دانشکده علوم

گروه آموزشی فیزیک

پایان‌نامه برای دریافت درجه‌ی کارشناسی ارشد

در رشته‌ی فیزیک گرایش بنیادی

عنوان:

استفاده از نگاشت‌های آشوبناک جفت شده‌ی همزمان در رمزنگاری

استاد راهنما:

دکتر صدیف احدپور کلخوران

پژوهشگر:

نرجس مقصودی ولنی

تابستان ۱۳۹۵

نام خانوادگی دانشجو: مقصودی ولنی نام: نرجس

عنوان پایان‌نامه:
استفاده از نگاشت‌های آشوبناک جفت شده‌ی همزمان در رمزنگاری

استاد راهنما: دکتر صدیف احدپور کلخوران

مقطع تحصیلی: **کارشناسی ارشد** رشته: فیزیک
گرایش: بنیادی دانشگاه: **محقق اردبیلی**
دانشکده: علوم تاریخ دفاع: ۱۳۹۵/۰۶/۲۹ تعداد صفحات:۱۰۲

چکیده:

همزمان‌سازی آشوب به فرآیندی گفته می‌شود که در آن دو (یا چند) سیستم آشوبناک (مشابه یا نامشابه) یک خاصیت از حرکتشان را برای رسیدن به یک رفتار مشترک به واسطه‌ی جفت‌شدگی یا نیرو تنظیم می‌کنند. همزمان-سازی آشوب روش‌های ارتباطات را تغییر داده است و مانند یک سیستم رمز کامل عمل می‌کند. همزمان‌سازی سیستم‌های آشوبناک جفت‌شده به بخش جدایی ناپذیر رمزنگاری تبدیل شده است. . از آن‌جایی که همزمان‌سازی آشوب در لایه‌ی فیزیکی سیستم انتقال کار می‌کند، باعث حالت‌های سریع ارتباطات می‌شود. رمزنگاری مبتنی برآشوب کاملا از ویژگی‌های دینامیک آشوبناک استفاده می‌کند از جمله، دترمنیسم، ارگودیسی، غیرتناوبی بودن و وابستگی قوی به تغییرات کوچک در هر پارامتر سیستم . رمزنگاری آشوبناک در مقایسه با رمزنگاری سنتی دارای مزیت هایی شامل قابل اجرا بودن برای داده هایی با حجم بالا و قابلیت پیاده سازی در سخت افزار و نرم افزار، هزینه-ی پایین و سرعت قابل توجه می باشد. یکی از اهداف در این پژوهش معرفی روش های استفاده ازنگاشت های جفت شده آشوبناک همزمان برای ارتقاء امنیت می باشد.

کلیدواژه‌ها: آشوب، رمزنگاری، نگاشت جفت‌شده، همزمان‌سازی.

فهرست مطالب

شماره و عنوان مطالب **صفحه**

فصل اول: سیستم‌های آشوبناک جفت شده

فصل دوم: همزمان‌سازی سیستم‌های آشوبناک جفت شده

فصل سوم: کاربرد سیستم‌های جفت شده‌ی آشوبناک همزمان در ارتباطات امن و رمزنگاری

فهرست جدول‌ها

شماره و عنوان مطالب **صفحه**

فهرست شکل‌ها

شماره و عنوان مطالب **صفحه**

۱ فصل اول

سیستم های آشوبناک جفت شده

۱-۱- مقدمه

مطالعه‌ی سیستم‌های دینامیکی از اواسط سال‌های ۱۶۰۰میلادی آغاز شده است که این به دنبال کشف قوانین جاذبه و حرکت و معرفی معادلات دیفرانسیل توسط نیوتن[۱] و توجیه قوانین کپلر در مورد حرکت سیارات بر پایه‌ی آن‌ها بوده است. نیوتن به این روش مسئله‌ی دو جسم (حرکت زمین به دور خورشید) را حل کرد و نتیجه‌ی معروف این‌که نیروی جاذبه‌ی گرانشی متناسب با $1/r^2$ (r فاصله‌ی بین دو جسم است) می‌باشد، به دست آمد.

وقتی ریاضیدان‌ها و فیزیکدان‌ها خواستند این مسئله را به سه جسم تعمیم دهند مثلا برای خورشید، زمین و ماه، متوجه شدند که حل این مسئله غیرممکن است. تا بالاخره در اواخر ۱۸۰۰ میلادی هانری پوانکاره به جای این‌که بخواهد مکان دقیق سیارات را در تمام زمان‌ها به دست آورد، مسئله‌ی پایداری یا ناپایداری سیستم خورشیدی را مطرح کرد و در مورد امکان بروز آشوب[۲] بحث کرد. تا اوایل قرن بیستم به این اظهار نظر در مورد آشوب اعتنایی نشد. زمانی آشوب مورد توجه قرار گرفت که مسائلی مانند نوسانگرهای غیر خطی و کاربرد آن‌ها در فیزیک و علوم مهندسی از جمله در: لیزر، رادار، رادیو و غیره مطرح شدند. در اواخر دهه ۱۹۵۰ میلادی به دنبال کشف کامپیوترهای با سرعت بالا، دانشمندان معادلاتی را که قبلا نمی‌توانستند حل کنند، حل کردند و درک بهتری از سیستم‌های غیرخطی به دست آوردند.

ادوارد لورنتس[۳] در سال ۱۹۶۳ میلادی با معرفی حرکت آشوبناک در جاذب‌های عجیب کار مهمی در این زمینه انجام داد. بعدها افراد دیگری آثار تجربی آشوب را در سیال‌ها، اندرکنش‌های شیمیایی، مدارهای الکترونیکی، نوسانگرهای مکانیکی و نیمه رساناها بررسی کردند. در دهه‌ی ۱۹۷۰ میلادی دو

۱- Newton

۲- Chaos

۳- Edward Lorenz

شاخه‌ی دیگر در دینامیک معرفی شدند: ۱-فراکتال‌ها[۱] توسط مندل بروت: شکل‌های گرافیکی زیبایی که توسط کامپیوتر به دست آمده بود شامل می‌شد. ۲- در حوزه‌ی بیولوژی- ریاضی کاربرد داشت و توسط وینفری مطرح شد: نوسانگرهای غیرخطی را در بیولوژی به کار برد.

۱-۲- آشوب

آشوب یا بی‌نظمی، یک رفتار طولانی مدت غیرتناوبی در یک سیستم معین است؛ که وابستگی حساس به شرایط اولیه را داراست. رفتار طولانی غیرتناوبی به این معنی است که، وقتی در سیستم‌های دینامیکی زمان به سمت بی‌نهایت میل می‌کند، مسیر این سیستم‌ها به نقاط ثابت منتهی نمی‌شود و معین‌بودن سیستم به معنی تصادفی نبودن پارامترها یا شرایط‌اولیه است. سیستم‌های آشوبناک، حساس به شرایط اولیّه هستند و این تفاوت اصلی این سیستم‌ها و سیستم‌های غیرآشوبناک است. سیستم‌های دینامیکی غیرآشوبناک رفتاری تناوبی، امّا سیستم آشوبناک هیچ تناوب غالبی ندارد و دوره‌ی تناوبش بی‌نهایت است.

۱-۲-۱- اثر پروانه‌ای

عبارت اثر پروانه‌ای در پی مقاله‌ای از ادوارد لورنتس به وجود آمده است. او در اجلاس IES[۲] در سال ۱۹۷۲ مقاله‌ای را با این عنوان ارائه داد که آیا بال زدن پروانه‌ای در برزیل می‌تواند باعث ایجاد تندباد در تگزاس شود؟ لورنتس در حال تحقیق روی ریاضیات بسیار ساده‌ای از آب و هوای زمین، به یک معادله دیفرانسیل غیر قابل حل رسید. وی برای حل این معادله به روش‌های عددی با رایانه متوسل شد. او برای این‌که بتواند این کار را در روزهای متوالی انجام دهد، نتیجه‌ی آخرین خروجی یک روز را به عنوان شرایط اولیه‌ی روز بعد وارد می‌کرد. لورنتس در نهایت مشاهده کرد که نتیجه‌ی شبیه سازی‌های مختلف با شرایط اولیه‌ی یکسان با هم کاملا متفاوت است. بررسی خروجی چاپ شده رایانه نشان دادکه رویال

۱- Fractals

۲- Institute of Education Science

مکعب[1]، رایانه‌ای که لورنتس از آن استفاده می‌کرد، خروجی را تا چهار رقم اعشار گرد می‌کند. از آن‌جایی که محاسبات داخل این رایانه با شش رقم اعشار صورت می‌گرفت، از بین رفتن دو رقم آخر باعث چنین تاثیری شده بود. مقدار تغییرات در عمل گرد کردن نزدیک به اثر بال زدن یک پروانه است. مشاهدات لورنتس باعث پررنگ شدن مبحث نظریه‌ی آشوب شد.

اثر پروانه‌ای در واقع بیانگر رد روابط خطی بین علت و معلول و تایید غیر خطی بودن روابط در پدیده‌ها و سیستم‌ها می‌باشد. به این معنی که یک تغییر جزئی در شرایط اولیه می‌تواند به نتایج وسیع و پیش‌بینی نشده در سیستم منجر گردد.

۱-۳- سیستم دینامیکی

محیط عمل پدیده‌ی آشوب، سیستم‌های دینامیکی است. یک سیستم دینامیکی شامل یک فضای فاز مجرد یا حالت فازی است که مختصاتش، حالت دینامیکی سیستم را با به‌کارگیری قوانین دینامیکی مشخص می‌کند. یک سیستم دینامیکی می‌تواند منظم یا آشوبناک باشد.

عنوان سیستم دینامیکی به سیستم‌هایی نسبت داده می‌شود که در گذر زمان دستخوش تحول می‌شوند. بنابراین یک سیستم دینامیکی را می‌توان توسط سه پارامتر زمان، حالت‌ها و قاعده‌هایی که نشان دهنده‌ی نحوه‌ی تحول این حالت‌ها می‌باشد، شکل داد (بوچارا[2]، ۲۰۰۴).

این سیستم‌ها به دو دسته تقسیم می‌شوند: سیستم دینامیکی خطی و سیستم دینامیکی غیر خطی.

سیستم های دینامیکی غیرخطی به دو شکل مورد مطالعه قرار می‌گیرند:

۱. به وسیله‌ی معادله‌ی دیفرانسیل؛ در صورتی که تحول سیستم نسبت به زمان پیوسته باشد.

---

[1]- Royal MCBee

[2]- Boccara

۲. به وسیله‌ی نگاشت‌های تکرار؛ در صورتی که تحول سیستم نسبت به زمان گسسته باشد. نگاشت لوجستیک یکی از مشهورترین و پر کاربردترین این نگاشت‌ها، در حوزه‌ی دینامیک غیرخطی است.

نگاشت‌های آشوبناک مختلفی در رمزنگاری، نهان‌نگاری و پنهان‌نگاری کاربرد دارند. از این سیستم‌ها برای مطالعه‌ی بسیاری از علوم از جمله: فیزیک، نجوم، ریاضیات، بیولوژی، شیمی، اقتصاد، هواشناسی و... استفاده می‌شود.

۱-۴- مفاهیم اولیه در سیستم‌های دینامیکی غیرخطی

وقتی ابعاد فضای فاز از n=1، افزایش یابد، در هر مرحله، پدیده‌های جدیدی اتفاق می‌افتد که می‌توان به نقاط ثابت در سیستم‌های یک بعدی (n=1) و دو شاخه شدن در سیستم‌های دو بعدی (n=2) و آشوب در سیستم‌های سه بعدی (n=3) اشاره کرد. این مفاهیم در ادامه مورد بررسی قرار می‌گیرند.

۱-۴-۱- نقاط ثابت

نقاط ثابت در بررسی رفتار نگاشت‌ها از اهمیت خاصی برخوردار است و بر اساس آن می‌توان نحوه‌ی تحول سیستم را درک کرد. در تعریف نقطه‌ی ثابت می‌توان گفت که هر نقطه از مدار یک نگاشت که شرط زیر در آن صدق کند نقطه‌ی ثابت مدار به شمار می‌آید (استروگتز[۱]، ۱۹۹۴).

$$F(x^*) = x^* \qquad (۱-۱)$$

از دید هندسی هم می توان به این طریق نقطه‌ی ثابت را توصیف کرد که : « نقطه‌ی ثابت نقطه‌ای است که از تقاطع خط $y = x$ و منحنی $y = F(x)$ به وجود می‌آید».

[۱]- Strogatz

برای به دست آوردن نقاط ثابت یک سیستم پیوسته، تابع را برابر صفر قرار می‌دهیم ($f(\tilde{x})=0$)؛ همچنین برای به دست آوردن نقاط ثابت در سیستم گسسته، تابع را برابر $\tilde{x}$ قرار می‌دهیم ($f(\tilde{x}) = \tilde{x}$).

نقاط ثابت را بر حسب پایداری، می‌توان به چهار دسته تقسیم کرد:

۱. اگر شرط $|f'(x)| < 0$ برقرار باشد، آنگاه با افزایش زمان (تکرار)، به نقطه‌ی ثابت میل می‌کند؛ که به آن نقطه‌ی ثابت پایدار می‌گویند.

۲. اگر شرط $|f'(\tilde{x})| > 0$ برقرار باشد، آنگاه این نقطه‌ی ثابت، ناپایدار خواهد بود.

۳. در صورتی که $|f'(\tilde{x})| = 1$ باشد، نقطه‌ی ثابت پایدار حاشیه‌ای خواهد بود.

۴. نقاط ثابتی که در آن‌ها شرط $|f'(\tilde{x})| = 0$ برقرار باشد، فوق‌پایدار گویند.

۱-۴-۲- دوشاخگی

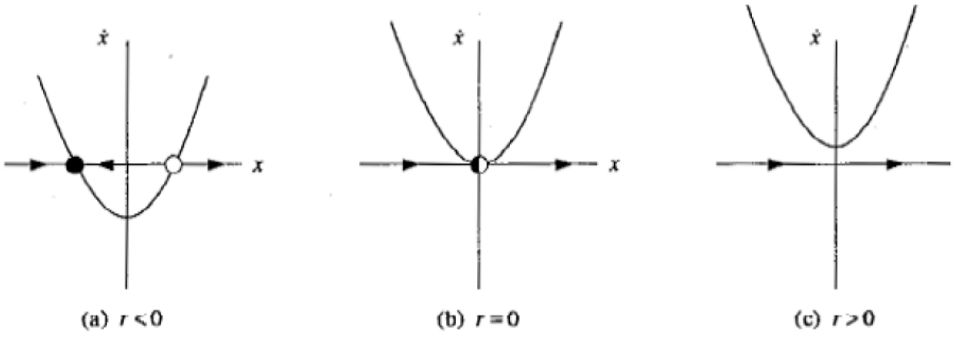
در سیستم‌های دینامیکی، نقاط ثابت می‌توانند خلق یا نابود شوند یا تغییر ماهیت دهند (پایداری آن‌ها تغییر کند یا از نوع جاذب به دافع یا برعکس تبدیل شوند). شروع تغییرات در رفتار نقاط ثابت، دو شاخه شدگی نامیده می‌شود. گذار به حالت دو شاخه شدگی با تغییر کمیتی به نام پارامتر کنترل دو شاخه شدگی صورت می‌گیرد. تغییر رفتار سیستم‌های دینامیکی را بر اساس این‌که پارامتر کنترل می‌تواند مثبت، منفی یا صفر باشد در سه گروه زیر می‌توان طبقه بندی کرد:

- دو شاخگی زینی:

این نوع دو شاخه شدگی به وسیله‌ی خلق یا نابودی نقاط ثابت معلوم می‌گردد و در نگاشت‌هایی که از یکی از ضابطه‌های زیر تبعیت می‌کنند رخ می‌دهد:

$$\dot{x} = r + x^2$$
$$\dot{x} = r - x^2 \qquad (۲-۱)$$

به عنوان نمونه، نمودار مربوط به معادله‌ی اول به ازای مقادیر مختلف پارامتر در شکل (۱-۱) رسم می‌گردد. نقاط توپر بیانگر نقاط ثابت پایدار، نقاط توخالی بیانگر نقاط ثابت ناپایدار و نقاط نیمه پر بیانگر حالت نیمه پایدار می‌باشند. از آن‌جا که در شکل میدان‌های برداری برای $r < 0$ و $r > 0$ متفاوت هستند، دوشاخه شدن در $r = 0$ رخ می‌دهد.



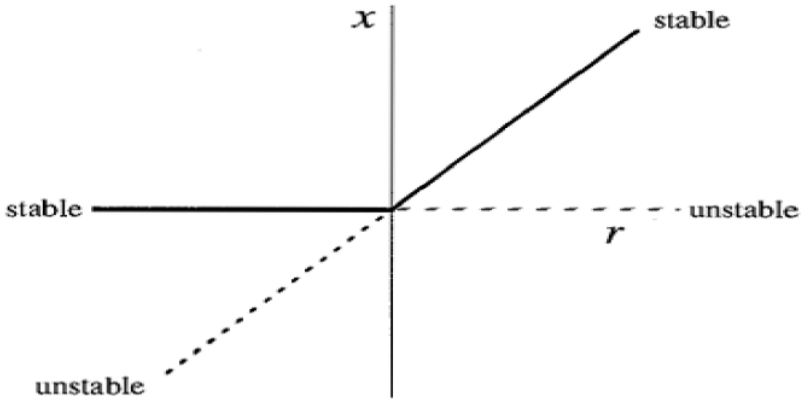
شکل۱-۱: دوشاخه شدگی زین اسبی (استروگتز، ۱۹۹۴)

- دو شاخه شدن گذار بحرانی:

در این نوع دوشاخه شدگی هرگز شاهد خلق یا نابودی نقاط ثابت سیستم نیستیم بلکه، با تغییر پارامتر کنترل، فقط نوع پایداری آن‌ها تغییر می‌کند. ضابطه‌ی کلی سیستمی که این دوشاخه شدگی را نشان می‌دهد، به صورت زیر است:

$$\dot{x} = rx - x^2 \qquad (۳-۱)$$

در شکل (۱-۲) این معادله را برای r های مختلف رسم می‌کنیم که یک نقطه‌ی ثابت در $x^* = 0$ برای تمام مقادیر r دیده می‌شود.



شکل ۱-۲: نمودار دو شاخه شدگی گذار بحرانی (استروگتز، ۱۹۹۴)

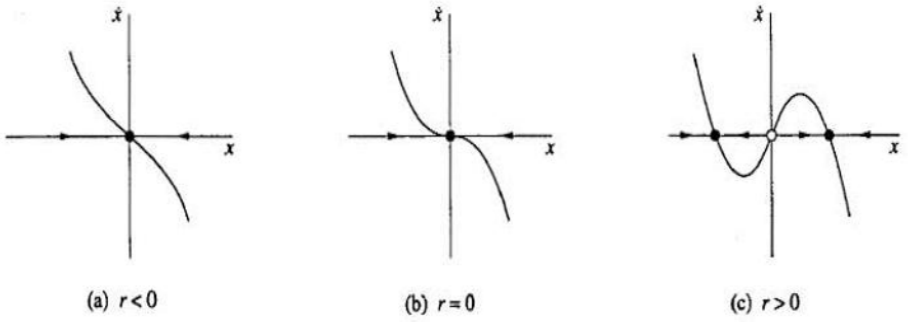
- دوشاخگی چنگالی:

در بسیاری از مسائل فیزیکی تقارن فضایی بین چپ و راست وجود دارد. دو شاخه شـدگی چنگـالی در این مسائل دیده می‌شود. این حالت دارای معادله‌ای به یکی از دو صورت زیر است:

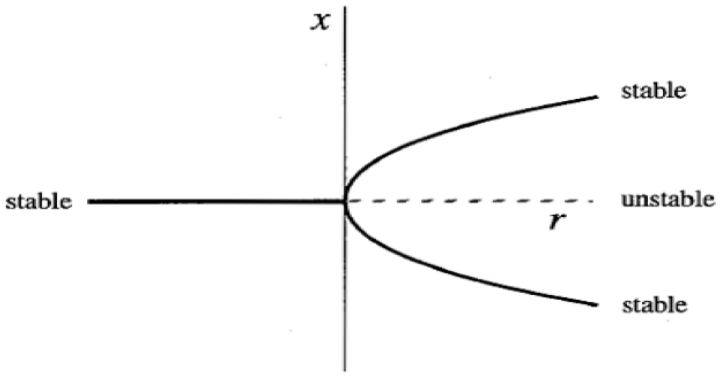
حالت اول، دوشاخه شدگی چنگالی خیلی بحرانی نامیده می‌شود و معادله‌ی آن به صورت زیر است:

$$\dot{x} = rx - x^3 \qquad (۴-۱)$$

این معادله تحت تبدیل $x \to -x$ ناوردا می‌باشد. این ناوردایی، بیان ریاضی تقارن چپ و راست می-باشد. به عنوان نمونه، نمودار مربوط به معادله‌ی (۱-۴) به همراه نمودار دوشاخه شدگی بـه صـورت زیـر رسم می‌شود:



شکل ۱-۳: دو شاخه شدن چنگالی (استروگتز، ۱۹۹۴)



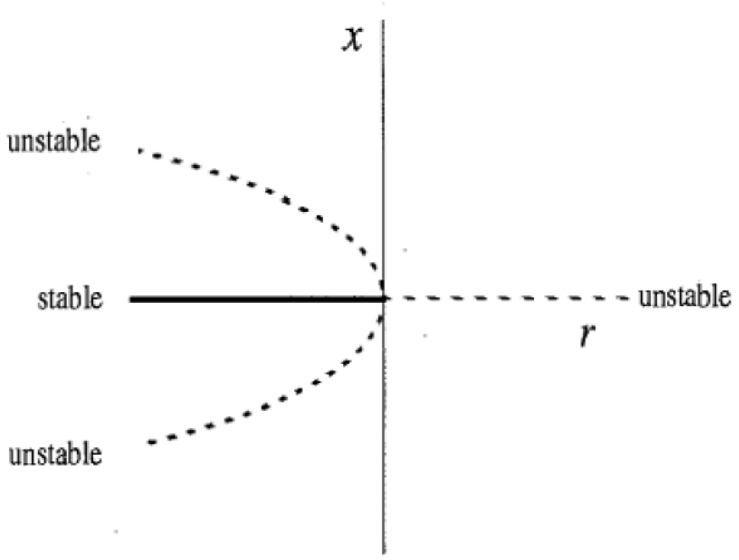
شکل۱-۴: دو شاخه شدن چنگالی خیلی بحرانی(استروگتز، ۱۹۹۴)

در نمودار (۱-۴) وقتی $r < 0$ است مبدا، تنها نقطه‌ی ثابت (پایدار) است. وقتی $r = 0$ است مبدا هنوز پایدار بوده اما خیلی ضعیف است (این یک حالت بحرانی است). بالاخره وقتی $r > 0$ است مبدا ناپایدار بوده و دو نقطه‌ی ثابت پایدار در $x^* = \pm\sqrt{r}$ ظاهر می‌شود.

حالت دوم، دو شاخه شدگی چنگالی زیربحرانی بوده و با معادله‌ی زیر مشخص می‌شود:

$$\dot{x} = rx + x^3 \quad (۵-۱)$$

نمودار دو شاخه شدن چنگالی زیر بحرانی در شکل زیر نشان داده شده است:



شکل ۱-۵: نمودار دو شاخه شدن چنگالی زیر بحرانی(استروگتز، ۱۹۹۴)

۱-۴-۳- نمای لیاپانوف

نمای لیاپانوف توسط ریاضیدان روسی لیاپانوف[۱] در سال ۱۸۹۲ میلادی برای کنترل پایداری معادلات دیفرانسیل غیر خطی مورد استفاده قرار گرفت. این روش امکان مطالعه‌ی پایداری معادلات دیفرانسیل را بدون حل آن‌ها امکان‌پذیر می‌سازد. با توجه به این‌که برای مطالعه‌ی سیستم‌های دینامیکی

[۱]- Lyapanov

غیر خطی باید آن‌ها را توسط نگاشت‌ها مورد بررسی قرار دهیم، به توصیف نمای لیاپانوف کـه مطالعـه‌ی رفتار سیستم‌ها توسط نگاشت را به صورت عددی میسر می‌سازد پرداخته می‌شود.

برای این‌که یک سیستم را بی‌نظم بنامیم باید نشان دهیم که سیستم وابستگی حساس بـه شـرایط اولیه دارد، یعنی این که دو مسیر که خیلی نزدیک به هم شروع می‌شوند، خیلی سریع به طـور نمـایی از هم واگرا شده و آینده‌ی متفاوتی پیدا می‌کنند (استفانسکی[1] و همکاران، ۲۰۰۵). همان‌طور که گفته شد، وابستگی حساس معادلات دیفرانسیل بی‌نظم، با نمای لیاپانوف تعریف می‌گردد، حال این تعریف را بـرای نگاشت‌های یک بعدی بسط می‌دهیم.

فرض می‌کنیم x_0 نقطه‌ای در لحظه‌ی t در روی یک مسـیر و $\delta_0 + x_0$ نقطـه‌ای نزدیـک بـه آن در روی مسیر دیگر باشد که δ_0 بی‌نهایت کوچک بوده و معرف میزان اولیه‌ی جدایی این دو نقطه است. اگر میزان جدایی این دو نقطه بعد از n تکرار توسط δ_n نمایش داده شود، رابطه‌ای به صـورت معادلـه‌ی زیـر مابین دو نقطه برقرار است:

$$|\delta_n| = |\delta_0| e^{n\lambda}, \qquad (۶-۱)$$

در این صورت می‌توان λ را به عنوان نمای لیاپانوف معرفی کرد.

با مثبت شدن نمای لیاپانوف (مقدار λ) فاصله‌ی دو نقطه به صورت نمایی افزایش می‌یابـد، یعنـی سیستم به سمت آشوبناک شدن میل پیدا می‌کند. با منفی شدن مقدار λ، نقطه‌ی ثابت رفتار پایـداری از خود نشان می‌دهد، یعنی سیستم به حالت پایدار می‌رسد. شرط $\lambda=0$، بیانگر حالت حاشیه‌ای است.

محاسبه‌ی فرمول نمای لیاپانوف:

با توجه به این‌که $\delta_n = f^n(x_0 + \delta_0) - f^n(x_0)$ ، به دست می‌آوریم:

$$\lambda = \frac{1}{n} \ln \left| \frac{f^n(x_0 + \delta_0) - f^n(x_0)}{\delta_0} \right| = \frac{1}{n} \ln \dot{f}^n(x_0), \qquad (۷-۱)$$

عبارت داخل لگاریتم را به وسیله‌ی قانون زنجیره‌ای بسط می‌دهیم:

$$\dot{f}^n(x_0) = \Pi_{i=0}^{n-1} \dot{f}(0), \qquad (۸-۱)$$

---

[1]- Stefanski

پس داریم:

$$\lambda = \frac{1}{n}\ln\left|\Pi_{i=0}^{n-1}\dot{f}(0)\right| = \frac{1}{n}\Sigma\ln\left|\dot{f}(0)\right|, \quad (۹-۱)$$

که اگر $n \to \infty$، این معادله به صورت معادله‌ی زیر نوشته می‌شود که بیانگر نمای لیاپانوف است.

$$\lambda = \lim_{n\to\infty}\left\{\frac{1}{n}\Sigma_{i=0}^{n-1}\ln\left|\dot{f}(0)\right|\right\}, \quad (۱۰-۱)$$

برای نقاط پایدار و مدارهای پایدار، $\lambda < 0$ و برای جاذب‌های آشوبناک $\lambda > 0$ است .

۱-۵- جذب کننده‌ها

یک جذب کننده[۱] مجموعه‌ای از تمام مسیرهایی است که به سمت یک نقطه‌ی ثابت، حلقه‌ی محدود یا ... همگرا می‌شوند. نوع دیگری از جذب کننده‌ها وجود دارند که آن‌ها را جذب کننده‌های عجیب[۲] می‌نامند. جذب کننده‌های عجیب به شدت به شرایط اولیه حساس هستند و به آن‌ها عجیب گفته می‌شود چون متشکل از مجموعه‌ای از فراکتال‌ها است.

۱-۶- سیستم‌های آشوبناک

با رشد اینترنت، برنامه‌های کاربردی برای ارتباطات دیجیتال امروزی ساخته شد. محرمانه بودن این ارتباط دیجیتال در اکثر مواقع امری ضروری است. رمزنگاری ابزار مهمی برای محرمانه‌کردن و اختصاصی‌کردن اطلاعات محرمانه می‌باشد. نگاشت‌های آشوبناک دارای خواص حساس‌بودن به شرایط اولیه و پارامتر کنترل، غیرقابل پیش‌بینی بودن، ارگودیسی و غیره هستند. همه‌ی این خواص‌ها آن‌را مناسب برای طراحی بسیاری از روش‌های رمزنگاری کرده است. از نگاشت آشوبناک برای جاسازی اطلاعات محرمانه، در یک فضای تصادفی از عناصر سازنده‌ی فایل پوشش به‌کار می‌رود. در این فصل به

---

۱ - Attractors

۲ - Strange attractors

معرفی نگاشت‌های جفت‌شده و هم‌چنین سیستم‌های آشوبناک مـی‌پـردازیم و در فصـل‌هـای بعـدی بـه همزمان‌سازی و کاربرد آن‌ها در سیستم‌های ارتباط امن خواهیم پرداخت.

۱-۶-۱- نگاشت‌های جفت‌شده

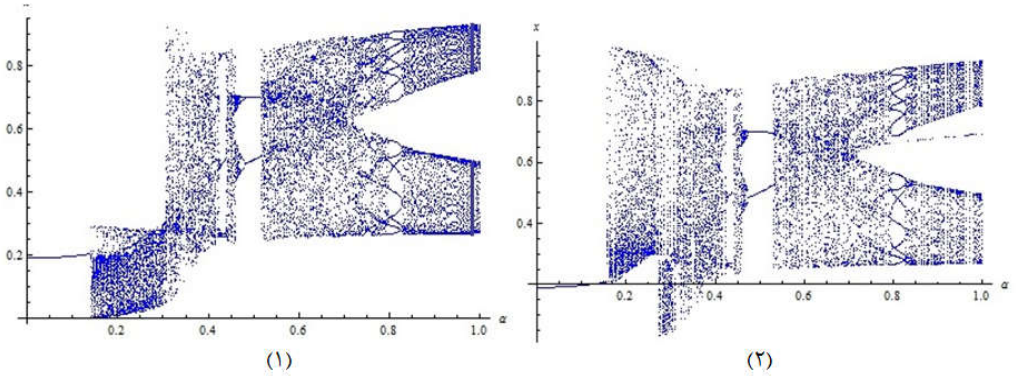
تفاوت این نگاشت با نگاشت‌های دیگر، وجود پارامتر جفت‌شدگی در معادله‌ی آن است. معادله‌ی آن به‌صورت زیر نشان داده می‌شود؛

$$\begin{cases} X_{k+1} = [(1-\varepsilon)f_1(x_{m+1}) + \varepsilon f_2(y_{m+1}) \\ Y_{k+1} = [(1-\varepsilon)f_1(y_{m+1}) + \varepsilon f_2(x_{m+1}) \end{cases} \quad (۱۱-۱)$$

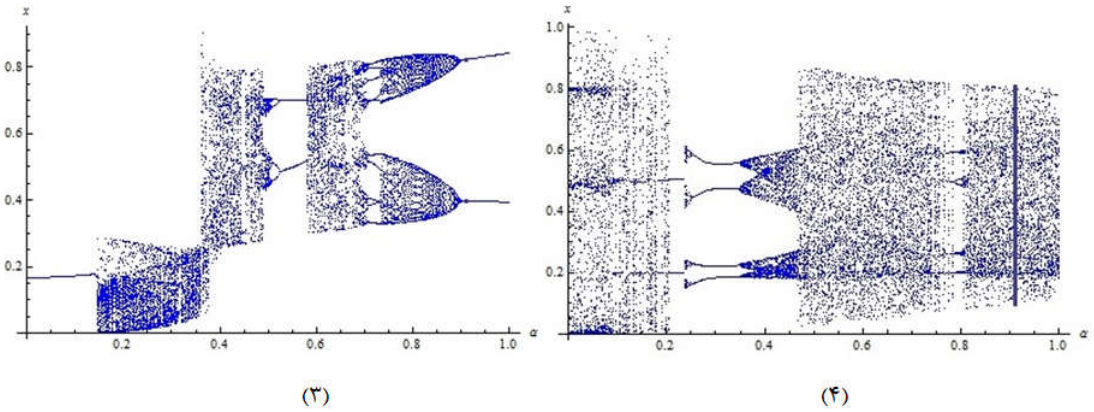
در معادله‌ی (۱-۱۱)، ϵ پارامترِ جفت‌شـدگی در بـازه‌ی ($۰ \leq \epsilon \leq ۱$)، مقـادیر اولیـه نیـز در بـازه‌ی ($۰ \leq x \leq ۱$) و ($۰ \leq y \leq ۱$) هستند؛ همچنین پـارامترهـای کنتـرل بـه‌ترتیـب در بـازه‌ی ($۰ \leq \alpha \leq ۱$ و $۰ \leq \beta \leq ۲$)، قرار دارند، (بهنیا و همکاران، ۲۰۱۴). توابعِ f_1 و f_2 نیز به‌صورت زیر تعریف می‌شوند؛

$$f_1(x_{m+1}) = \frac{\alpha^2 4x_m(1-x_m)}{1+(\alpha^2-1)4x_m(1-x_m)}$$
$$f_2(y_{m+1}) = \frac{\beta^2(2y_m-1)^2}{4y_m(1-y_m)+\beta^2(2y_m-1)^2} \quad (۱۲-۱)$$

نمودار دوشاخه‌شدگی این نگاشت به‌صورت شکل (۱-۶) خواهد بود.



(۱) (۲)



شکل۱-۶: نمودار دوشاخه‌شدن نگاشت جفت‌شده، در شرایط و پارامترهای مختلف (گلباز، ۱۳۹۳)

در شکل (۱-۶)، نمودارهای دوشاخه‌شدن برای شرایط و پارامترهای مختلف نشان داده شده است. در تصویر (۱)، نمودار با شرایط اولیه‌ی (۰٫۵و۰٫۱) و β=۱٫۶۷ و همچنین ثابت جفت‌شدگی ϵ=۰٫۳، نشان داده شده است؛ در تصویر (۲)، شرایطِ اولیه را به (۰٫۳و۰٫۷) تغییر داده‌ایم و پارامترهای دیگر با تصویر(۱) برابر است. در تصویر (۳)، β=۱٫۲۵ و متغیرهای دیگر با تصویر (۱) برابر است؛ در تصویر (۴)، ϵ=۰٫۸ و متغیرهای دیگر با تصویر (۱) برابر است.

۱-۶-۲- سیستم لورنتس

مطالعه‌ی خود در زمینه‌ی سیستم‌های آشوبناک را با معادلات لورنتس آغاز می‌کنیم (استروگتز، ۱۹۹۴):

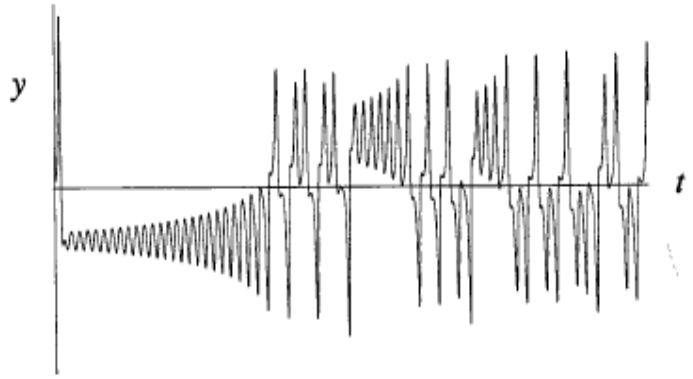
$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = rx - y - xz \\ \dot{z} = xy - bz \end{cases} \quad (۱-۱۳)$$

در این معادلات، σ، r و b پارامترهای مثبت هستند. ادوارد لورنتس در سال ۱۹۶۳ این سیستم سه بعدی را از یک مدل کاملا ساده شده از همرفت در جو به دست آورد. لورنتس دریافت که این سیستم به ظاهر ساده‌ی دترمینیستیک می‌تواند دینامیک به شدت نامظمی داشته باشد: روی محدوده‌ی گسترده‌ای از پارامترها، حل این سیستم به طور نامنظمی نوسان می‌کند،هرگز دقیقا تکرار نمی‌شود اما همیشه در ناحیه‌ی محدودی از فضای فاز باقی خواهد ماند. هنگامی که وی مسیرها را در سه بعد رسم کرد دریافت

که به یک مجموعه‌ی پیچیده ختم خواهد شد که اکنون جاذب آشوبناک نامیده می‌شود. بر خلاف نقـاط ثابت پایدار یا چرخه‌های محدود، جاذب آشوبناک یک نقطه یا منحنی یا حتی یک سطح نیست بلکه یک فراکتال با بعد فراکتالی بین ۲ و ۳ می‌باشـد.در معـادلات لـورنتس σ عـدد پرانتـل[۱]، r عـدد ریلـی[۲] و b نامگذاری نشده اما در مسئله‌ی همرفت به ارتفاع لایه‌ی شاره مرتبط می‌باشد (لورنتس، ۱۹۶۳).

سیستم لورنتس (۱-۱۳) دو نوع نقطه‌ی ثابت دارد. مبدا $(x^*, y^*, z^*) = (۰،۰،۰)$ برای تمام مقـادیر پارامترهـا نقطـه‌ی ثابـت مـی‌باشـد. بـرای مقـادیر $r > ۱$، یـک جفـت نقطـه ثابـت پایـدار $x^* = y^* = \pm\sqrt{b(r-1)}$، $z^* = r - 1$ وجود دارد که لورنز آن‌ها را به ترتیب c^+ و c^- نامید. هنگامی‌کـه $r \to 1^+$ میل کند، این دو مقدار در مبدا با یکدیگر ادغام شده و دو شاخه‌شدگی چنگالی خواهیم داشت.

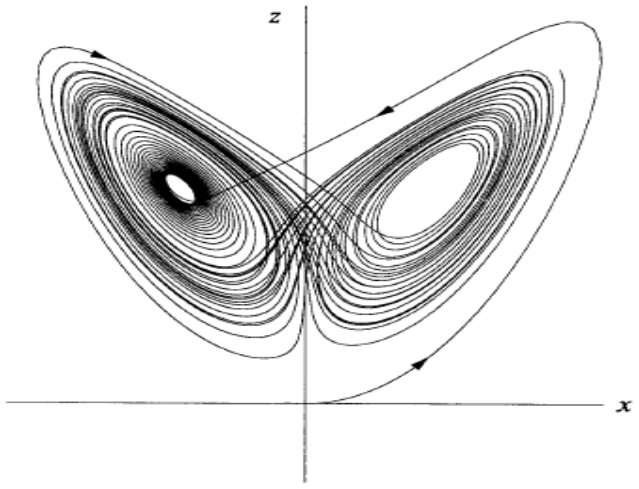
لورنتس محاسبات عددی برای مشـاهده‌ی رفتـار طـولانی مـدت سیسـتم را انجـام داد. وی حالـت خاص σ=۱۰، $r = ۲۸$ و $b = ۸/۳$ را مطالعه کرد. وی محاسبات را از شرط اولیه‌ی (۰،۱،۰)، نزدیک بـه یک نقطه‌ی زینی در مبدا آغاز کرد. شکل (۱-۷) حل حاصل را برای $y(t)$ رسم می‌کند.



شکل ۱-۷: حل سیستم لورنتس با شرایط اولیه‌ی (۰،۱،۰) (منبع: استروگتز، ۱۹۹۴)

[1]- Prandtl
[۲]- Rayleigh

بعد از یک گذار اولیه، حل این مسئله وارد نوسانات نامنظمی می‌شود که با میل زمان به بی‌نهایت ($t \to \infty$) ، ادامه خواهد یافت، اما هرگز به طور دقیق تکرار نمی‌شود. این حرکت نامتناوب می‌باشد. هنگامی که $x(t)$ برحسب $z(t)$ رسم شود یک الگوی پروانه‌ای ظاهر می‌شود که در شکل (۱-۸) مشاهده می‌کنید.



شکل ۱-۸: شکل اثر پروانه‌ای در سیستم لورنتس (منبع: استروگتز، ۱۹۹۴)

۱-۶-۳- سیستم لو

بعد از مطالعه‌ی سیستم لورنتس، بسیاری از سیستم‌های مرتبط با آن(که معمولا لورنتس‌گونه نامیده می‌شوند) مورد مطالعه قرار گرفته‌اند. از بین این سیستم‌های مورد مطالعه سیستم لو[۱] توجه بسیاری به خود جلب کرده است. سیستم لو یک سیستم گذار نوعی است که جاذب‌های چن[۲] و لورنتس را مرتبط می‌سازد و گذار از یکی به دیگری را نشان می‌دهد. در این بخش توصیف مختصری از روش پیش نهادی در(چن و یوتا[۳]، ۲۰۰۰)، که منجر به پیدا کردن این جاذب آشوبناک گردید ارائه می‌دهیم.

[۱] - Lu
[۲]- Chen
[۳]- Ueta

با سیستم کنترل شده لورنتس شروع می‌کنیم:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cx - xz - y + u \\ \dot{z} = xy - bz \end{cases} \quad (۱۴-۱)$$

که c, b و a ثابت‌هایی هستند که در حال حاضر در محدوده آشوب نمی‌باشند و u کنترل کننده بازخورد غیرخطی است که به شکل زیر تعریف می‌شود:

$$u = l_1 x + l_2 y + l_3 z \quad (۱۵-۱)$$

l_1 , l_2 و l_3 مقادیر ثابتی هستند که باید تعیین شوند. ژاکوبین سیستم کنترل شده محاسبه شده در نقطه (x_0, y_0, z_0) شده است:

$$J(x,y,z) = \begin{pmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} & \frac{\partial f_1}{\partial z} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} & \frac{\partial f_2}{\partial z} \\ \frac{\partial f_3}{\partial x} & \frac{\partial f_3}{\partial y} & \frac{\partial f_3}{\partial z} \end{pmatrix} \quad (۱۶-۱)$$

$$J(x_0,y_0,z_0) = \begin{pmatrix} -a & a & 0 \\ c + l_1 - l_0 & l_2 - 1 & l_3 - x_0 \\ y_0 & x_0 & b \end{pmatrix} \quad (۱۷-۱)$$

برای پیدا کردن تعادل سیستم (۱-۱۴) – (۱-۱۵)، اجازه دهید:

$$\frac{dx}{dt} = \frac{dy}{dt} = \frac{dz}{dt} = 0 \quad (۱۸-۱)$$

واضح است اگر $l_3{}^2 + 4b(c + l_1 + l_2 - 1) > 0$ ،آن‌گاه سه نقطه‌ی تعادل وجود دارد:

$$(0,0,0,)\,, \left(x_+, y_+, \frac{x_+{}^2}{b}\right), \left(x_-, y_-, \frac{x_-{}^2}{b}\right)$$

$$x_\pm = y_\pm = \frac{l_3}{2} \pm \frac{\sqrt{l_3{}^2 + 4b(c + l_1 + l_2 - 1)}}{2} \quad (۱۹-۱)$$

از آن جایی که l_3 در ویژه مقادیر مشارکت ندارد، در نمای لیاپانوف سیستم نقش ندارد. برای ساده شدن کنترل کننده می‌توانیم $l_3 = 0$ قرار دهیم. پس، مشاهده می‌کنید که ثابت‌هایl_1, l_2 ، می‌توانند با محاسبه ژاکوبین سیستم (۱-۱۷) در دو نقطه تعادل غیر صفر تعیین شود. برای داشتن رفتار آشوبناک، این دو نقطه تعادل غیر صفر نمی‌توانند پایدار باشند، بنابراین، ژاکوبین باید حداقل یک ویژه مقدار ناپایدار

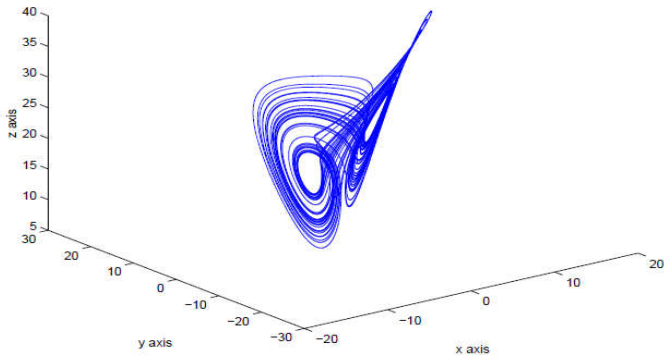
در هر یک از این دو نقطه تعادل داشته باشد. آزمون‌های آزمایشی مختلف نشان می‌دهد که کنترل کننده باید به شکل زیر ساده شود:

$$u = -cx + (c+1)y \qquad (۲۰-۱)$$

بنابراین سیستم آشوبناک جدید به صورت زیر به دست می‌آید (لو و چن،۲۰۰۲):

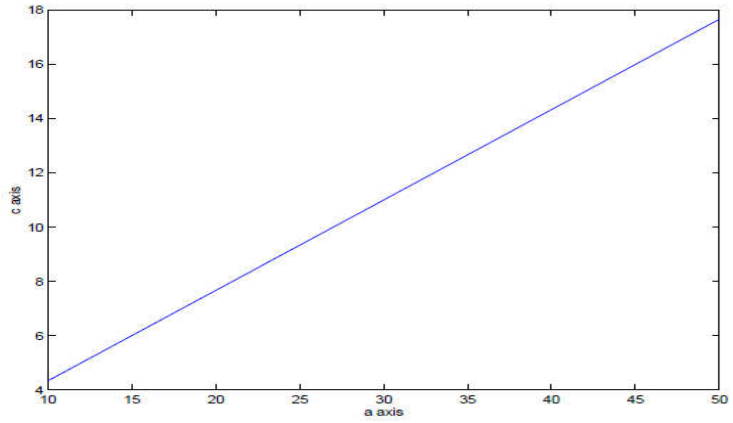
$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = -xz + cy \\ \dot{z} = xy - bz \end{cases} \qquad (۲۱-۱)$$

این سیستم به ازای مقادیر a =۳۶، b =۳ و c = ۲۰ جاذب آشوبناک دارد. شکل (۱-۹) نمودار فاز این جاذب آشوبناک رانمایش می‌دهد.

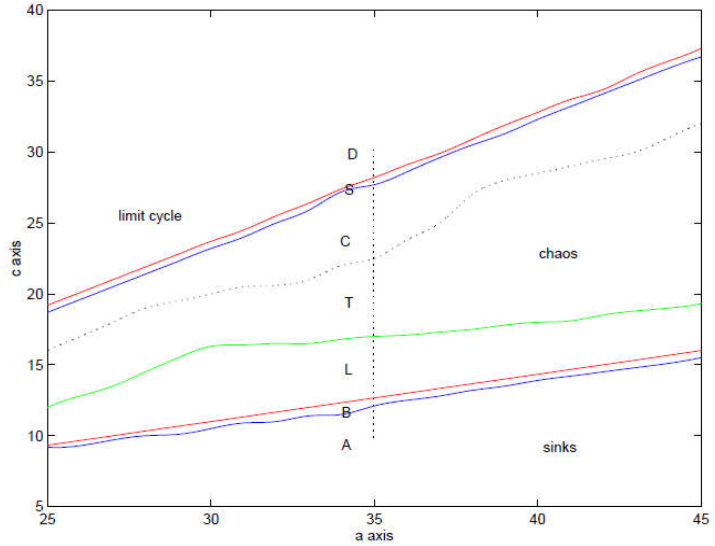


شکل ۱-۹: نمودار فاز سیستم آشوبناک لو به ازای مقادیر a=۳۶، b=۳، c=۲۰ (منبع: لو و همکاران، ۲۰۰۴)

در سیستم آشوبناک لو با ثابت نگه داشتن پارامتر b و تغییر دو پارامتر دیگر شاهد دوشاخه شدن پیوسته‌ی هاوف خواهیم بود که در شکل (۱-۱۰) نمایش داده شده است.



شکل ۱-۱۰: نمودار دوشاخگی پیوسته هاوف سیستم(۱-۲۱)،۳=b (منبع: لو و همکاران، ۲۰۰۲)



شکل۱-۱۱: نمودار رفتار دینامیکی سیستم (۱-۲۱)،۳ =b (منبع: لو و همکاران، ۲۰۰۲)

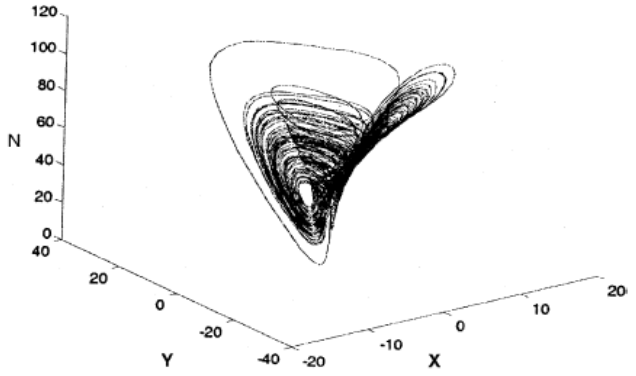
۱-۶-۴- سیستم لیو

لیو[۱] یک سیستم از معادلات دیفرانسیل مستقل سه بعدی با تنها دو جمله‌ی درجه‌ی دوم پیشنهاد داده است که مطابق زیر توصیف می‌شود:

[۱]- Liu

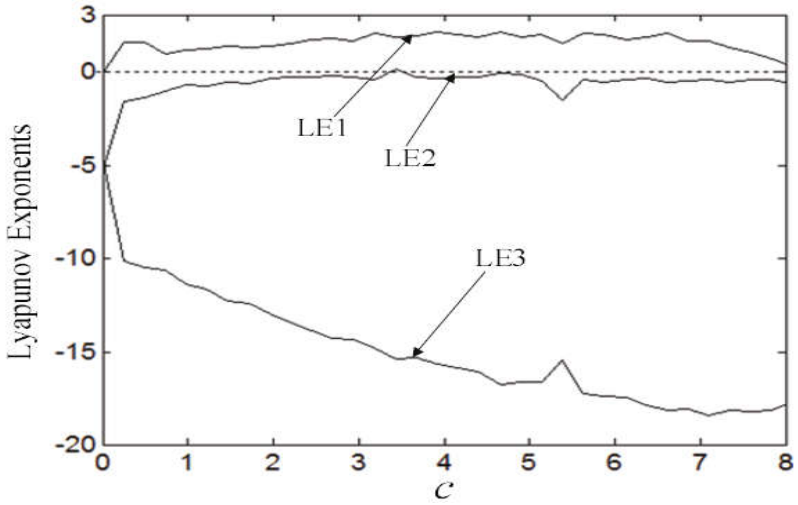
$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - kxz \\ \dot{z} = -cz + hx^2 \end{cases} \quad (۲۲-۱)$$

که $(x,y,z) \in R^3$ متغیرهای حالت، $(a,b,c) \in R^3$پارامترهای حقیقی مثبت و c در یک محدوده‌ی معین تغییر می‌کند. جاذب آشوبناک به دست آمده از این سیستم بر اساس محاسبات عددی و هم‌چنین تجزیه و تحلیل‌های تئوری یک جاذب پروانه‌ای شکل می‌باشد،که دینامیک آشوبناک پیچیده‌ای را نمایش می‌دهد.(لیو، ۲۰۰۴)

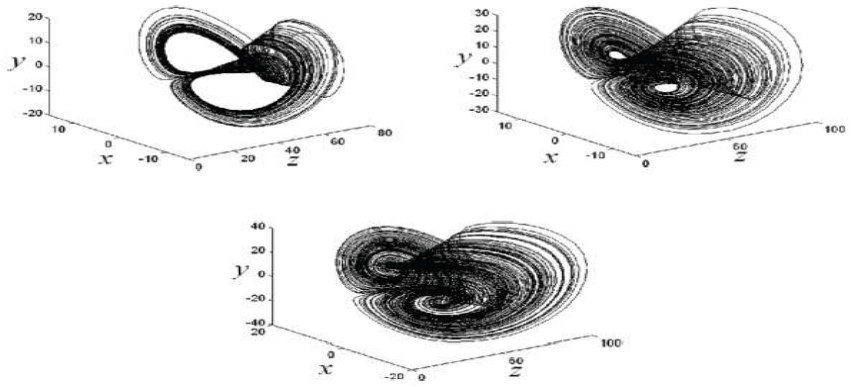


شکل ۱-۱۲: جاذب آشوبناک سیستم لیو (منبع: لیو و همکاران، ۲۰۰۴)

در سیستم لیو، هنگامی که c در یک محدوده‌ی بزرگ تغییر می‌کند سیستم حاصل می‌تواند هنوز آشوبناک باشد و رفتار پیچیده تری نسبت به سیستم لیو اصلی داشته باشد. ودر مقایسه با پارامترهای دیگر،پارامتر c برای استفاده در مدولاسیون پارامتر مناسب‌تراست.شکل (۱-۱۳) طیف نمای لیاپانوف سیستم (۱-۲۲) را نشان می‌دهد، هنگامی‌که $c \in [0.5, 8]$ باشد،سیستم (۱-۲۲) همیشه آشوبناک است. جاذب آشوبناک سیستم لیو با c متفاوت در شکل (۱-۱۴) نشان داده شده است.



شکل ۱-۱۳: طیف نمای لیاپانوف سیستم لیو (۱-۲۲) با $a=10, b=40, c\in[0,8]$ (منبع: اکسو، ۲۰۱۱)



شکل ۱-۱۴:جاذب آشوبناک سیستم لیو (۱-۲۲) به ازای مقدیر مختلف c (منبع: اکسو، ۲۰۱۱)

سیستم لیو یک جاذب پروانه‌ای شکل مشابه جاذب لورنتس دارد اما معادل آن نمی‌باشد. مطالعات موجود نشان داده‌اند که سیستم لیو معادل سیستم مروکا-شیمیزو[۱] است و یک مثال نشان دهنده‌ی جاذب آشوبناک می‌باشد.

[۱] - shimizu-morioka

Family name: Maghsoudi Velni Name: Narjes

Title of Thesi:Application of synchronized chaotic pair-coupled maps in cryptography

Supervisor: Sodeif Ahadpour Kalkhoran (Ph.D)

Graduate Degree **M.Sc.**

Major: Physics Specialty**:** Funddamental Physic

University: **Mohaghegh Ardabili** Faculty: Basic sciences

Graduation date: Sep 2016 Number of pages:102

Abstract :

Synchronization of chaos refers to a process wherein two (or many) chaotic systems (either equivalent or nonequivalent) adjust a given property of their motion to a common behavior due to a coupling or to a forcing. Chaos synchronization has changed the approach of communication, it works as a whole cryptosystem. Synchronization of coupled chaotic systems has become an integral part of cryptography. It allows effectively fast modes of communication as it works in the physical layer of the transmission system. Chaos based cryptography fully exploits the characteristics of chaotic dynamics, vs. determinism, ergodicity, sensitive dependence on initial conditions, randomness, a strong dependence on any minimal variation of any parameter of the system. Chaotic cryptography has advantages compared to traditional cryptography, including applicable for high-volume data and the ability to implement in hardware and software, low cost and speed is impressive. One goal of this study is to introduce methods of using the synchronized chaotic pair-coupled maps in cryptography to enhance security.

Keywords: chaos, cryptography, pair- coupled maps, synchronization.

University of Mohaghegh Ardabili
Faculty of Sciences
Department of Physic

Thesis is approved for the degree of M.Sc.
In Physics

Title:

Application Of Synchronized Chaotic Pair-Coupled Maps In Cryptography

Supervisor:
Sodeif Ahadpour Kalkhoran (Ph.D)

By:
Narjes Maghsoudi Velni

Summer 2016