตร์ที่ใช้สำหรับการสร้างสัญญาณอลวนอย่างง่ายของ Sprott มีหลายรูปแบบ เพื่อแสดงให้เห็นตัวอย่างในการสร้างสัญญาณอลวนจะเลือกสมการที่ใช้ sgn(x) และ H(x) เนื่องจากง่ายในการสร้าง ดังสมการด้านล่าง

$$\dddot{x} = -0.5\ddot{x} - \dot{x} - x + \text{sgn}(x) \tag{1}$$

$$\dddot{x} = -0.5\ddot{x} - \dot{x} + x - \text{sgn}(x) \tag{2}$$

$$\dddot{x} = -0.7\ddot{x} - \dot{x} - x + H(x) \tag{3}$$

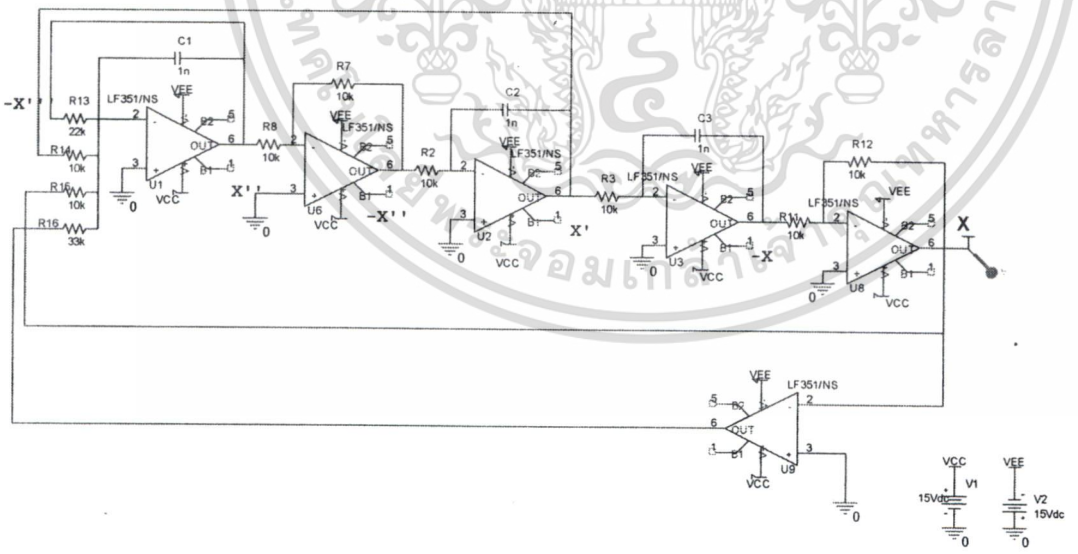
จากสมการ (1) เราสามารถที่จะจำลองพฤติกรรมโดยใช้โปรแกรม Matlab ได้ดังรูปที่ 3.3



รูปที่ 3.3 แบบจำลองการสร้างสัญญาณอลวนของสมการ (1)

เราสามารถสร้างวงจรกำเนิดสัญญาณอลวนจากสมการ (1) แสดงได้ดังรูปที่ 3.4 โดยในทางปฏิบัติการสร้างวงจรอินทิเกรเตอร์แบบลบสามารถสร้างได้ง่ายกว่าอินทิเกรเตอร์แบบบวก ดังนั้นเราจึงต้องเพิ่มออปแอมที่ทำหน้าที่กลับขั้ว

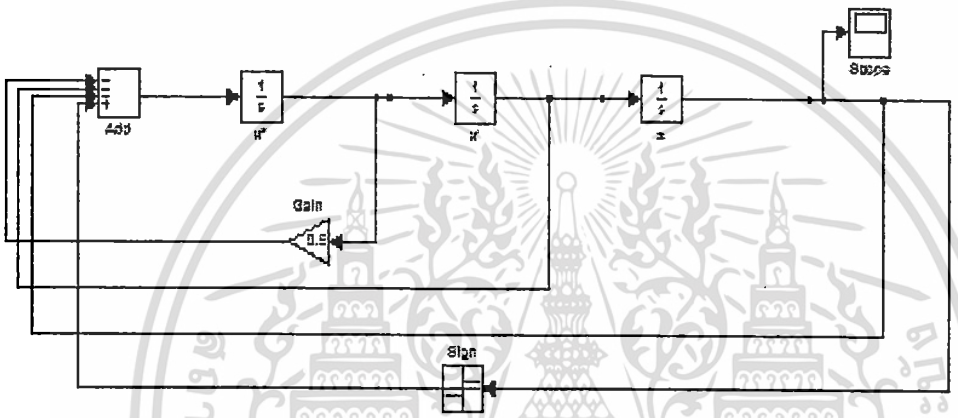
การจำลองวงจรจากสมการที่ (1) โดยใช้โปรแกรม Pspice



รูปที่ 3.4 แสดงวงจรที่ออกแบบโดยใช้โปรแกรม Pspice ของสมการ (1)

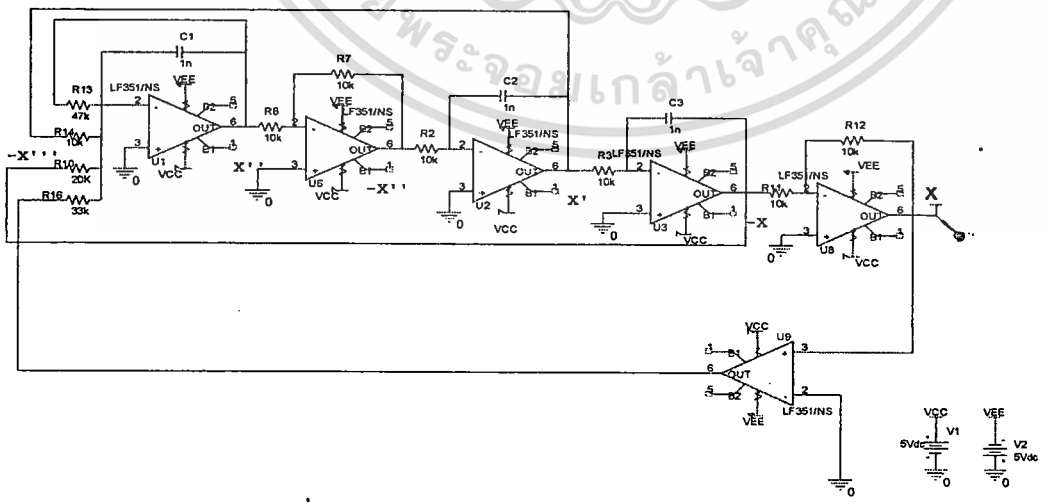
จากรูปที่ 3.4 จะเห็นว่าที่ออปแอมป์ U8 ให้เอาท์พุต X เนื่องจากเอาท์พุทที่ออกจาก U3

(คือ –X) ถูกนำมาผ่านออปแอมป์เพื่อที่จะทำการกลับเครื่องหมาย สำหรับอินพุทของ U3 นั้นจะเป็น x' ซึ่งเมื่อผ่านอินทิเกรเตอร์ U3 ก็จะได้เอาท์พุทเป็น –X เนื่องจากเป็น inverting amplifier และสำหรับค่าอินพุทและเอาท์พุทของอินทิเกรเตอร์แต่และตัวก็ใช้ในการพิจารณาเช่นเดียวกัน โดยมีอินทิเกรเตอร์ U9 ทำหน้าที่เป็นวงจรที่ใช้ในการเปรียบเทียบ ซึ่งหากแรงดันที่เข้ามาที่ขา 2 มีค่ามากว่าแรงดันอ้างอิงที่ขา 3 เอาท์พุทที่ได้จะเป็น –Vsat แต่หากแรงดันที่เข้ามาที่ขา 2 มีค่าน้อยกว่าแรงดันอ้างอิงที่ขา 3 เอาท์พุทที่ได้จะเป็น +Vsat (Inverting Comparator) ดังนั้นจะได้ว่าที่อินพุทของอินทิเกรเตอร์ U1 คือ $\dddot{x} = -0.5\ddot{x} - \dot{x} - x + \mathrm{sgn}(x)$ ซึ่งตรงกันกับสมการที่ (1)
จากสมการ (2) เราสามารถที่จะจำลองพฤติกรรมโดยใช้โปรแกรม Matlab ได้ดังรูปที่ 3.5



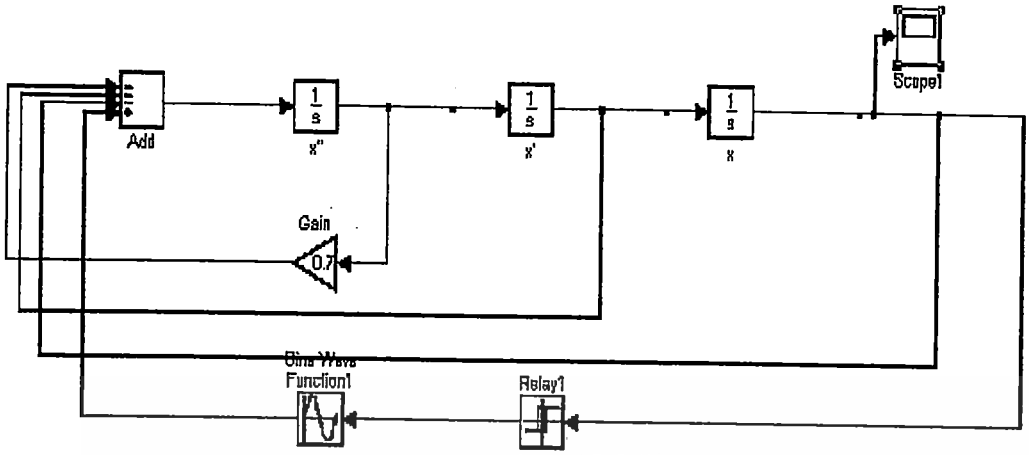
รูปที่ 3.5 โมเดลจำลองการสร้างสัญญาณอลวนโดยใช้สมการ (2)

และสามารถสร้างวงจรกำเนิดสัญญาณอลวนจากสมการ (2) แสดงได้ดังรูปที่ 3.6 แสดงวงจรที่ออกแบบโดยใช้โปรแกรม Pspice

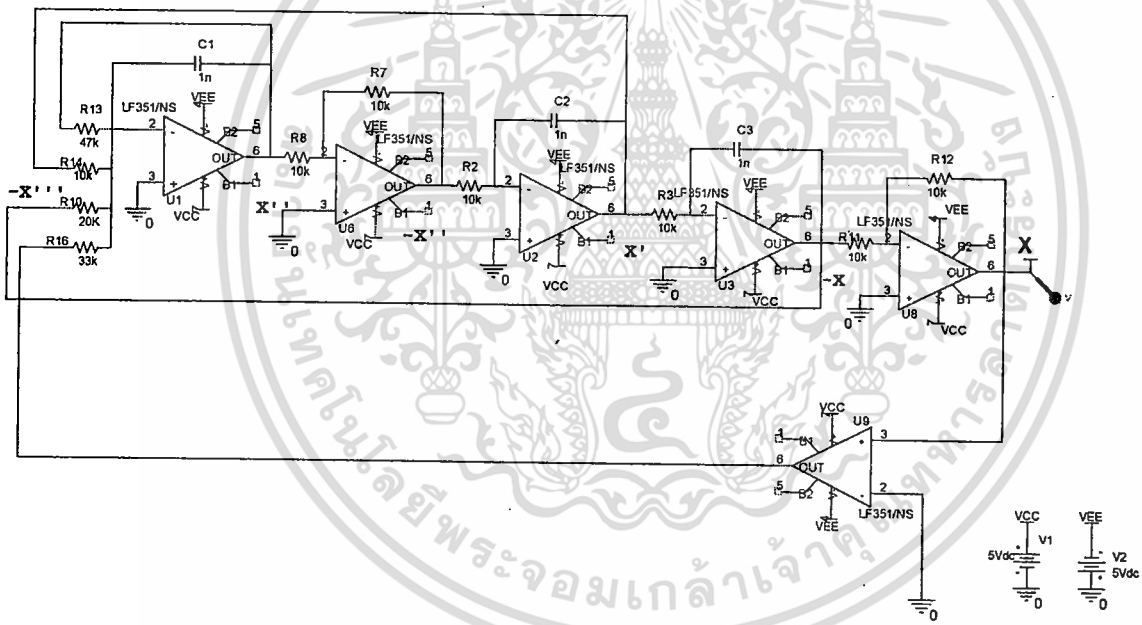


รูปที่ 3.6 สร้างสัญญาณอลวนโดยใช้สมการ (3)

และสามารถสร้างวงจรกำเนิดสัญญาณอลวนจากสมการ (3) แสดงได้ดังรูปที่ 3.7



รูปที่ 3.7 รูปสร้างวงจรกำเนิดสัญญาณอลวนจากสมการ (3)



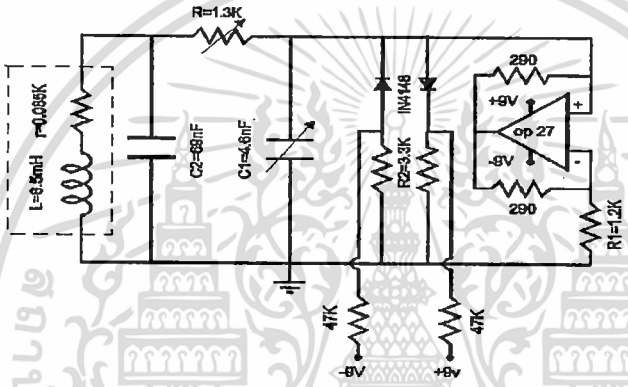
รูปที่ 3.8 แสดงวงจรที่ออกแบบโดยใช้โปรแกรม Pspice

3.3 วงจร Chua's

ในการออกแบบวงจรที่มีการนำทฤษฎีของ Chaos มาใช้นั้น จะมีรูปแบบวิธีการที่นำมาใช้อยู่มากมาย แต่ส่วนใหญ่จะเลือกใช้วงจร Chua's ซึ่งเป็นวงจรพื้นฐานที่เป็นที่นิยมแบบหนึ่งของ Chaotic วงจร Chua's เป็นวงจรที่แสดงผลออกมาในรูปแบบ 3 มิติ ที่สร้างได้ง่าย มีความเสถียรทนทาน มีความปลอดภัยสูง ลักษณะการเคลื่อนที่เป็นแบบม้วนที่มีความซับซ้อน

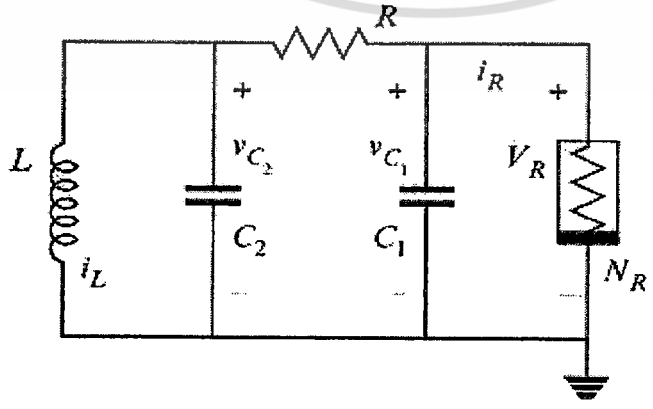
วงจร Chua's เราจะสามารถแบ่งไปออกเป็น 2 แบบ

แบบไม่เป็นเชิงเส้น (Nonlinear element) หรือเรียกว่า Chua's Diode ซึ่งวงจรจะมี **Diode** เป็นส่วนประกอบ



รูปที่ 3.9 Chua circuit diagram แบบ nonlinear element

แบบเชิงเส้น (Linear elements) ซึ่งวงจรจะประกอบไปด้วย resistor, inductor, capacitor ซึ่งเป็นรูปแบบที่เราใช้ในการศึกษา



รูปที่ 3.10 Chua's circuit diagram แบบ linear elements

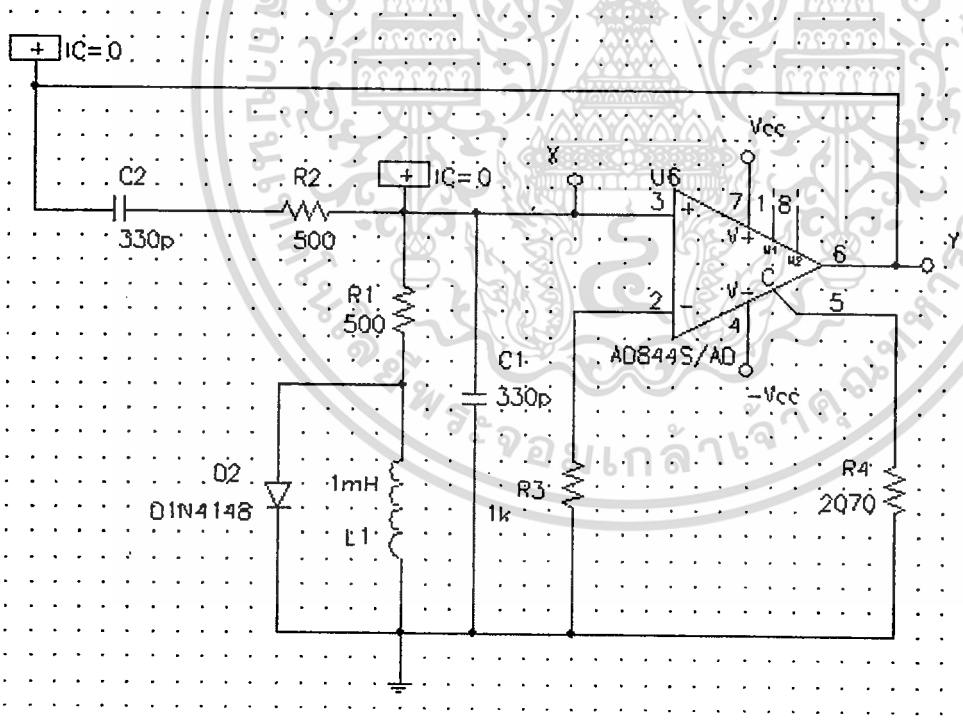
สมการแสดงสถานะของวงจร Chua's

$$
\begin{aligned}
C_1 \frac{dv_{c_1}}{dt} &= G\left(v_{c_2} - v_{c_1}\right) - g\left(v_{c_1}\right) \\
C_2 \frac{dv_{c_2}}{dt} &= G\left(v_{c_1} - v_{c2}\right) + i_L \\
L \frac{di_L}{dt} &= -v_{c_2} - R_L i_L
\end{aligned}
\qquad (4)
$$

$$
g\left(v_R\right) = m_0 v_R + \frac{1}{2}\left(m_1 - m_0\right)\left(\left|v_R + B_p\right| - \left|v_R - B_p\right|\right)
$$

3.4 วงจร High frequency Wien-type chaotic oscillator [2]

เป็นวงจรที่ประยุกต์จากวงจรวีนบริดจ์โดยส่วนของการป้อนกลับจะมีตัวเหนี่ยวนำและไดโอดที่เป็นอุปกรณ์นอนลิเนียร์ต่อร่วมเข้าไปทำให้เกิดสัญญาณแรนดัม นอกจากนี้ยังมีแนวคิดในการทำงานในย่านความถี่สูงจึงมีการใช้ Op-Amp ที่ผลตอบสนองในย่านความถี่สูงมาใช้



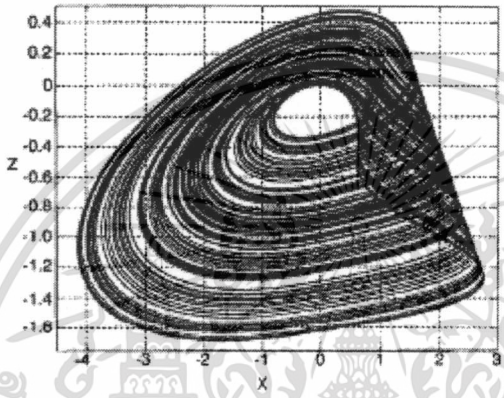
รูปที่ 3-11 ภาพวงจร High frequency Wien-type chaotic oscillator

โดยวงจรจะมีความสัมพันธ์กับรูปแบบสมการ

$$\begin{bmatrix} X' \\ Y' \\ Z' \\ \varepsilon W' \end{bmatrix} = \begin{bmatrix} k-2 & -1 & 0 & 1 \\ k-1 & -1 & 0 & 0 \\ 0 & 0 & 0 & \beta \\ 1 & 0 & -1 & -(1+a) \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ a \end{bmatrix} \quad (5)$$

เมื่อ $a = \alpha \quad W \geq 1, \; a = 0 \quad W < 1$

โดยมี $\mathbf{K}, \varepsilon, \alpha, \beta$ เป็นค่าคงที่ซึ่งเมื่อ $\mathbf{K} = 2.15, \varepsilon = 0.004, \alpha = 15, \beta = 0.21$ จะเกิดสัญญาณอลวนขึ้นและเมื่อพอร์ตด้วย สมการจะได้รูปดังนี้



รูปที่ 3-5กราฟแสดงผลจากสมการ High frequency Wien-type chaos ในระนาบ XZ

$\mathbf{K} = 2+R_2/R_1$

$\varepsilon = C_D/C$

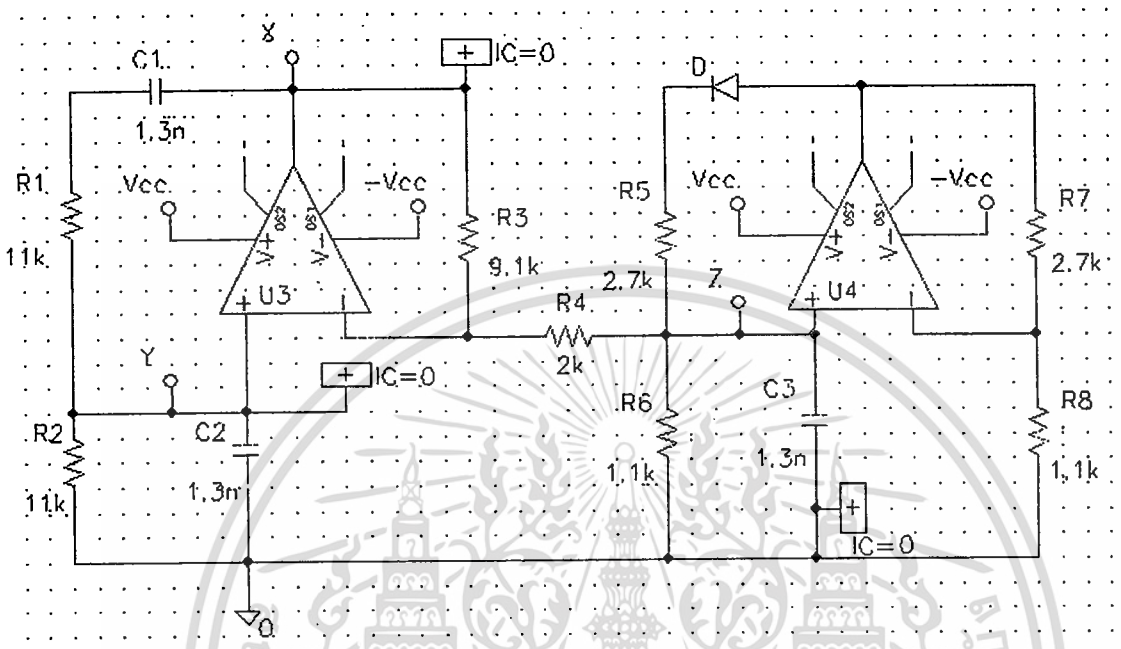
$\alpha = R/R_D$

$\beta = R^2C/L$

โดยค่าR_D,C_D คือ ค่าความต้านทานและค่าความจุที่ตัวไดโอดตามลำดับ เราจะกำหนดค่าของอุปกรณ์อิเล็กทรอนิกส์ดังนี้ $C_1 = C_2 = C = 330pF$, $R_1 = R_2 = R = 500\Omega$, $L = 1mH$, $R_3 = 1K\Omega$, $R_4 = 2070\Omega$ เพื่อให้ได้ค่าใกล้เคียงกับค่าคงที่ที่เกิดสภาวะอลวน และใช้ Op-Amp AD844 เพื่อตอบสนองความถี่สูง

3.6 วงจร Simple RC chaotic oscillator [3]

เป็นวงจร ที่มีแนวคิดในการใช้วงจรวีนบริดจ์ที่มีส่วนของอุปกรณ์นอนลิเนียร์ต่อร่วมอยู่ สำหรับเป็นวงจรป้อนกลับ



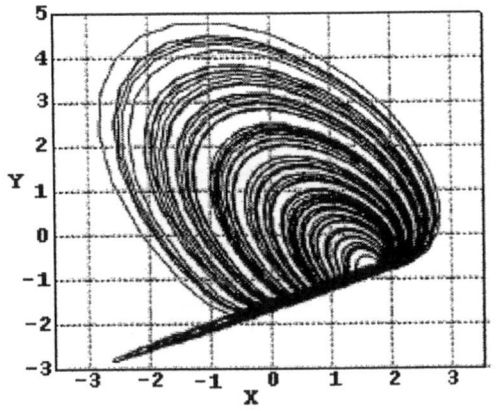
รูปที่ 3-13 ภาพวงจร Simple RC chaotic oscillator

โดยวงจรจะมีความสัมพันธ์กับรูปแบบสมการ

$$\begin{bmatrix} X' \\ Y' \\ Z' \end{bmatrix} = \begin{bmatrix} -1 & k_1 - 1 & -k_1 + 1 \\ -1 & k_1 - 2 & -k_1 + 1 \\ 0 & k_1 & -k_1 - \alpha \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ \beta(z-1)H(z-1) \end{bmatrix} \quad (6)$$

เมื่อ H(u) เป็น Heaviside function คือ $H(u<0) = 0$, $H(u \geq 0) = 1$

โดยมี K_1, α, β เป็นค่าคงที่ซึ่งเมื่อ $K_1 = 5$, $\alpha = 10$, $\beta = 14$ จะเกิดสัญญาณอลวนขึ้น และเมื่อพอร์ตด้วย สมการจะได้รูปดังนี้



รูปที่ 3-14 กราฟแสดงผลจากสมการ Simple RC chaos ในระนาบ XY

$$K_1 = 1+R_3/R_4$$

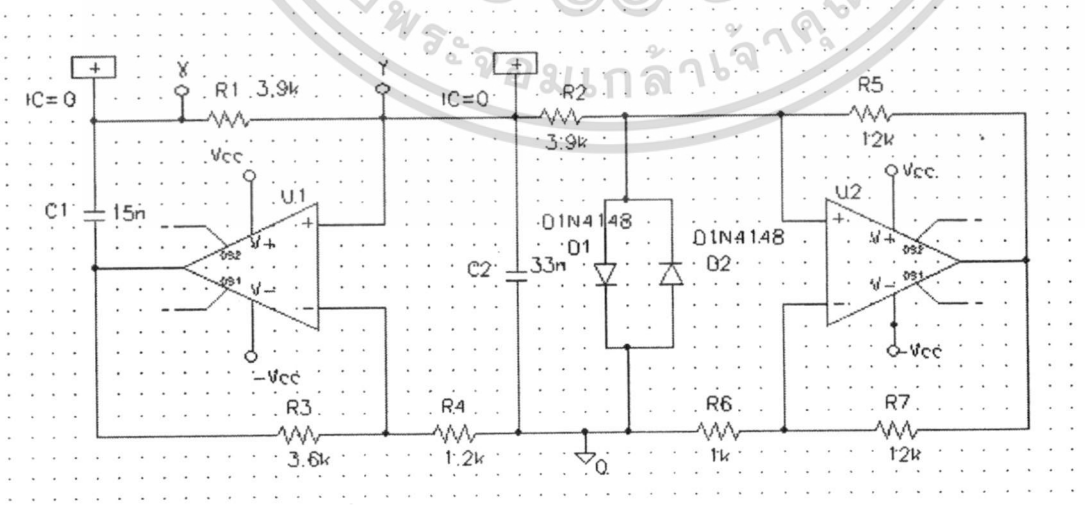
$$\alpha = R/R_6$$

$$\beta = R/R_8$$

เราจะกำหนดค่าของอุปกรณ์อิเล็กทรอนิกส์ได้ดังนี้ $C_1 = C_2 = C_3 = C = 1.3nF$, $R_1 = R_2 = R = 11K\Omega$, $R_3 = 9.1\ K\Omega$, $R_4 = 2K\Omega$, $R_5 = R_7 = 2.7\ K\Omega$, $R_6 = 1.1\ K\Omega$, $R_8 = 780\Omega$ เพื่อให้ได้ค่าใกล้เคียงกับค่าคงที่ที่เกิดสภาวะอลวน

3.7 วงจร Double scroll in a simple '2D' chaotic oscillator [4]

เป็นการนำเอาวงจรวีนบริดจ์ โดยใช้วงจร Negative impedance converter (NIC) ที่มีลักษณะของเอาท์พุต เป็นรูปแบบใกล้เคียงกับ Square Wave มาเป็นส่วนวงจรป้อนกลับเพื่อสร้างสัญญาณแรนดัม



รูปที่ 3-15 ภาพวงจร Double scroll in a simple '2D' chaotic oscillator

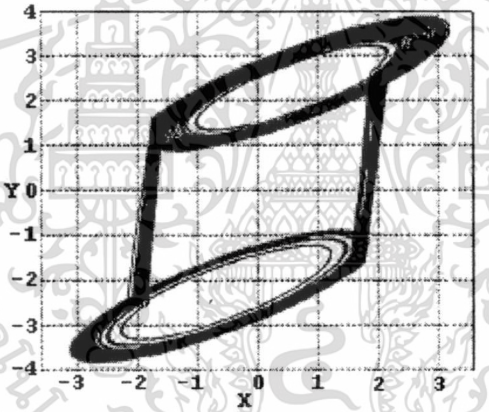
โดยวงจรจะมีความสัมพันธ์กับรูปแบบสมการ

$$\begin{bmatrix} X' \\ aY' \end{bmatrix} = \begin{bmatrix} -1 & k_1 - 1 \\ -1 & k_1 - 1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} + \begin{bmatrix} 0 \\ -S(Y) \end{bmatrix} \quad (7)$$

เมื่อ $S_{i+1}(Y) = S_i [1-2H(S_iY-b)]$

และ H(u) เป็น Heaviside function คือ $H(u<0) = 0$, $H(u \geq 0) = 1$

โดยมี $\mathbf{K_1}$, $\mathbf{K_2}$, **a**, **b** เป็นค่าคงที่ซึ่งเมื่อ $\mathbf{K_1} = 4.06$, $\mathbf{K_2} = 13$, $\mathbf{a} = 2$, $\mathbf{b} = 3$ จะเกิดสัญญาณอลวนขึ้นและเมื่อพอร์ตด้วย สมการจะได้รูปดังนี้



รูปที่ 3-16 กราฟแสดงผลจากสมการ Double scroll in a simple 2D chaos ในระนาบ XY

$\mathbf{K_1} = R_3/R_4+1$

$\mathbf{K_2} = R_7/R_6+1$

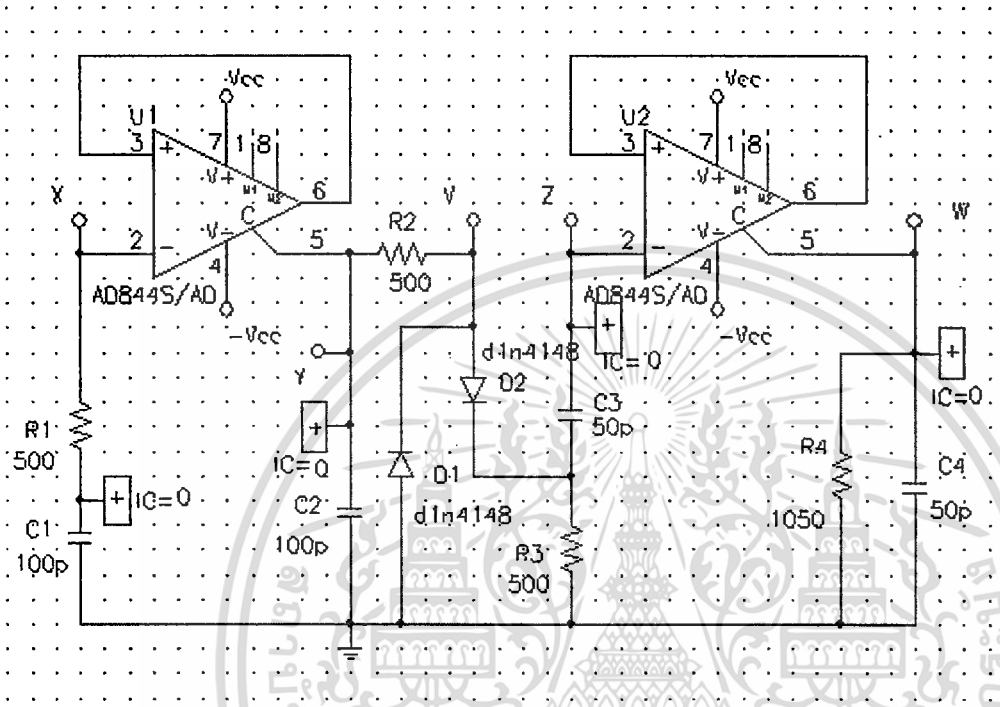
$\mathbf{a} = C_2/C_1$

$\mathbf{b} = R/R_6-1$

โดยเราจะกำหนดค่าของอุปกรณ์อิเล็กทรอนิกส์ได้ดังนี้ $R_1 = R_2 = R = 3.9\ K\Omega$, $R_3 = 3.6\ K\Omega$, $R_4 = 1.2\ K\Omega$, $R_5 = R_7 = 12\ K\Omega$, $R_6 = 1\ K\Omega$, $C_1 = 10$ nF, $C_2 = 15$ nF เพื่อให้ได้ค่าใกล้เคียงกับค่าคงที่ที่เกิดสภาวะอลวน

3.8 วงจร Hyper chaotic oscillator [5]

เป็นวงจรที่สร้างขึ้นมาใช้ในย่านความถี่สูงเช่นเดียวกับวงจร High frequency Wien-type chaotic oscillator [2] แต่ในวงจรนี้แหล่งกำเนิดทั้งสองจะใช้ Op-Amp ในย่านความถี่สูงทั้งสองวงจร

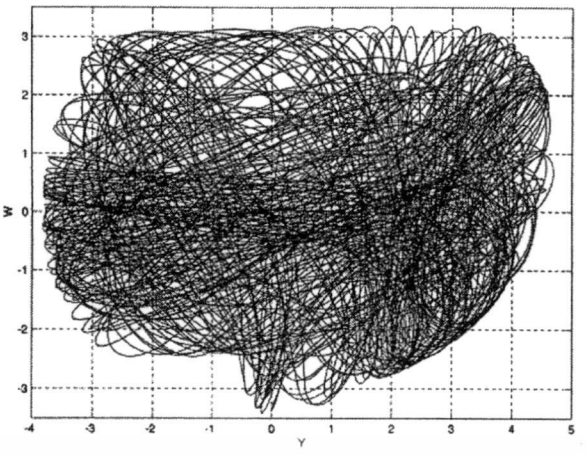


รูปที่ 3-17 ภาพวงจร Hyper chaotic oscillator

โดยวงจรจะมีความสัมพันธ์กับรูปแบบสมการ

$$\begin{bmatrix} 2X' \\ Y' \\ 2Z' \\ W' \\ \varepsilon V' \end{bmatrix} = \begin{bmatrix} -1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -(1+a_1) & 1+a_1 & -a_1 \\ 0 & 0 & -(1+a_1) & 1+a_1+1/k & -a_1 \\ 0 & 1 & -a_1 & a_1 & -(1+a_1+a_2) \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \\ W \\ V \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ a_1 \\ a_1 \\ a_1 - a_2 \end{bmatrix} \quad (8)$$

โดยมี **K**, ε, α เป็นค่าคงที่ซึ่งเมื่อ **K** = 1.7, ε = 0.01, α = 10 จะเกิดสัญญาณอลวนขึ้น และเมื่อพอร์ตด้วย สมการจะได้รูปดังนี้



รูปที่ 3-18 กราฟแสดงผลจากสมการ Hyper chaos ในระนาบ YW

$$\mathbf{K} = R_4/R$$
$$\varepsilon = C_D/C$$
$$\alpha = R/R_D$$

โดยเราจะกำหนดค่าของอุปกรณ์อิเล็กทรอนิกส์ได้ดังนี้ $C_2 = C_4 = C = 50pF$, $C_1 = C_3 = 100pF$, $R_1 = R_2 = R_3 = R = 500\Omega$, $R_4 = 1050\Omega$ เพื่อให้ได้ค่าใกล้เคียงกับค่าคงที่ที่เกิดสภาวะอลวน และใช้ Op-Amp AD844 เพื่อตอบสนองความถี่สูง

3.9 สัญญาณอลวนแบบผีเสื้อหลายปีก

สำหรับการสร้างสัญญาณอลวนแบบผีเสื้อหลายปีกได้ปรับปรุงมาจากวงจรอลวนปีกผีเสื้อของ LUI ซึ่งสมการนี้มีลักษณะคล้ายสมการของ Lorenz แต่ในเทอมที่ไม่เป็นเชิงเส้น สามารถปรับปรับให้มีรูปแบบที่ซับซ้อนได้ง่ายโดยสมการของ LUI แสดงได้คือ

$$\begin{aligned} x' &= -ax + ay \\ y' &= bx - kxz \\ z' &= -cz + hx^2 \end{aligned} \qquad (9)$$

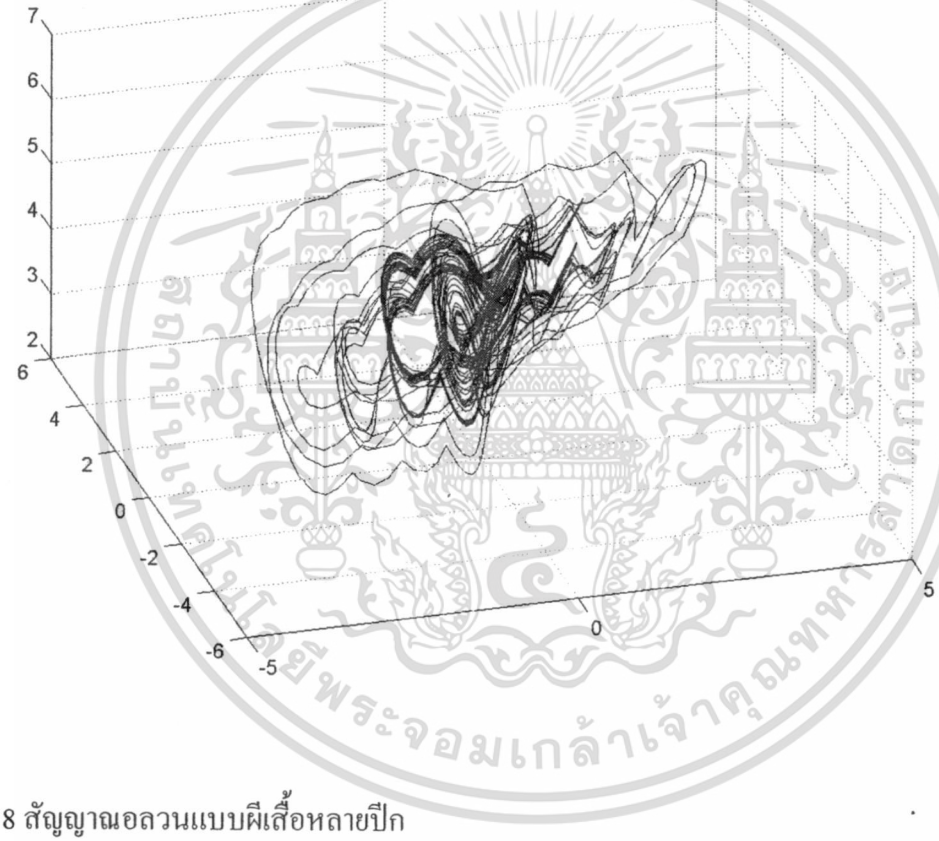
โดยค่า $a = 10, b = 40, c = 2.5, h = 4, k = 1$ เป็นค่าคงที่

ในการเคลื่อนที่ของวงโคจรสัญญาณอลวนระหว่างจุดสมดุลย์สองจุดในมิติ 3 ระนาบ ดังนั้นในการเพิ่มความซับซ้อนของสัญญาณอลวนกระทำได้โดยเพิ่มจุกสมดุลย์ในระบบ หรือปรับปรุงฟังก์ชันไม่เป็นเชิงเส้น x^2 ให้มีค่า f(x) หรือสมการผีเสื้อหลายปีกที่พบใหม่ได้คือ

$$
\begin{aligned}
x' &= -ax + ay \\
y' &= bx - k_1 xz \\
z' &= -cz + hf(x)
\end{aligned}
\qquad (10)
$$

โดยค่า *f(x)* แสดงได้คือ $f(x) = |x| + \sum_{i=1}^{m} \left(1 + \frac{1}{2}\mathrm{sgn}(x-i) - \frac{1}{2}\mathrm{sgn}(x-i)\right)$

โดยในการพิสูจน์ว่าสัญญาณอลวนสามารถกำเนิดได้จริง ได้ทำการทดลองสร้างขึ้นโดยใช้วงจรอิเล็คทรอนิกส์



รูปที่ 3-18 สัญญาณอลวนแบบผีเสื้อหลายปีก

3.10. การสร้างสัญญาณอลวนแบบกำเนิดด้วยคลื่นกระตุ้นหลายปีก

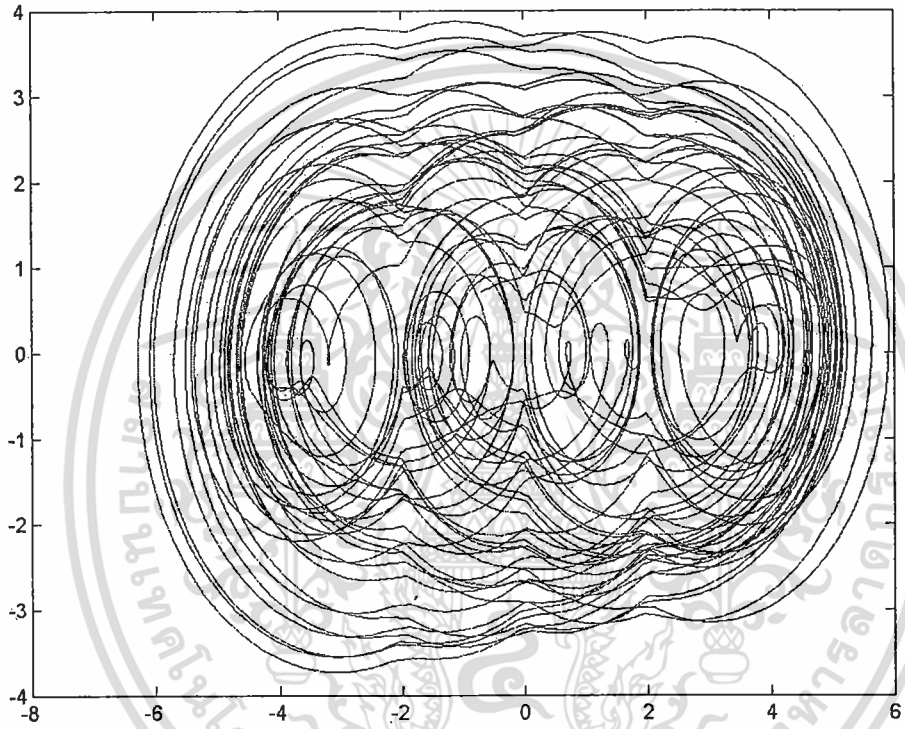
ทำการปรับปรุงจากสมการ

$$
\begin{aligned}
x' &= -ax + by \\
y' &= -x + k \cdot \mathrm{sgn}(x) + A\sin(\omega t)
\end{aligned}
\qquad (11)
$$

ให้มีรูปแบบหลายปีกโดย

$$\begin{aligned} x' &= -ax + by \\ y' &= -x + k \cdot f(x) + A\sin(\omega t) \end{aligned} \qquad (12)$$

โดย $f(x) = \sum_{i=1}^{m} \left(\frac{1}{2}\mathrm{sgn}(x+i) + \frac{1}{2}\mathrm{sgn}(x-i) \right)$



รูปที่ 3-19สัญญาณอลวนแบบกำเนิดด้วยคลื่นกระตุ้นหลายปีก

3.11 การสัญญาณอลวนแบบหลายสกอร์โดยการ Chaotification จากระบบ Van der Pol

เสนอการกำเนิดสัญญาณ เคออสแบบหลายสกอร์โดยอาศัยหลักการ Chaotification ของ Van der Pol ร่วมกับฟังก์ชันเชิงท่อน

สำหรับสมการ Van der Pol แสดงได้

$$\begin{aligned} x' &= y \\ y' &= -x + y - x^2 y \end{aligned} \qquad (13)$$

จัดให้อยู่ในรูปแบบของ Jerk [โดยการเพิ่มสเตท z

$$x' = y$$
$$y' = z$$
$$z' = -x + y - x^2 y \qquad (14)$$

ประมาณเทอม $x^2 \approx |x|$ ทำการ Chaotification เพื่อให้เกิดระบบเป็นเคออส

$$x' = ay + bz$$
$$y' = cz$$
$$z' = -x + y - |x|y \qquad (15)$$

หาจุดสมดุลของระบบโดยให้ $x' = y' = z' = 0$ แล้วจะได้จุดสมดุลจุดเดียวคือ ที่ $P^{\circ} = (0,0,0)$ และค่า Jacobian matrix ของระบบคือ

$$J = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ -1 - \mathrm{sgn}(x) & 1 - |x| & -1 \end{bmatrix} \qquad (16)$$

ดังนั้นค่าสมการคุณสมบัติที่จุดสมดุล P^0 มีค่า

$$\lambda^3 + \lambda^2 + (b - c)\lambda + ac \qquad (17)$$

จากสมการ (15) ระบบเป็นระบบ dissipative

$$\nabla F = \frac{\partial Fx}{\partial x} + \frac{\partial Fy}{\partial y} + \frac{\partial Fz}{\partial z} < -1 \qquad (19)$$

จากเงื่อนไขของ Routh-Hurwitz เพื่อให้ระบบไม่มีเสถียรภาพ ต้องให้ $a. > 0, c > 0, b < 0$ และเพื่อให้แอทแทรกเตอร์เกิดขึ้นหลายสกอร์เราดัดแปลงฟังก์ชัน $|x|$ ให้เป็นฟังก์ชันเชิงท่อน ดังนั้นแสดงระบบ (4)ใหม่คือ

$$x' = ay + bz$$

$$y' = cz$$
$$z' = -x + y - f(x)y \qquad (20)$$

โดย $f(x)$ เป็นฟังก์ชันเชิงท่อนแสดงได้

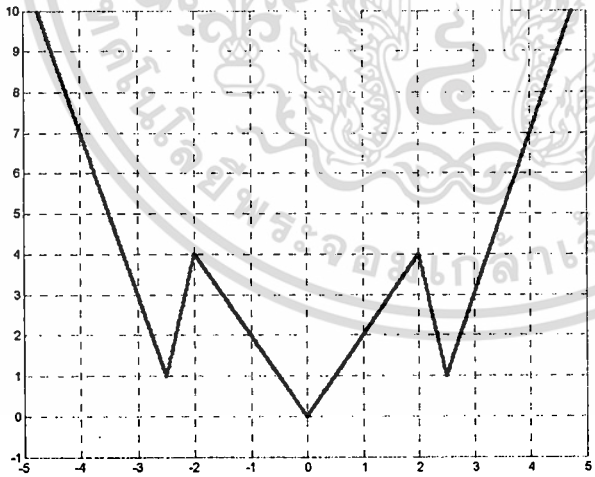
$$f(x) = m_0|x| + \sum_{i=1}^{n} \{-m_{ai}(|x+a_i| + |x-a_i|) + m_{bi}(|x+b_i| - |x-b_i|)\} + k \qquad (21)$$

ค่า n แสดงจำนวนสกอร์ที่เพิ่มขึ้นที่ละคู่โดยตัวอย่างฟังก์ชันเชิงท่อนที่สร้างแอแทรกเตอร์แบบขนาด 4 สกอร์คือ

$$f_1(x) = 2|x| - 4(|x+2| - |x-2|) + 5(|x+2.5| - |x-2.5|) - 9 \qquad (22)$$

โดยแสดงกราฟของฟังก์ชัน $f_1(x)$ ได้ในรูปที่ 1

ให้ $b = -2.6, c = 40$ และ a เป็นค่า Bifurcation โดยค่าเป็นฟังก์ชันเชิงท่อน แสดงดังสมการที่ 22 ค่า Lyapunov ของระบบโดยการปรับค่า a แสดงได้ดังตาราง

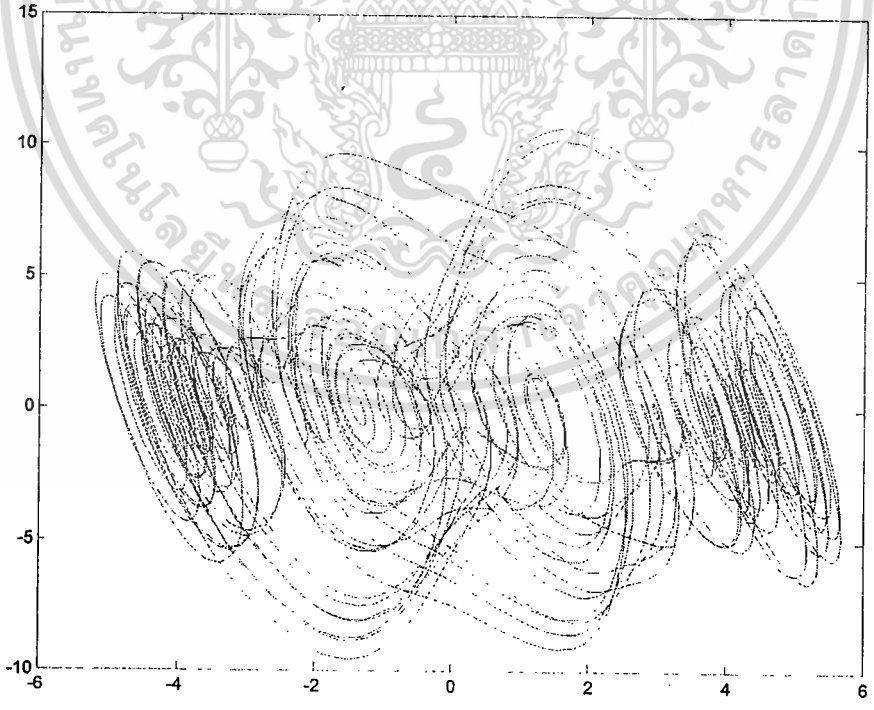


รูปที่ 3.20 ฟังก์ชันเชิงท่อนที่ใช้สร้างแอทแทรกเตอร์ขนาด 4

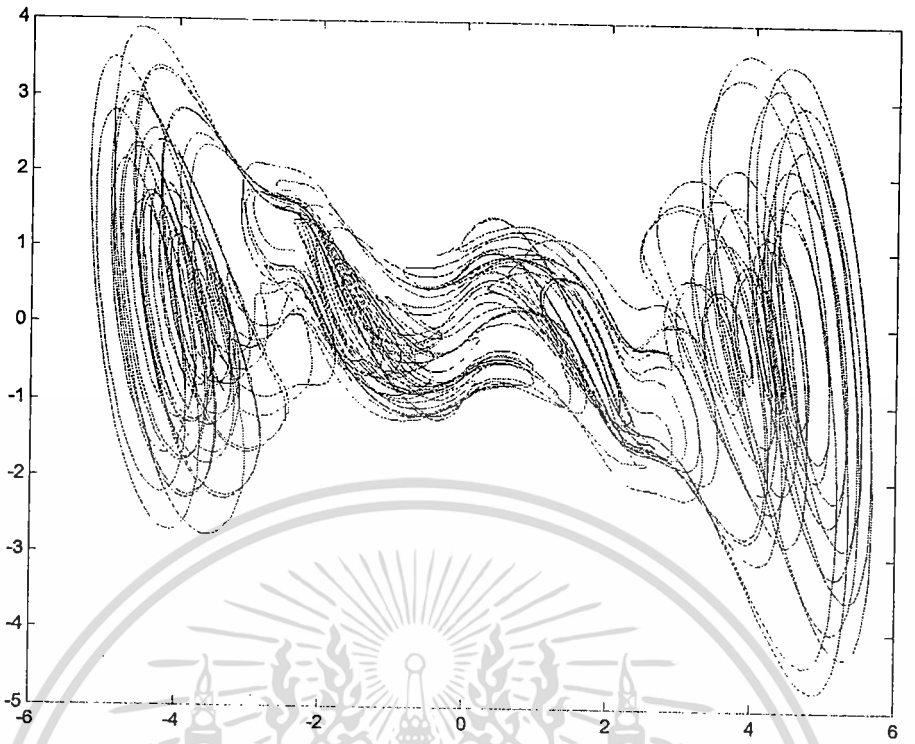
ตารางแสดงค่า Lyapunov exponent เมื่อปรับค่า a

a	λ_1	λ_2	λ_3
1.0	0.555349	0.006062	-1.561817
1.1	0.856586	-0.034182	-1.822688
1.2	0.898078	-0.050844	-1.847504
1.3	0.970703	-0.031014	-1.939922
1.4	1.201645	0.001540	-2.203425
1.5	1.257758	-0.043563	-2.214456
1.6	1.159612	-0.045195	-2.114699
1.7	1.220882	-0.055359	-2.165843
1.8	1.112988	-0.068541	-2.044766
1.9	1.166988	-0.040717	-2.126600
2.0	1.038487	-0.064196	-1.974613

ผลของการจำลองระบบ (8) โดยโปรแกรม MATLAB พารามิเตอร์ $a = 1.2, b = -2.6, c = 40$

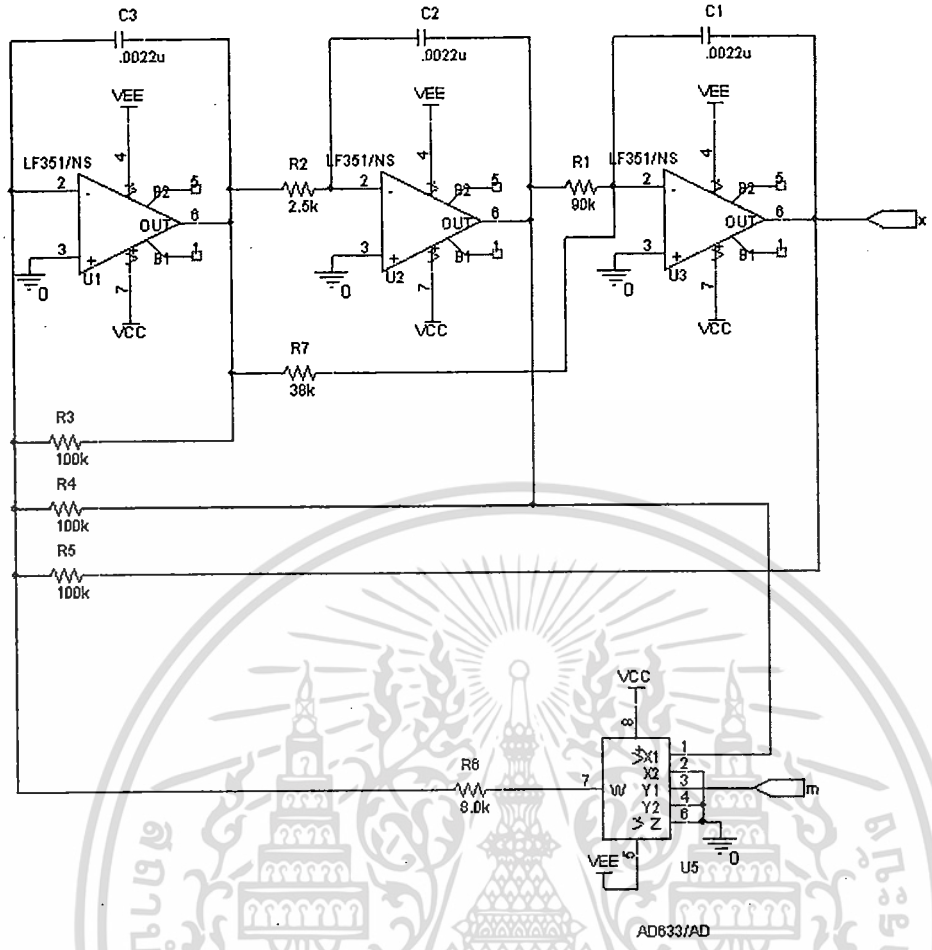


รูปที่ 3.21 พฤติกรรมของระบบในระนาบ x-y

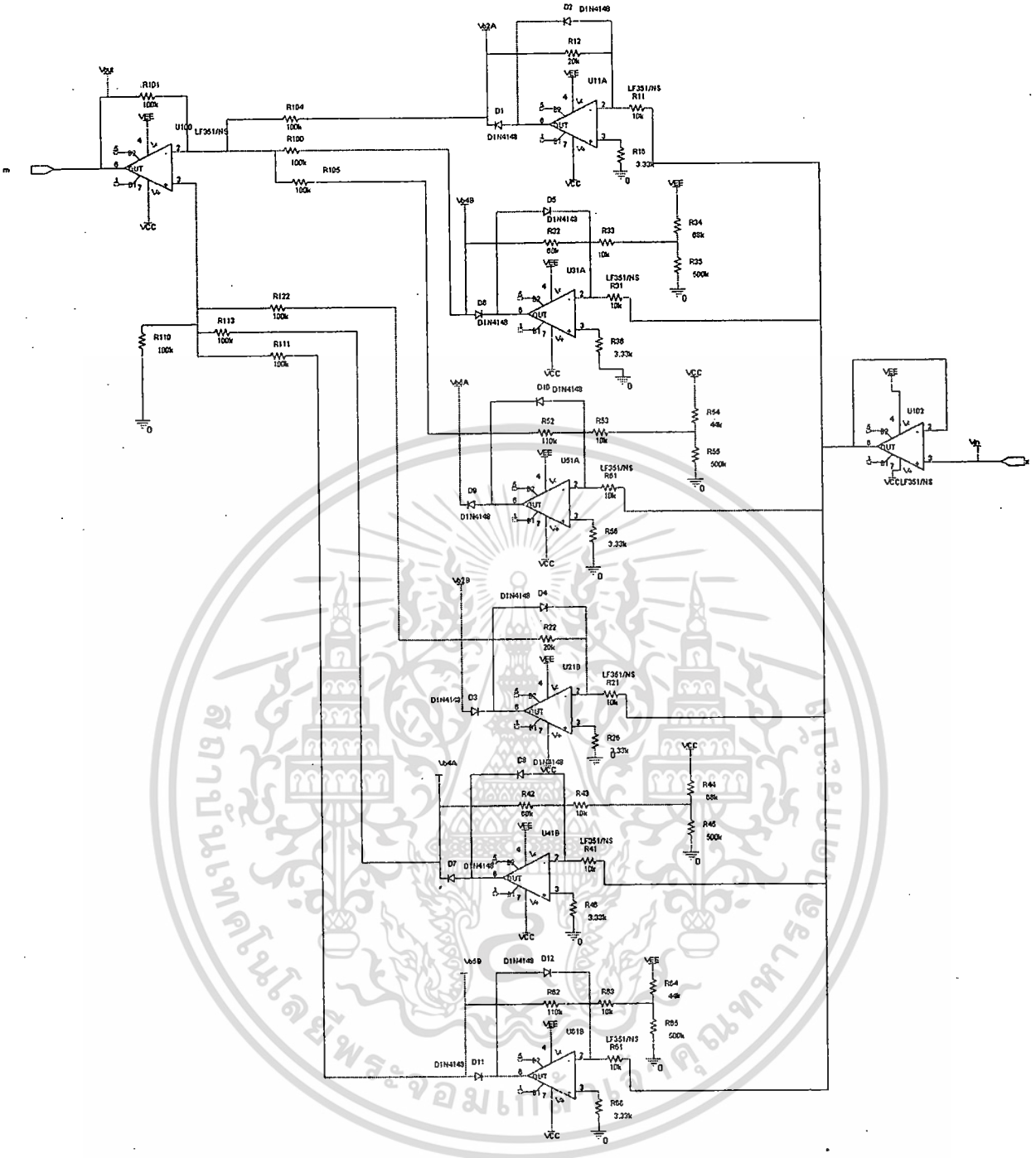


รูปที่ 3.22 พฤติกรรมของระบบในระนาบ x-z

การสร้างวงจรในทางปฏิบัติสำหรับวงจรอินทีเกรท ใช้วงจร Inverting-Integrator โดยวงจรคูณกระทำได้โดยใช้ AD633 ค่าของ a,b และ c ปรับที่ความต้านทาน R1,R7 และ R2 ตามลำดับ สำหรับสร้างวงจร PWL ดังรูป 3.24 โดยแต่ละท่อนของกราฟในรูปที่ 3.22 สร้างจากวงจร Half wave-rectify โดยขนาดความชันของฟังก์ชันกระทำได้โดยปรับอัตราการขยายของ Op-Amp โดยที่ความชันขนาด -4 จะเกิดจากอัตราความชันขนาด 2 และ -6 และความชันขนาด 5 เกิดจากความชันขนาด 11 และ -6



รูปที่ 3.23 วงจรส่วน Integrator และวงจรคูณ



รูปที่ 3.24 วงจรส่วนฟังชันเชิงท่อน

ผลของการจำลองการทำงานของวงจรโปรแกรมด้วย PSpice และรูปของสัญญาณที่สร้างจากการวัดระนาบ x-z ในทางปฏิบัติที่พารามิเตอร์ $a = 1.2, b = -2.6, c = 40$ ดังรูปที่ 4 และ 5 ตามลำดับ

บทที่ 4

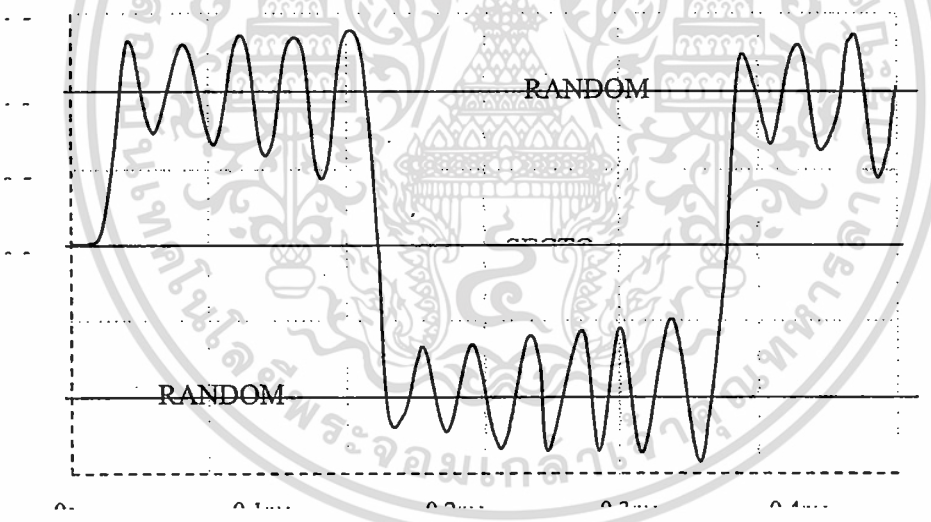
การออกแบบวงจรกำเนิดบิตสุ่ม (Random bit source)

การออกแบบวงจรที่ใช้ในการสร้างบิตสุ่ม จะมีสัญญาณอยู่สองลักษณะคือมีการแบ่งช่วงและไม่มีการแบ่งช่วง การออกแบบวงจรจึงต้องทำเป็นสองลักษณะ

4.1 วงจรกำเนิดบิตสุ่มของสัญญาณที่มีการแบ่งช่วง

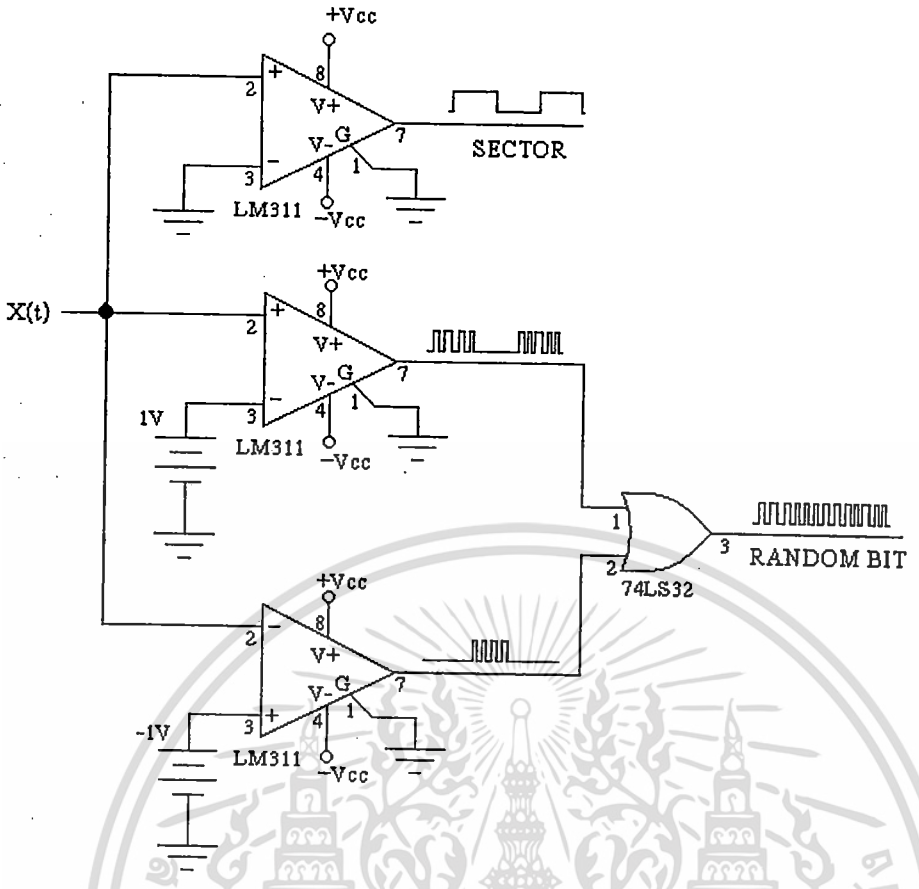
การ Sampling สัญญาณจะมีอยู่ 2 ส่วนคือ

-ส่วนของการสร้างบิตสุ่ม จะทำการเปรียบเทียบสัญญาณในระดับที่เกิดคุณสมบัติสุ่มขึ้น โดยในสัญญาณลักษณะนี้จะต้องเปรียบเทียบสัญญาณ 2 ระดับ โดยถ้าดูในตัวอย่างสัญญาณรูปที่3-9 คือต้องทำการเปรียบเทียบในระดับ 1 V และ -1 V แล้วนำมารวมกัน -ส่วนของการแบ่งช่วง โดยจะทำการเปรียบเทียบสัญญาณในระดับ 0V ก็จะได้ช่วงของสัญญาณอลวน



รูปที่ 4.1 ภาพการ Sampling สัญญาณอลวนที่มีการแบ่งช่วง

จากหลักการข้างต้นนำมาออกแบบวงจรโดยใช้วงจรเปรียบเทียบแรงดันในการตัดสัญญาณอลวน ใน 3 ระดับและในส่วนการนำสัญญาณมารวมกันจะใช้ไอซีTTL 74LS32 จะได้ดังนี้



รูปที่ 4.2 ภาพวงจรกำเนิดบิตสุ่มของสัญญาณที่มีการแบ่งช่วง

X(t) คือ สัญญาณอลวน

SECTOR คือ สัญญาณดิจิตอลที่ใช้ในการแบ่งช่วงของBit sequence โดยในแต่ละช่วงจะมีจำนวนบิตสุ่มที่ไม่แน่นอน

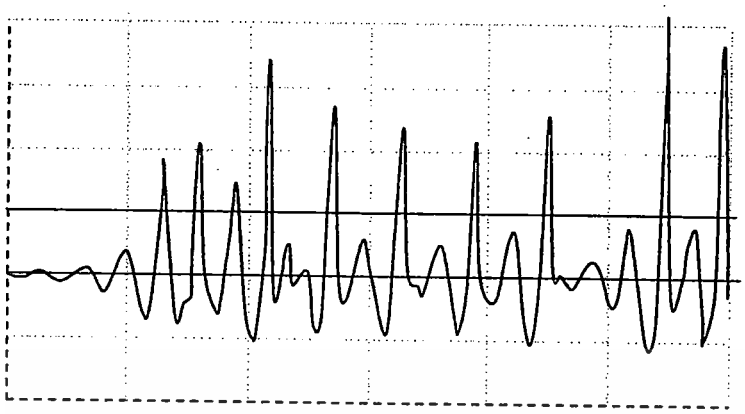
RANDOM BIT คือ บิตสุ่มที่ได้จากการเปรียบเทียบสัญญาณในสภาวะสุ่มของสัญญาณอลวน

4.2 วงจรกำเนิดบิตสุ่มของสัญญาณที่ไม่มีการแบ่งช่วง

การ Sampling สัญญาณจะมีอยู่ 2 ส่วนคือ

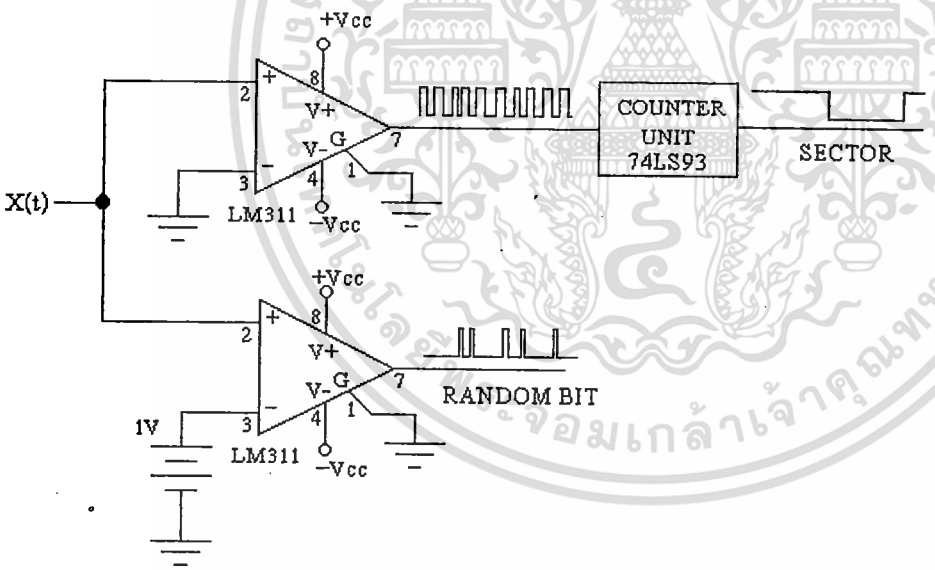
-ส่วนของการสร้างบิตสุ่ม จะทำการเปรียบเทียบสัญญาณในระดับที่เกิดคุณสมบัติสุ่มขึ้น

-ส่วนของการแบ่งช่วง โดยจะทำการเปรียบเทียบสัญญาณในระดับที่เกิดลูกคลื่นมากที่สุด และในส่วนนี้เมื่อทำการ Sampling แล้วจะต้องใช้วงจรนับ เพื่อช่วยขยายช่วงในการกำหนดค่าบิตของบิตสุ่ม



รูปที่ 4.3 ภาพการ Sampling สัญญาณอลวนที่ไม่มีการแบ่งช่วง

จากหลักการข้างต้นนำมาออกแบบวงจรโดยใช้วงจรเปรียบเทียบแรงดันในการตัดสัญญาณอลวน ใน 2 ระดับและในส่วนการแบ่งช่วงสัญญาณจะใช้ไอซีTTL 74LS93 ซึ่งเป็นวงจรนับเพื่อนำพัลส์ที่ได้จากการเปรียบเทียบแรงดันในระดับ 0 V จำนวน 8 ลูกในการแบ่งช่วงหนึ่งช่วง



รูปที่ 4.4 ภาพวงจรกำเนิดบิตสุ่มของสัญญาณที่ไม่มีการแบ่งช่วง

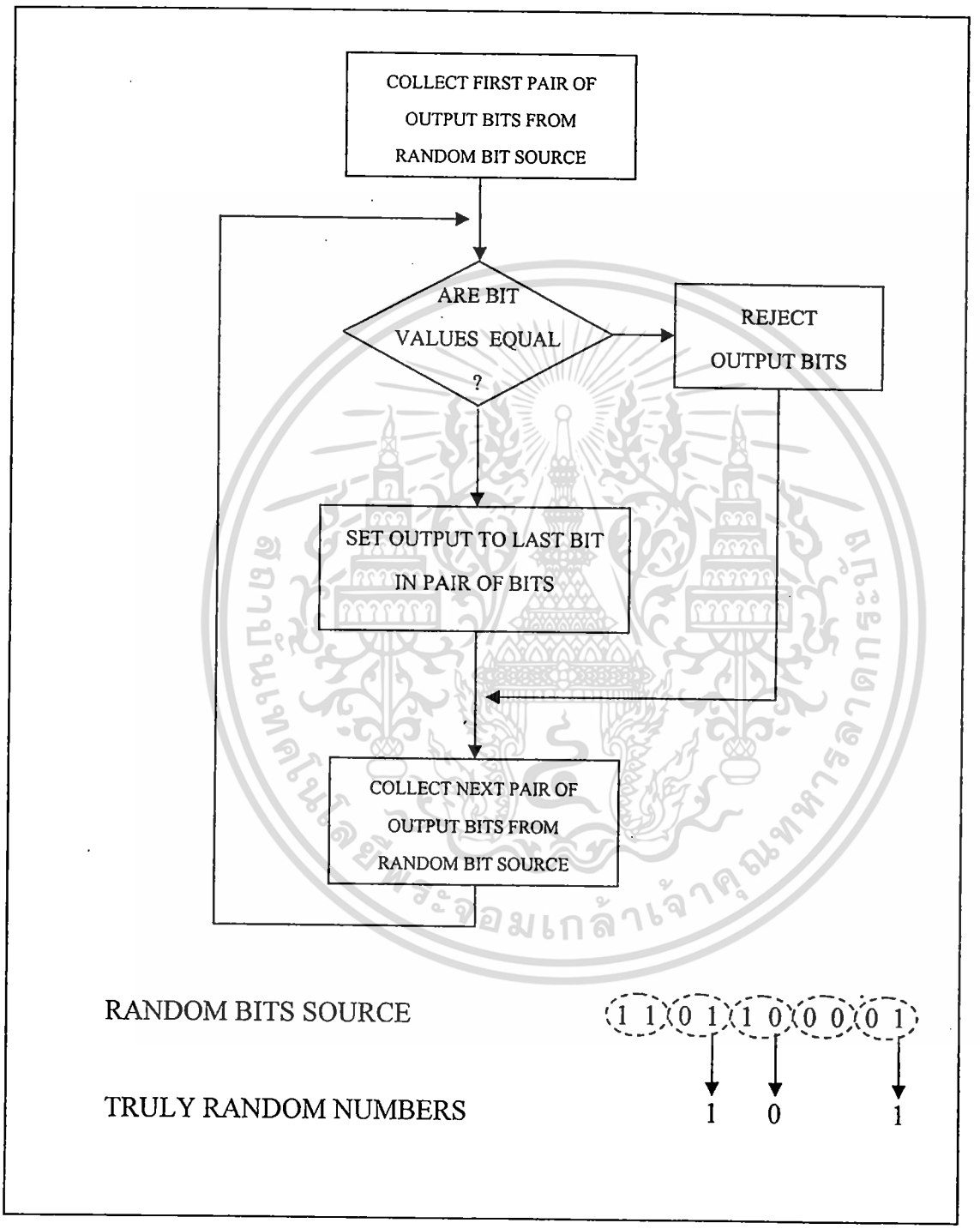
X(t) คือ สัญญาณอลวน

SECTOR คือ สัญญาณดิจิตอลที่ใช้ในการแบ่งช่วงของBit sequence โดยในแต่ละช่วงจะมีจำนวนบิตสุ่มที่ไม่แน่นอน

RANDOM BIT คือ บิตสุ่มที่ได้จากการเปรียบเทียบสัญญาณในสภาวะสุ่มของสัญญาณอลวน

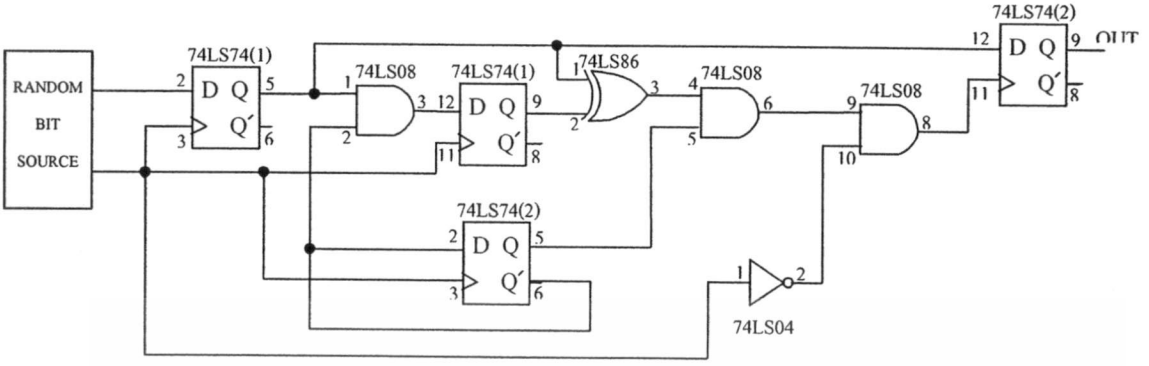
4.3 การออกแบบวงจรเลือกค่าสุ่มจริง

การออกแบบวงจรเลือกค่าสุ่มจริงในโครงงานนี้เราจะใช้หลักการของวอนนูแมน(Von neumanns technique) เมื่อนำหลักการของ วอนนูแมนมาเขียนเป็น Block Diagram จะได้ดังนี้



รูปที่ 4.5 Block Diagram ตามหลักการของ วอนนูแมน(Von neumanns technique)

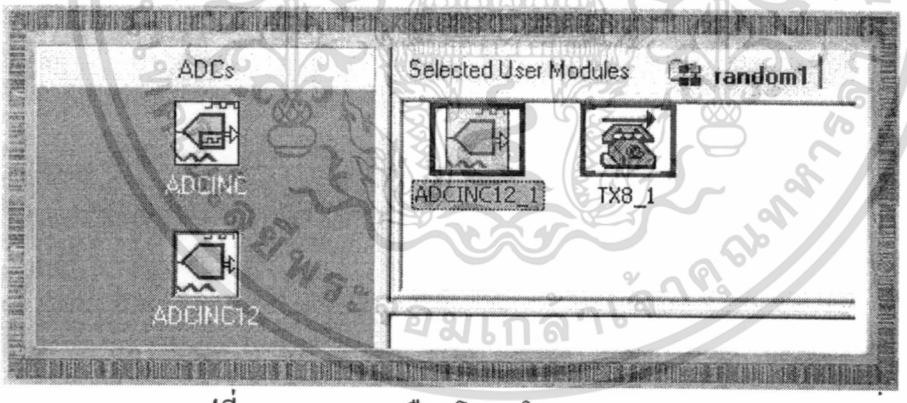
เมื่อออกแบบวงจรตามBlock Diagram จะได้วงจรดังนี้



รูปที่ 4.6 ภาพวงจรตามหลักการของ วอนนูแมน(Von neumanns technique)

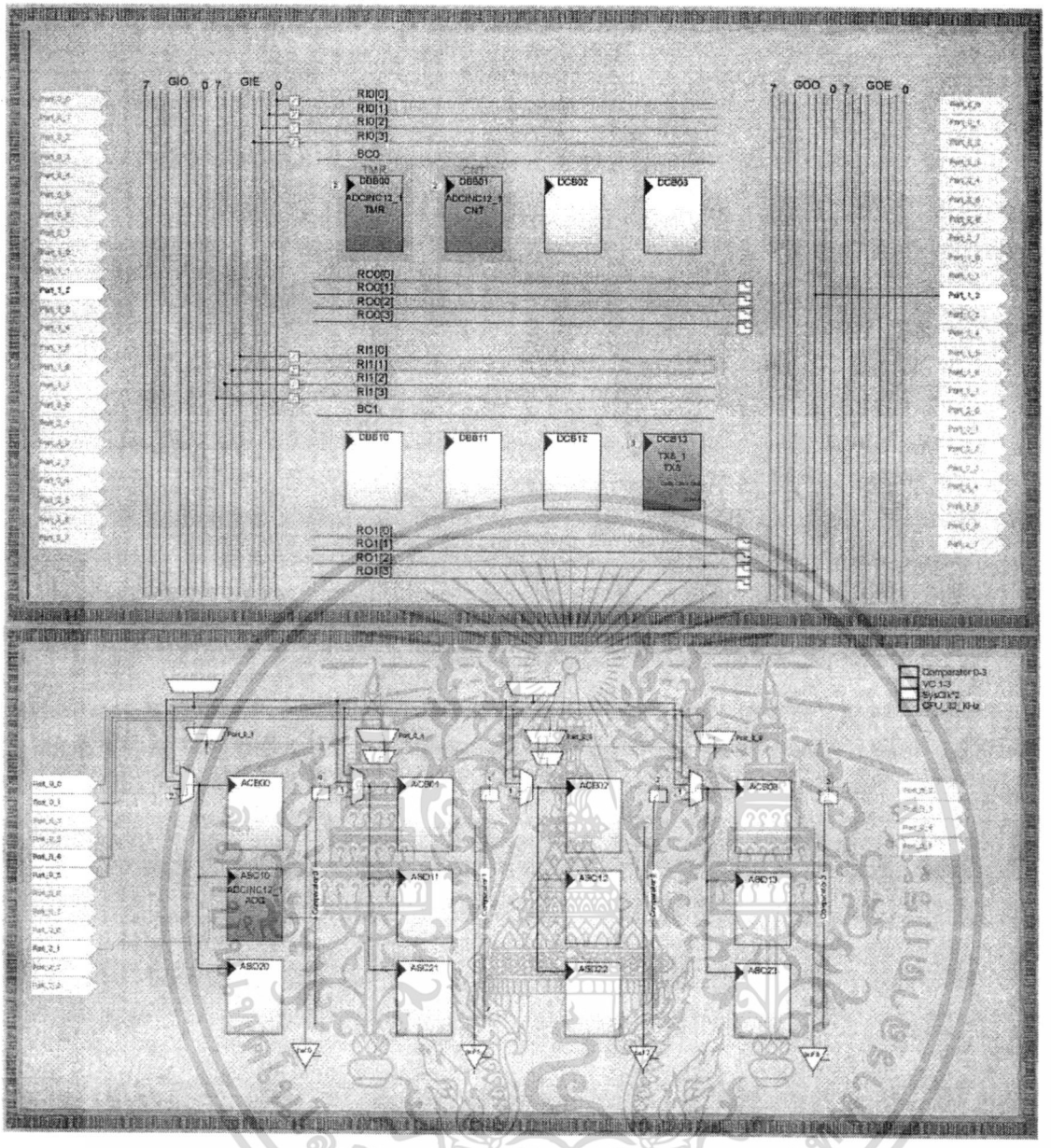
4.4 การออกแบบวงจรลงบน PSOC

1 เลือกโมดูลภายใน Psoc Designer ทำการเลือก ADINC12_1 เพื่อแปลงสัญญาณอนาล็อกเป็นดิจิตอล และเลือก TX8_1 เพื่อส่งออกผ่าน พอร์ต RS232 โดยเป็นการส่งค่าออกเพียงอย่างเดียว

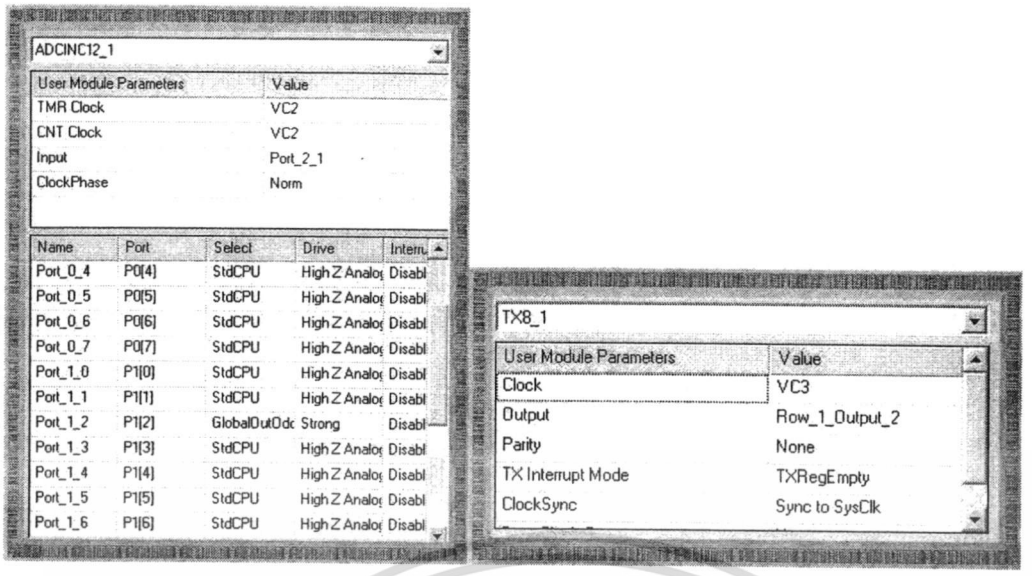


รูปที่ 4.7 แสดงการเลือกโมดูลในPsoc Designer

2 ทำการวางโมดูลแล้วเซ็ตค่าต่างๆ ดังแสดงในรูปที่4.5 และ4.6

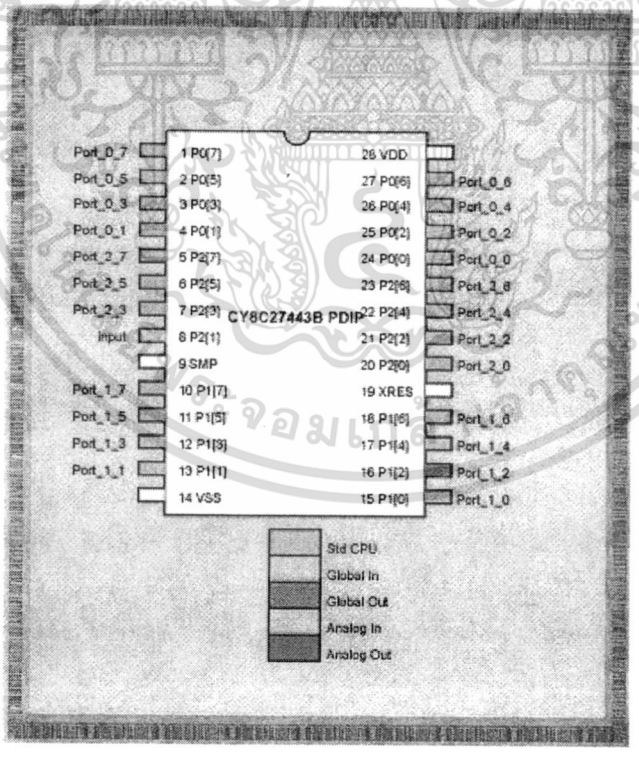


รูปที่4.8 แสดงการวางโมดูลใน Psoc Designer



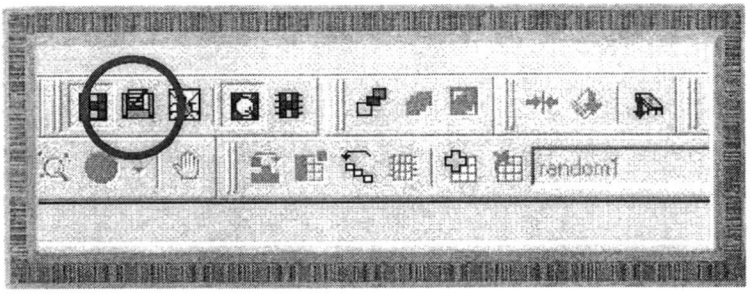
รูปที่4.9 แสดงการเซ็ตค่าของโมดูลต่างๆใน Psoc Designer

3 ตรวจสอบอินพุตและเอาท์พุตโดยสีเขียวแทนสัญญาณอินพุตแบบอนาล็อก ที่ขา 8 P2[1] และ เอาพุตที่ ขา 16 P1



รูปที่4.10 แสดงการแบ่งสีเพื่อบอกการทำงานของพอร์ตต่างๆ

4 ทำการเขียนโปรแกรมโดยเลือกที่สัญลักษณ์ดังภาพที่ 4.11



รูปที่4.11 แสดงสัญลักษณ์ในการเขียนโปรแกรม

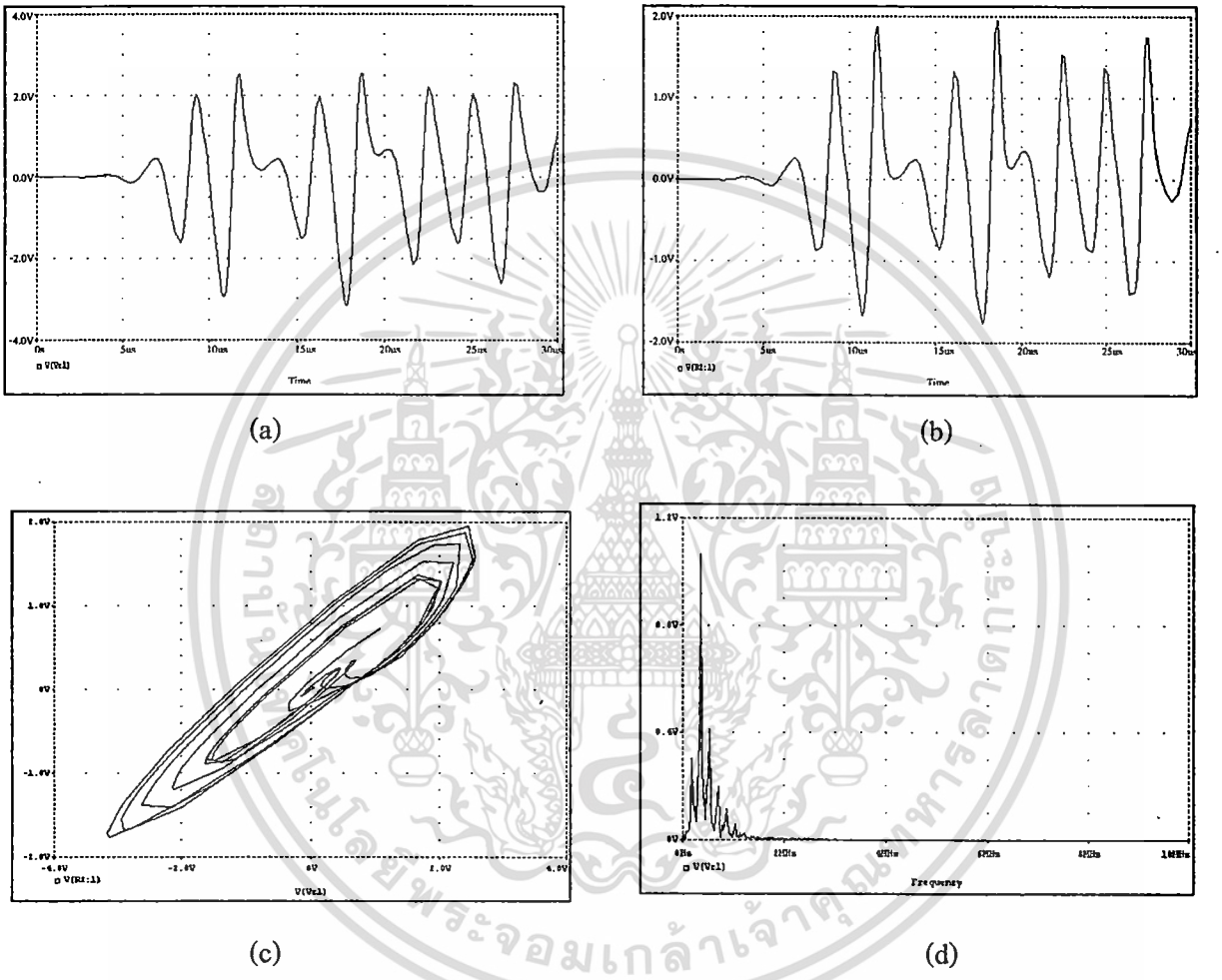
5 ทำการเบิร์นลง Psoc

บทที่ 5

ผลการทดลอง

5.1 ผลการจำลองวงจรอลวนกับโปรแกรม PSPICE

5.1.1 ผลที่ได้จากวงจร High frequency Wien-type chaotic oscillator [2]



(a) (b)

(c) (d)

รูปที่ 5-1 สัญญาณจากโปรแกรม PSPICE ของวงจร High frequency Wien-type chaotic oscillator [2]

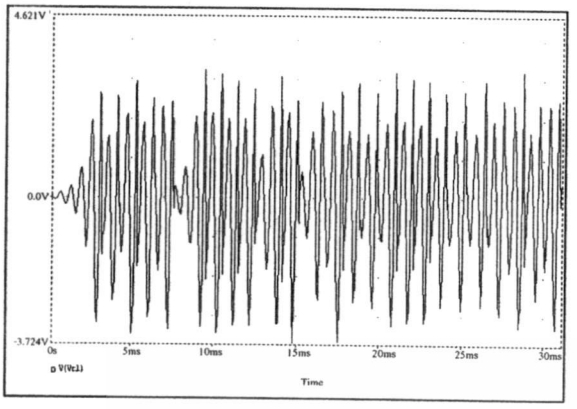
(a) แสดงระนาบ X เทียบกับเวลา

(b) แสดงระนาบ Y เทียบกับเวลา

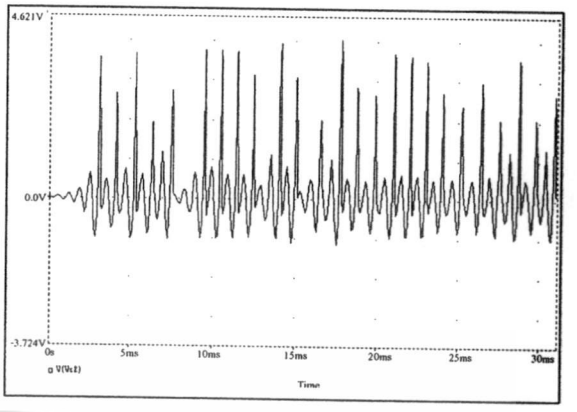
(c) แสดงระนาบ XY

(d) แสดงspectrum ของสัญญาณ

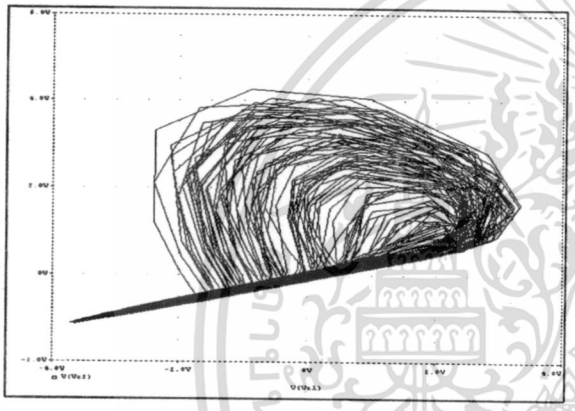
5.1.2 ผลที่ได้จากวงจร Simple RC chaotic oscillator [3]



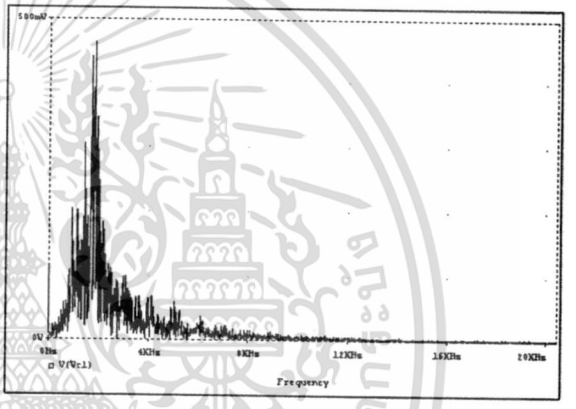
(a)



(b)



(c)



(d)

รูปที่ 5-2 สัญญาณจากโปรแกรม PSPICE ของวงจร Simple RC chaotic oscillator [3]

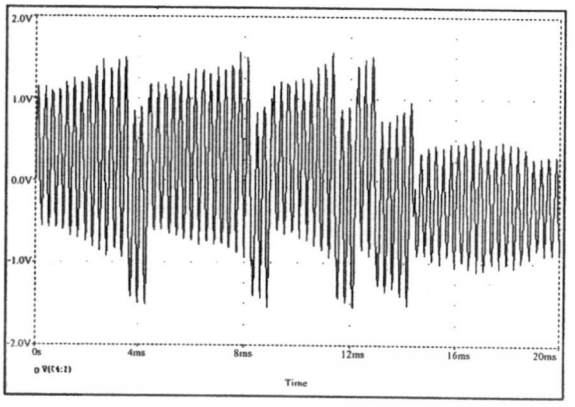
(a) แสดงระนาบ X เทียบกับเวลา

(b) แสดงระนาบ Y เทียบกับเวลา

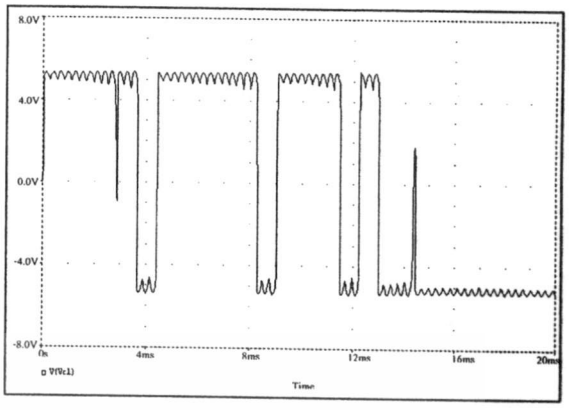
(c) แสดงระนาบ XY

(d)แสดงspectrum ของสัญญาณ

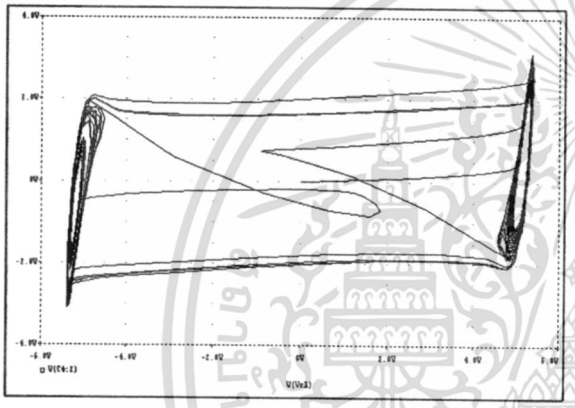
5.1.3 ผลที่ได้จากวงจร Double scroll in a simple '2D' chaotic oscillator [4]



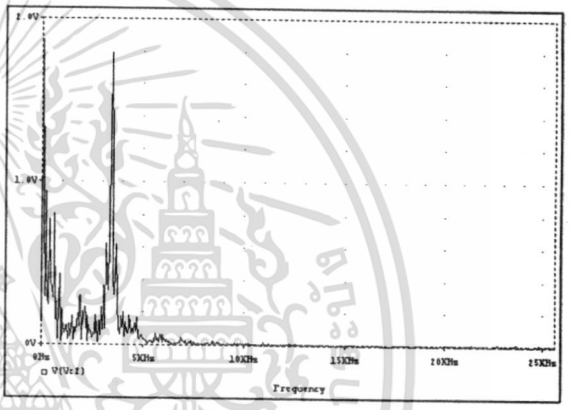
(a)



(b)



(c)



(d)

รูปที่ 5-3 ภาพสัญญาณจากโปรแกรม PSPICE ของวงจร Double scroll in a simple '2D' chaotic oscillator [4]

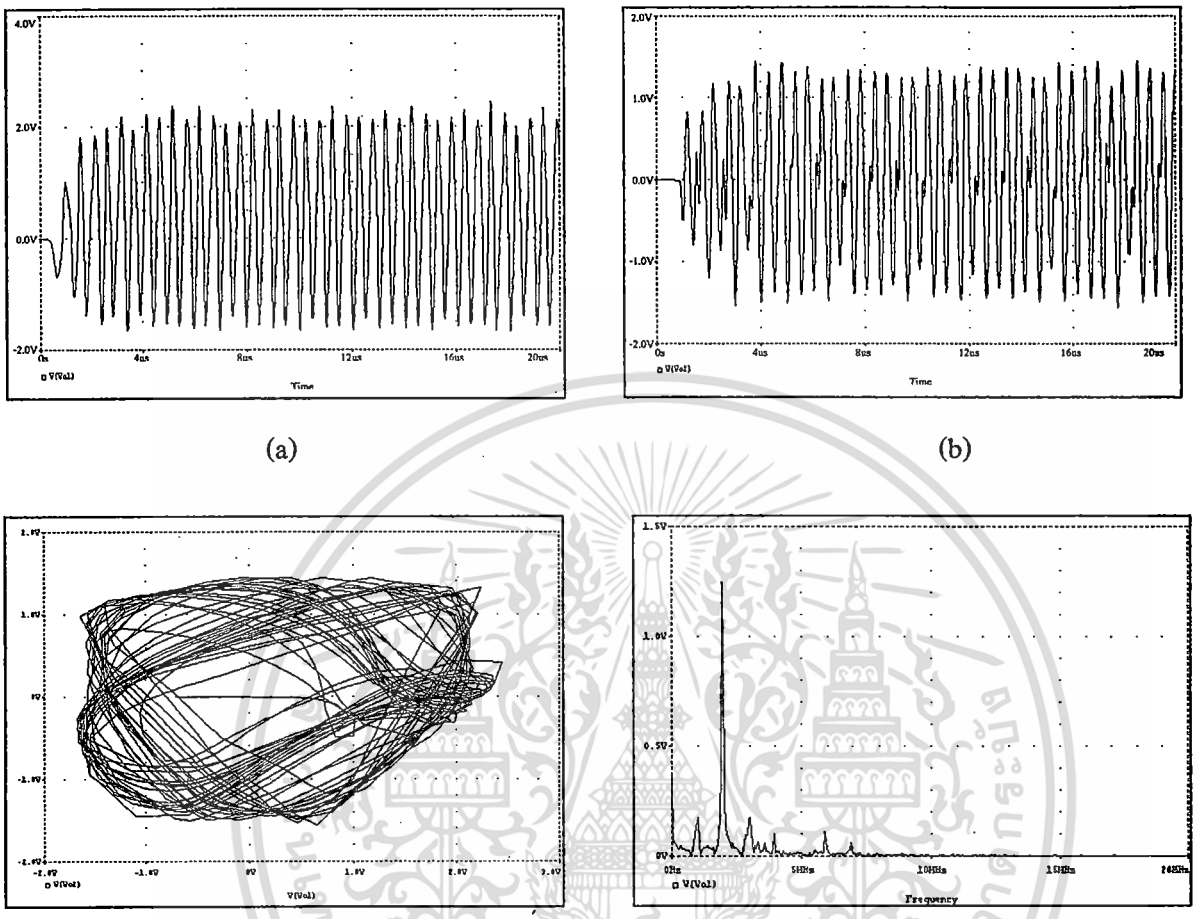
(a) แสดงระนาบ X เทียบกับเวลา

(b) แสดงระนาบ Y เทียบกับเวลา

(c) แสดงระนาบ XY

(d) แสดงspectrum ของสัญญาณ

5.1.4 ผลที่ได้จากวงจร Hyper chaotic oscillator [5]



(a) (b)

(c) (d)

รูปที่ 5-4 ภาพสัญญาณจากโปรแกรม PSPICE ของวงจร Hyper chaotic oscillator [5]

(a) แสดงระนาบ X เทียบกับเวลา

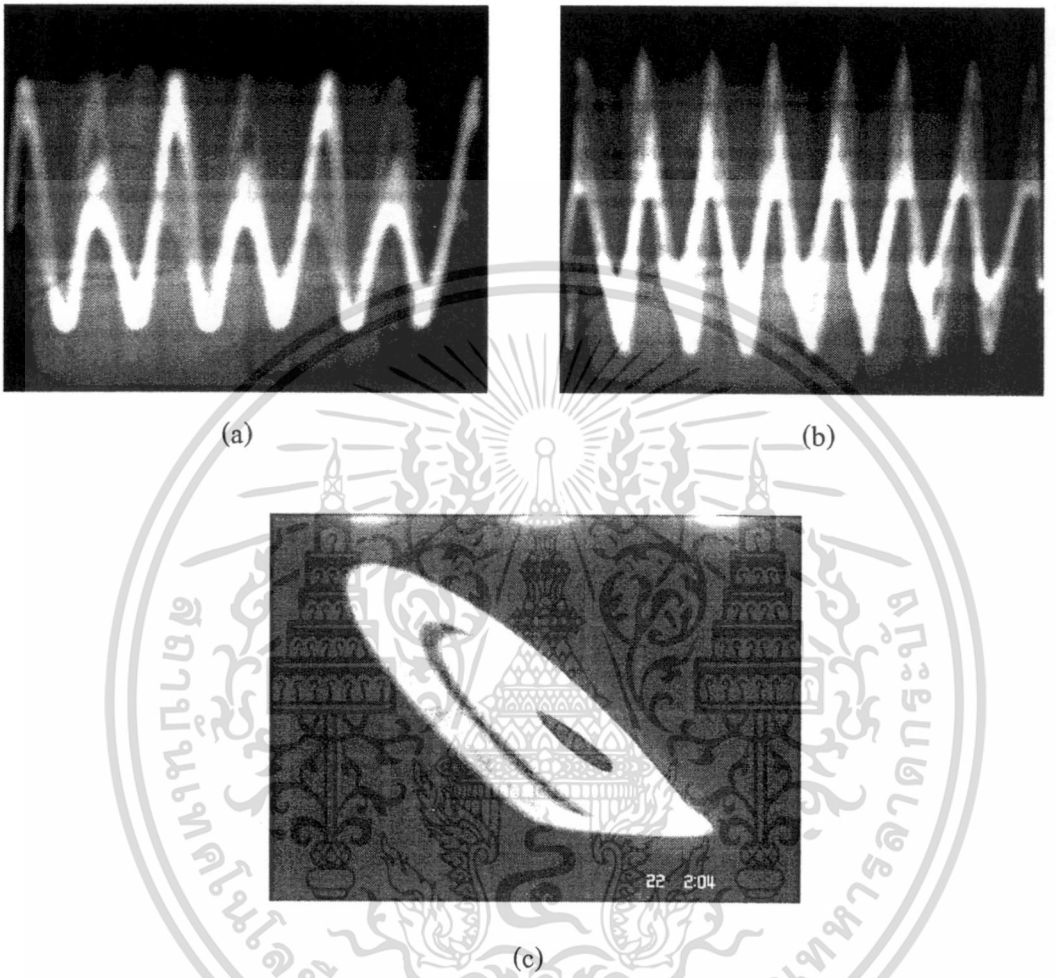
(b) แสดงระนาบ Y เทียบกับเวลา

(c) แสดงระนาบ XY

(d) แสดงspectrum ของสัญญาณ

5.2 ผลจากการต่อวงจรอลวนวัดโดยสโคป

5.2.1 ผลจากการต่อวงจร High frequency Wien-type chaotic oscillator [2]



(a) (b)

(c)

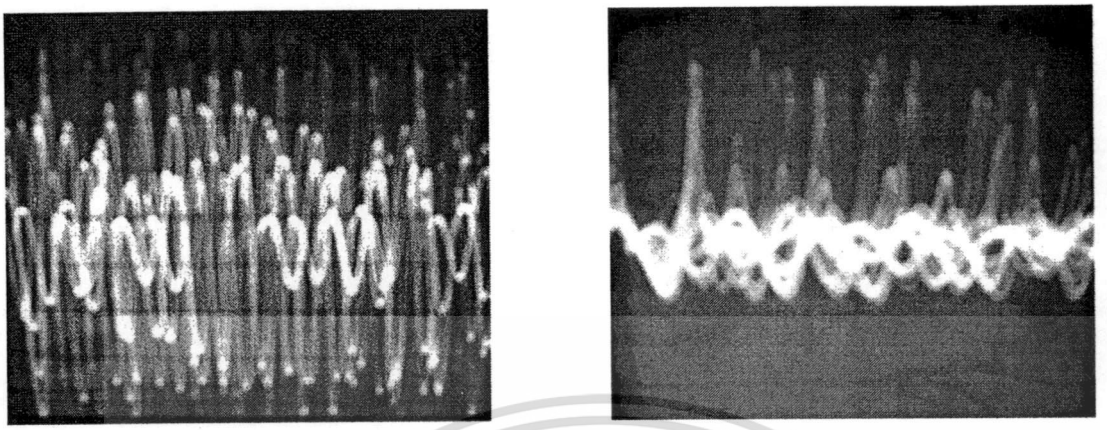
รูปที่ 5-5 ภาพสัญญาณวัดจากสโคป ของวงจร High frequency Wien-type chaotic oscillator [2]

(a) แสดงระนาบ X เทียบกับเวลา (1us/div, 1v/div)

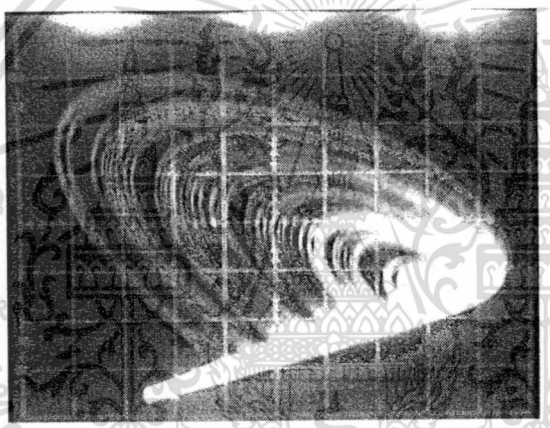
(b) แสดงระนาบ Y เทียบกับเวลา (1us/div, 0.5v/div)

(c) แสดงระนาบ XY

5.2.2 ผลจากการต่อวงจร Simple RC chaotic oscillator [3]



(a) (b)



(c)

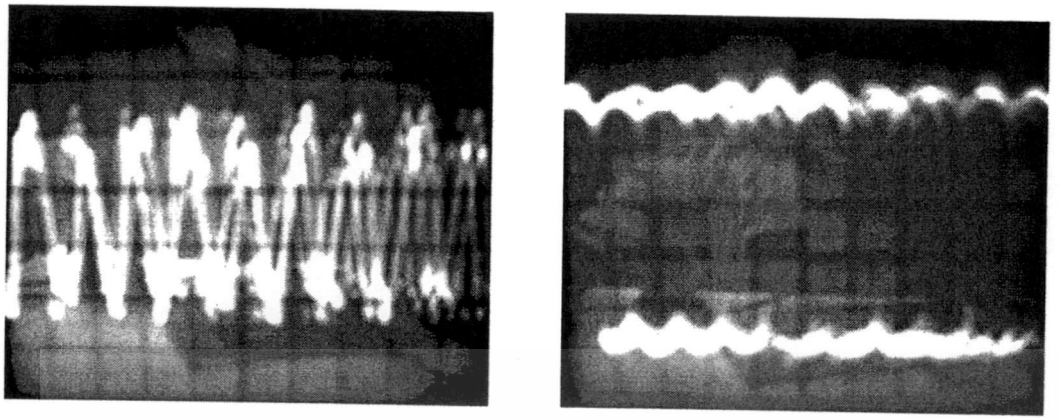
รูปที่ 5-6 ภาพสัญญาณวัดจากสโคป ของวงจร Simple RC chaotic oscillator [3]

(a) แสดงระนาบ X เทียบกับเวลา (5ms/div, 1v/div)

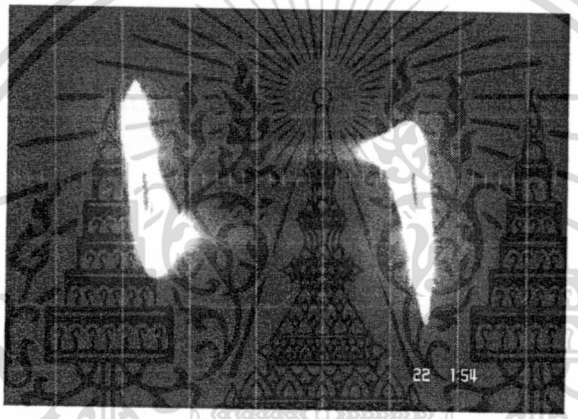
(b) แสดงระนาบ Y เทียบกับเวลา (2ms/div, 1v/div)

(c) แสดงระนาบ XY

5.2.3 ผลจากการต่อวงจร Double scroll in a simple '2D' chaotic oscillator [4]



(a) (b)



(c)

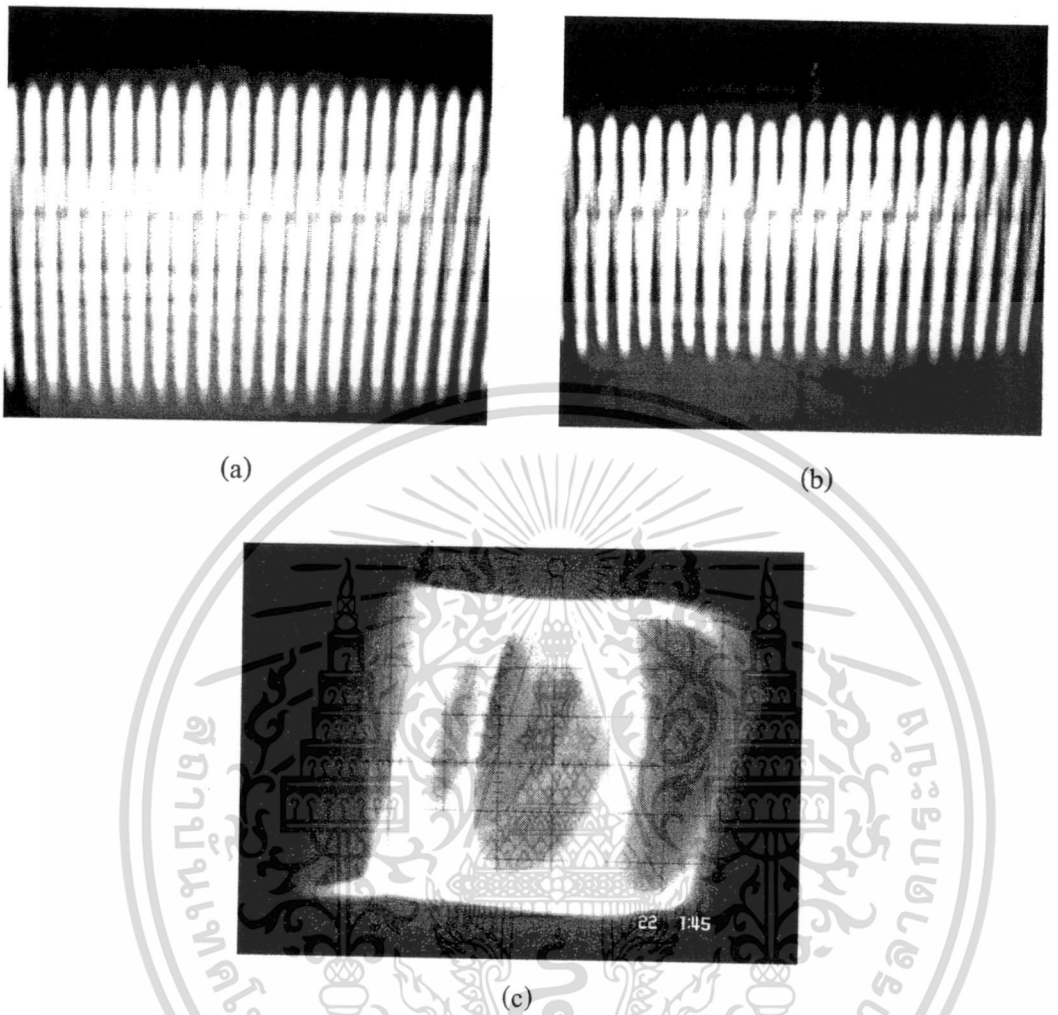
รูปที่ 5-7 สัญญาณวัดจากสโคป ของวงจร Double scroll in a simple '2D' chaotic oscillator

(a) แสดงระนาบ X เทียบกับเวลา (1ms/div, 1v/div)

(b) แสดงระนาบ Y เทียบกับเวลา (1ms/div, 1v/div)

(c) แสดงระนาบ XY

5.2.4 ผลจากวงจร Hyper chaotic oscillator [5]



(a) (b)

(c)

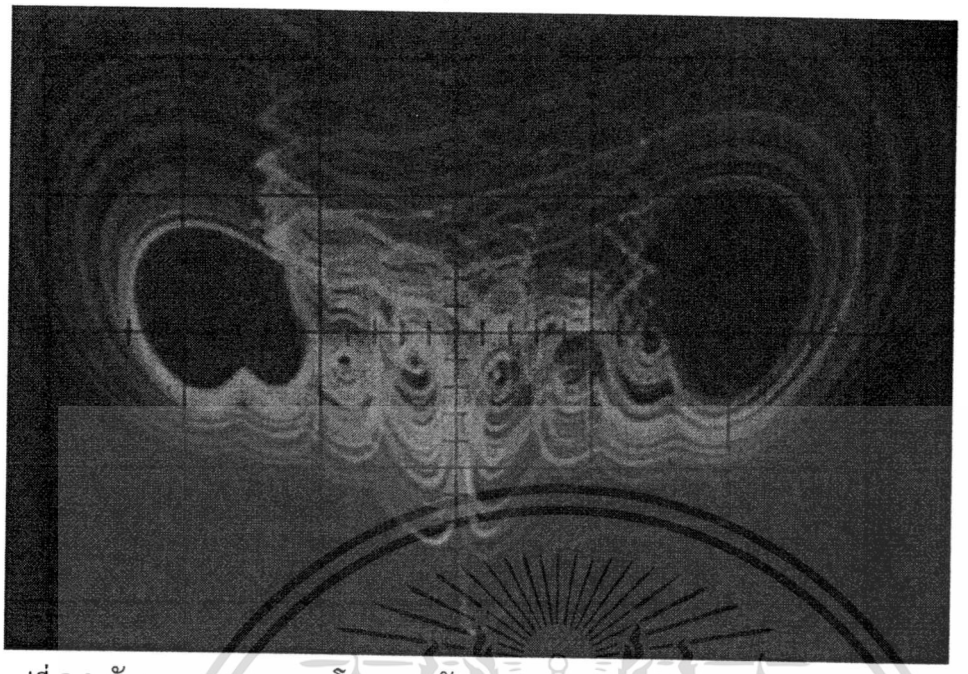
รูปที่ 5-8 สัญญาณวัดจากสโคป ของวงจร Hyper chaotic oscillator [5]

(a) แสดงระนาบ X เทียบกับเวลา (1us/div, 1 v/div)

(b) แสดงระนาบ Y เทียบกับเวลา (1us/div, 1v/div)

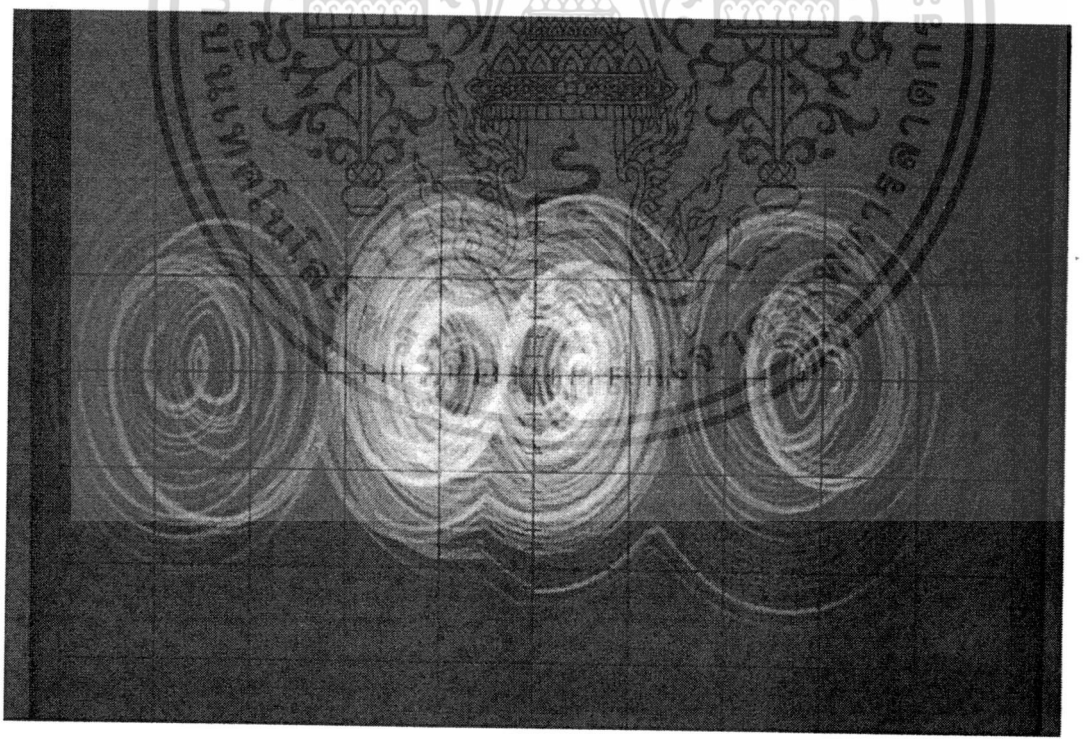
(c) แสดงระนาบ XY

5.2.5 ผลจากวงจรอลวนแบบผีเสื้อหลายปีก(3.9)



รูปที่ 5.9 สัญญาณจากวงจรโดยแรงดันแกน X-Z

5.2.6 ผลจากวงจรสัญญาณอลวนแบบกำเนิดด้วยคลื่นกระตุ้นหลายปีก(3.10)



รูปที่ 5.10 สัญญาณจากวงจรโดยแรงดันแกน x-y

ผลลัพธ์การทดสอบมาตรฐาน FIPS 140-1

การที่จะผ่านการทดสอบได้นั้นค่าบิตสุ่มจะต้องผ่านกฎทั้ง 4 ข้อ ซึ่งได้อธิบายไปแล้ว ผลลัพธ์ที่ได้เป็นดังนี้

Circuits	Monobit Test 9654<N<10346	Poker Test 1.03<X<57.4	Runs Test		Long Run Test < 34
High frequency Wien-type chaotic oscillator [2]	N=10,132	X=62.849	B_1=2,472 B_2=1,348 B_3=668 B_4=297 B_5=166 B_{6+}=80	G_1=2,495 G_2=1,289 G_3=642 G_4=285 G_5=152 G_{6+}=76	No long run
Passed Test?	Pass	Fail	Fail		Pass

Circuits	Monobit Test 9654<N<10346	Poker Test 1.03<X<57.4	Runs Test		Long Run Test < 34
Simple RC chaotic oscillator [3]	N=10,079	X=12.6512	B_1=2,512 B_2=1,208 B_3=500 B_4=380 B_5=155 B_{6+}=128	G_1=2,457 G_2=1,162 G_3=688 G_4=322 G_5=158 G_{6+}=177	No long run
Passed Test?	Pass	Pass	Fail		Pass
Double scroll in a simple '2D' chaotic oscillator [4]	N=10,069	X=12.1088	B_1=2,584 B_2=1,222 B_3=574 B_4=330 B_5=170 B_{6+}=143	G_1=2,410 G_2=1,261 G_3=623 G_4=312 G_5=150 G_{6+}=166	No long run

Passed Test?	Pass	Pass	Pass		Pass
Hyper chaotic oscillator [5]	N=9,998	X=37.234	B_1=2,502 B_2=1,358 B_3=633 B_4=293 B_5=137 B_{6+}=147	G_1=2,474 G_2=1,234 G_3=664 G_4=299 G_5=141 G_{6+}=134	No long run
Passed Test?	Pass	Pass	Pass		Pass

Multi-wing buffterfly attractor	N=	X=47.2548	B_1=2,568 B_2=1,758 B_3=523 B_4=295 B_5=147 B_{6+}=145	G_1=2,774 G_2=1,654 G_3=686 G_4=299 G_5=181 G_{6+}=164	No long run
Passed Test?	Pass	Pass	Pass		Pass

Nonautonomous MScroll	N=	X=12.688	B_1=2,512 B_2=1,208 B_3=500 B_4=380 B_5=155 B_{6+}=128	G_1=2,410 G_2=1,261 G_3=623 G_4=312 G_5=150 G_{6+}=166	No long run
Passed Test?	Pass	Pass	Pass		Pass

Chaotified VDP]	N=9,000	X=47.2548	B_1=2,568 B_2=1,278 B_3=623 B_4=225 B_5=147 B_{6+}=144	G_1=2,674 G_2=1,254 G_3=668 G_4=249 G_5=166 G_{6+}=184	No long run
Passed Test?	Pass	Pass	Pass		Pass

บทที่ 6
สรุปผลการทดลอง

จากงานวิจัยที่ได้จัดทำขึ้นมา เราได้ทำการพัฒนาค่าสุ่ม ซึ่งจะไม่เกิดรอบการวนซ้ำเหมือนกับค่าสุ่ม ที่สร้างจากโปรแกรม ซึ่งการพัฒนาโครงการนี้คงทำให้ผู้ที่ต้องการใช้ค่าสุ่มสามารถนำสัญญาณสุ่มที่ได้พัฒนาขึ้นมาไปใช้ประโยชน์ได้กันอีกกว้างขวาง และในเอกสารแต่ละบทนั้นได้อธิบายถึงงานวิจัยที่ได้จัดทำขึ้นมาเพื่อใช้ในการทำความเข้าใจ ทำการศึกษา และเป็นแนวทางในการพัฒนาต่อไป

สรุปผลการทดลอง

งานวิจัยเป็นการสร้างบิตสุ่มที่เกิดจากวงจรอลวนในรูปแบบต่าง ๆ โดยการสร้างวงจรอลวน 7 วงจร คือ

1.วงจร High frequency Wien-type chaotic oscillator [2]

2.วงจร Simple RC chaotic oscillator [3]

3.วงจร Double scroll in a simple '2D' chaotic oscillator [4]

4.วงจร Hyper chaotic oscillator [5]

5. วงจรMulti-wing buffterfly attractor

6.วงจรNonautonomous MScroll

7.วงจรChaotified VDP

จากการทดลองนี้ผลที่สรุปได้คือ วงจรอลวนที่ปรากฏงานวิจัยหัวข้อ1-4ผ่านมาตรฐาน FIPS 140-1 ทุกข้อคือวงจร Double scroll in a simple '2D' chaotic oscillator [4] ส่วนอีก 3 วงจรไม่ผ่านมาตรฐานเนื่องจากไม่ผ่านบททดสอบบางข้อ แต่วงจรที่ค้นพบใหม่คือหัวข้อ 5-7 สามารถผ่านการทดสอบหมด เรายังทราบว่าการกำหนดระดับแรงดันไฟในวงจรเปรียบเทียบแรงดันที่เหมาะสมในการSampling สัญญาณอลวนเพื่อให้กำเนิดค่าสุ่ม ให้มีค่าเอ็นโทรปีสูงที่สุด ก็จะได้ผลลัพธ์ของค่าสุ่มที่ดีที่สุดของแต่ละวงจรด้วย

5.2 ปัญหาที่เกิดขึ้นในการทดลอง

การเปลี่ยนแปลงค่าพารามิเตอร์ต่าง ๆ จะมีผลทางด้านความถี่ และรูปร่างของสัญญาณอย่างมาก แม้มีการเปลี่ยนแปลงเล็กน้อย ดังนั้นถ้าต้องการเปลี่ยนแปลงสัญญาณจึงต้องค่อย ๆ เปลี่ยนแปลงไปพร้อม ๆกัน ในพารามิเตอร์ที่มีความสัมพันธ์กัน มิฉะนั้นสัญญาณอลวนก็อาจจะหลุดหายไป อีกทั้งปัญหาของค่าอุปกรณ์อิเล็กทรอนิกส์ที่มีความคลาดเคลื่อนแม้เพียงเล็กน้อย ซึ่งมีผลกับวงจรที่มีช่วงการเกิดสัญญาณอลวนที่แคบ ก็อาจทำให้สัญญาณอลวนไม่เกิดขึ้น ส่วนในการเก็บผลในการทดสอบต่าง ๆ ต้องใช้เวลานานเนื่องจากต้องเก็บค่าของจำนวนบิตมาก ๆ เพื่อความเที่ยงตรงในการวัด

5.3 แนวทางในการพัฒนา

สัญญาณอลวนที่ได้ทดลองว่าสามารถนำไปสร้างค่าสุ่มได้เราสามารถเลือกวงจรที่ดีที่สุดนำไปใช้ในการจำลองทางวิทยาศาสตร์ การกำเนิดค่ารหัสผ่าน (Password) และการออกเลขรางวัล (lottery) ซึ่งจะก่อให้เกิดประสิทธิภาพที่ดีกว่าเดิม เนื่องจากสัญญาณอลวนเป็นสัญญาณที่คล้ายกับสัญญาณรบกวน แต่เราสามารถควบคุมการเกิดของสัญญาณได้โดยกำหนดค่าตัวแปรต่าง ๆ และค่าเริ่มต้นให้กับแหล่งกำเนิดสัญญาณ

บรรณานุกรม

[1] MustakE. Yalcm, Johan A. K. Suykens, Joos Vandewalle, True Random Bit Generation From a Double-Scroll Attractor, Regular papers,Vol.51, No. 7, July 2004.

[2] A.S. Elwakil, M.P. Kennedy, High frequency Wien-type chaotic oscillator, Electronics letters 11th June 1998.

[3] A. Tamasevicius, A. Namajunas, Simple RC chaotic oscillator, Electronics letters 23rd May 1996.

[4] A. Tamasevicius, G.Mykolaitis, A. Namajunas, Double scroll in a simple '2D' chaotic oscillator, Electronics letters 4th July 1996.

[5] A.S. Elwakil, M.P. Kennedy, Inductorless hyperchaos generator, Micrelectronics Joumal 30(1999) 739-743.

[6] A. Tamasevicius, G.Mykolaitis, A.Cenys, Wien-bridge chaotic circuit with comparator, Electronics letters 2nd April 1998.

[7] L. O. Chua, "Global unfolding of Chua's circuit," IEICE Trans. Fundamentals, vol.E76-A, pp. 704-734, May. 1993.

[8] E.N. Lorenz, "Deterministic nonperiodic flow," J Atomos Sci 20 (1963), pp. 130–141

[9] G. Chen, and T. Ueta, "Yet another chaotic attractor," Int. J. Bifurcation Chaos, vol. 9, pp. 1465-1466, 1999.

[10] M.E. Yalcin, J.A.K. Suykens, J. Vandewalle and S. Ozoguz, "Families of scroll grid attractors," Int J Bifurcat Chaos 7 (2002), pp. 23–41

[11] R. David, Random Testing of Digital Circuits: Theory and Application New York: Marcel Dekker, 1998.

[12]B. Schneier, Applied Cryptography New York: J Wiley, 1996.

[13] A. Menezes, P. Van Oorschot, and S. Vanstone, Ed. Handbook of Applied Cryptography Boca Raton, FL: CRC, 1997.

[14] D. Knuth, The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, 2nd ed. Reading, MA: Addison-Wesley, 1981.

[15] B. Jun and P. Kocher "The intel random number generator," A White Paper Prepared for Intel Corporation by Cryptography Research Inc

[16] Security Requirements for Cryptographic Modules, Federal Information Processing Standards FIPS 140-2, May 2001.

[17] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: National Institute for Standards and Technology, Special publication 800-22, 2001.

[18] G. Marsaglia, "DIEHARD: A Battery of Tests of Randomness," 1996, http://stat.fsu.edu/~geo/diehard.html

[19] D. Eastlake, S. Crocker, and J. Schiller, RFC 1750: Randomness recommendations for security: Network Working Group, Tech. Rep., 1994.

[20] D.P. Brown, M. Carl and E.A Dabbish, "Random number generator with digital feedback," US Patent No. US 4,853,884, August 1989.

[21] T. Onodera, S. Kanemoto and S.Tsunoyama, "Physical random number generator, method of generating physical random numbers and physical random number storing medium,"US Patent No. US 6,195,669, February 2001.

[22] D.P. Maher and J. Robert , "Hybrid natural random number generator," US Patent No. US 4,545,024, October 1985.

[23] S.A. Wilber, "Random number generator and generation method," US Patent No. US 7096242, 2006.

[24] E.J.Hoffman, "Random number generator," US Patent No. US 5,706,218, January 1998.

[25] P.Y. Liardet, "Random Number Generating Circuit and Process," US Patent No. US 6,581,078 B1, June 2003.

[26] Q. Le, "High speed random number generation," US Patent No. US 6,714,955, March 2004.

[27] S.E. Wells and D.A. Ward "Random number generator with entropy accumulation," US Patent No. 6,687,721, February, 2004.

[28] S.C. Albers,T.J. Callaghan, W.L. Rasmussen and R.A. Pajak, "Noise generator using combined outputs of two pseudo-random sequence generators," US Patent No. US 5,153,532, October 1992.

[29] G. Bernstein and M. Lieberman, "Secure random number generation using chaotic circuits," IEEE Trans. Circuits Syst., vol. 37, pp. 1157-1164, Sept. 1990.

[30] G.M. Bernstein and M. Lieberman, "Method and apparatus for generating secure random numbers using chaos, US Patent No. US 5,007,087, April 1991.

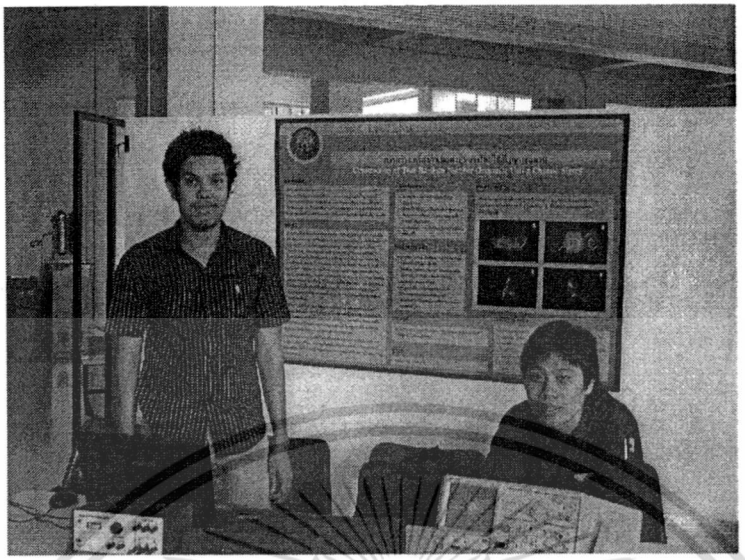
[31] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, V. Vignoli, "Low-hardware complexity PRBGs based on a piecewise-linear chaotic map," IEEE Trans. Circuits Syst II:, vol.53, pp. 329-333, May 2006.

[32] M.E. Yalcin, J.A.K Suykens and J. Vandewalle, "True random bit generation from a double-scroll attractor," IEEE Trans. Circuits Syst I: vol.51, pp. 1395-1404, July 2004.

[33] J. Von Neumann, "Various techniques used in connection with random digits," Applied Math Series, G. E. Forsythe, Ed. Boulder, CO: National Bureau of Standards, 1951, vol. 12, pp. 36-38.

[34] M. Yalcin, "Increasing the entropy of a random number generator using n-scroll chaotic attractors," Int. J. Bifurcat. Chaos, vol. 17, pp.4471-4479, Dec. 2007..

ภาคผนวก



แสดงผลงานวิจัยในงาน 50 ปีพระจอมเกล้าลาดกระบังในส่วนพระจอมเกล้าลาดกระบัง