
بسم الله الرحمن الرحيم


**دانشکده برق**

**گروه کنترل**

# بهبود عملکرد سیستم‌های مخابرات امن مبتنی بر آشوب

**دانشجو:**

**مسعود خدادادزاده**

**استاد راهنما:**

**دکتر حسین قلی زاده نرم**

**پایان نامه ارشد جهت اخذ درجه کارشناسی ارشد**

**شهریور ۱۳۹۳**

تقدیم به پدر و مادر مهربانم...

# تعهد نامه

اینجانب مسعود خدادادزاده دانشجوی دوره کارشناسی ارشد رشته کنترل دانشکده برق دانشگاه صنعتی شاهرود نویسنده پایان نامه **بهبود عملکرد سیستم‌های مخابرات امن مبتنی برآشوب** تحت راهنمائی دکتر قلی زاده متعهد می شوم .

- تحقیقات در این پایان نامه توسط اینجانب انجام شده است و از صحت و اصالت برخوردار است .
- در استفاده از نتایج پژوهشهای محققان دیگر به مرجع مورد استفاده استناد شده است .
- مطالب مندرج در پایان نامه تاکنون توسط خود یا فرد دیگری برای دریافت هیچ نوع مدرک یا امتیازی در هیچ جا ارائه نشده است .
- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی شاهرود می باشد و مقالات مستخرج با نام « دانشگاه صنعتی شاهرود » و یا « Shahrood University of Technology » به چاپ خواهد رسید .
- حقوق معنوی تمام افرادی که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند در مقالات مستخرج از پایان نامه رعایت می گردد.
- در کلیه مراحل انجام این پایان نامه ، در مواردی که از موجود زنده ( یا بافتهای آنها ) استفاده شده است ضوابط و اصول اخلاقی رعایت شده است .
- در کلیه مراحل انجام این پایان نامه، در مواردی که به حوزه اطلاعات شخصی افراد دسترسی یافته یا استفاده شده است اصل رازداری ، ضوابط و اصول اخلاق انسانی رعایت شده است .

**تاریخ**

**امضای دانشجو**

## مالکیت نتایج و حق نشر

- کلیه حقوق معنوی این اثر و محصولات آن (مقالات مستخرج ، کتاب ، برنامه های رایانه ای ، نرم افزار ها و تجهیزات ساخته شده است ) متعلق به دانشگاه صنعتی شاهرود می باشد . این مطلب باید به نحو مقتضی در تولیدات علمی مربوطه ذکر شود .
- استفاده از اطلاعات و نتایج موجود در پایان نامه بدون ذکر مرجع مجاز نمی باشد.

# چکیده

در این پایان‌نامه به‌منظور افزایش امنیت سیستم‌های مخابرات امن آشوبی، از ترکیب روش مدولاسیون پارامتر آشوبی، پنهان نگاری در تصویر و نگاشت‌های آشوبی چند مدال استفاده‌شده است. ابتدا روشی جدید برای پنهان نگاری تصویر با استفاده از نگاشت‌های آشوبی چند مدال که دو عدد (پارامترهای سیستم فرستنده) را به‌عنوان کلید دریافت می‌کند، ارائه کرده و سپس اطلاعات موردنظر از طریق جمع با پارامترهای سیستم آشوبی فرستنده با روش مدولاسیون آشوبی ارسال می‌گردد. روش بیان‌شده شامل یک سیستم گیرنده برای همگرایی مجانبی و تخمین پارامترهای نامعین سیستم آشوبی راسلر است. بهره سیستم گیرنده دائماً به‌وسیله کنترل‌کننده تطبیقی تنظیم می‌گردد تا خطای خروجی سیستم به صفر و پارامترها به مقدار واقعی همگرا شوند. از پارامترهای همگرا شده در گیرنده به‌عنوان کلید بازیابی اطلاعات برای تعیین خانواده و عضو نگاشت موردنظر استفاده می‌شود. با انتخاب این خانواده و عضو نگاشت، محل پیکسل‌ها برای بازیابی اطلاعات دریافت شده به دست می‌آید. درنهایت نحوه کاربرد روش پیشنهادی در غالب مثالی بیان می‌شود. در این مثال پیام مخفی در تصویر پنهان نگاری شده و با روش مدولاسیون آشوبی ارسال می‌گردد. در گیرنده با انجام سنکرون سازی تصویر موردنظر دریافت و پیام مخفی بازیابی می‌شود.

**کلمات کلیدی:** مخابرات امن آشوبی، نگاشت‌های آشوبی چندمدال، استگانوگرافی

**فهرست مطالب**

## فهرست اشکال

فهرست جداول:

# فصل اول: مقدمه

با پیشرفت علم و توسعه فنّاوری، پنهان‌سازی اطلاعات و انتقال امن آن‌ها نیز تکامل پیداکرده و جایگاه خود را به‌عنوان ابزاری نیرومند در جهت حفاظت از اطلاعات پیدا نموده است. امروزه ارتباط از طریق تجهیزات مخابراتی در سطوح مختلف به نحو چشمگیری افزایش‌یافته و به همین علت همواره خطر استراق سمع، دست‌کاری و مغشوش کردن اطلاعات توسط دشمن و یا افراد سودجو، آن را تهدید می‌کند.

یکی از روش‌هایی که برای افزایش امنیت مورداستفاده قرار می‌گیرد این است که اطلاعات موردنظر را رمزنگاری کرده و یا با افزایش امنیت ارسال اطلاعات و حتی ترکیب این دو از این تهدیدات جلوگیری کنیم. با روش‌های گوناگونی می‌توان امنیت ارسال اطلاعات را افزایش داد که یکی از ایمن‌ترین این روش‌ها استفاده از سیستم‌های آشوبی است. سیستم‌های آشوبی یک کلاس از سیستم‌های غیرخطی با دینامیک معین هستند که بسیار به شرایط اولیه حساس‌اند. از دیگر خصوصیات این سیستم‌ها این است که در محدوده خاصی از پارامترهای خود این خاصیت را نشان می‌دهند و یا به‌عبارت‌دیگر با تغییر پارامترها می‌توانند از حالت آشوبی خارج شوند. حساسیت شدید این سیستم‌ها به شرایط اولیه موجب می‌شود که رفتار سیستم قابلیت پیش‌بینی در یک بازه طولانی را نداشته باشد. البته حالت سیستم در لحظه بعد کاملاً معین است ولی در طولانی‌مدت نمی‌تواند با هیچ دقتی پیش‌بینی شود. بنابراین خاصیت حساسیت شدید به شرایط اولیه پیش‌بینی درازمدت را در این سیستم‌ها غیرممکن می‌کند [۱]. این سیستم‌ها همچنین طیف توان پیوسته‌ای دارند و باند فرکانسی آن‌ها شبیه نویز است [۲]. خاصیت غیرقابل‌پیش‌بینی بودن این سیستم‌ها و محدوده فرکانسی وسیع آن‌ها موجب شده است که این سیستم‌ها انتخاب مناسبی برای کد کردن و پوشانیدن[۱] اطلاعات در مخابرات امن شوند؛ بنابراین امنیت مخابرات آشوبی به حساسیت شدید سیستم‌های آشوبی به پارامتر و شرط اولیه بستگی دارد [۳].

[۱] Masking

روش‌های گوناگونی برای ارسال اطلاعات به طریق ایمن با رویکرد کنترلی ارائه‌شده است که این روش‌ها عبارت‌اند از:

۱) پوشش آشوبی[۲]

در این روش سیگنال پیام مستقیماً به یک سیگنال آشوبی اضافه می‌شود که این حامل می‌تواند یکی از سیگنال‌های سیستم آشوبی باشد. همچنین در این روش دامنه سیگنال ارسالی باید تا حد امکان کوچک بوده و بسیار کمتر از دامنه حامل آشوبی باشد در غیر این صورت می‌تواند منجر به ناپایداری کل سیستم شود. درنهایت با سنکرون سازی صورت گرفته در گیرنده و فرستنده سیگنال پیام بازیابی می‌شود [4].

۲) مدولاسیون آشوبی[۳]

در این روش پیامی که برای درایو کردن فرستنده ارسال می‌شود حالت‌ها یا پارامترهای سیستم آشوبی را از طریق یک فرآیند معکوس‌پذیر تغییر می‌دهد و درنهایت یک سیگنال اسکالر که تابعی از متغیرهای فرستنده و سیگنال اطلاعات است به گیرنده ارسال می‌کنند. در این روش برای مثال سیگنال اطلاعات می‌تواند برای مدوله کردن یک پارامتر از سیستم آشوبی استفاده شود. سیگنال حاصل در گیرنده دمودوله[۴] می‌شود و سیگنال اطلاعات با استفاده از دمودولاتور تطبیقی[۵] استخراج می‌شود [۵]. در این حالت خاص یعنی کد کردن پیام با مدولاسیون یک پارامتر، انتخاب صحیح پارامتر مدولاسیون سنکرون سازی در گیرنده را مستقل از مدولاسیون امکان‌پذیر می‌کند.

در مدولاسیون آشوبی برای استخراج اطلاعات در گیرنده باید بین گیرنده و فرستنده سنکرون سازی روی دهد. برای سنکرون سازی سیستم‌های آشوبی روش‌های متعددی ارائه‌شده است مانند کنترل

[۲] Chaotic Masking
[۳] Chaotic Modulation
[۴] Demodulator
[۵] Adaptive Demodulator

مقاوم[۴]، کنترل حالت لغزشی[۶][۵]، کنترل تطبیقی [۶-۸]، کنترل بهینه[۹]، و... . در این سنکرون سازی دو سیستم گیرنده و فرستنده آشوبی باقی می‌مانند ولی یکی با دیگری سنکرون می‌شوند (دو سیستم آشوبی در گیرنده و فرستنده در شرایط اولیه متفاوت کار می‌کنند). البته محدودیتی که این روش یعنی مدوله کردن حامل با سیگنال پیام وجود دارد این است که سیگنال ورودی به فرستنده باید با دقت انتخاب شود تا اطمینان حاصل شود که فرستنده و گیرنده آشوبی باقی می‌مانند.

مقایسه این دو روش نشان می‌دهد که حضور حامل آشوبی و آشفتگی‌های[۷] ایجادشده قابل‌شناسایی است و در عمل این روش‌ها از امنیت لازم برخوردار نمی‌باشند [۱۰]، بنابراین برای افزایش دادن امنیت ارتباط سه روش پیشنهاد می‌شود:

۱) استفاده از سیستم‌های فوق آشوب در فرستنده و گیرنده که به دلیل ساختار و دینامیک پیچیده‌تر رمزگشایی توسط مزاحم را مشکل می‌کنند [۷]. این سیستم‌ها که تعداد نماهای لیاپانوف مثبتشان بیشتر از یکی است این مزیت را دارند که خاصیت عدم پیش‌بینی بیشتری را دارا می‌باشند. در این سیستم‌ها ساختار فضای حالت به‌آسانی توصیف نمی‌شوند. همچنین این سیستم‌ها می‌توانند برای ارسال و دریافت تعداد زیادی سیگنال اطلاعاتی به‌صورت همزمان بکار روند؛ اما در سنکرون سازی این سیستم‌ها با مشکل مواجه هستیم و این کار به‌سختی صورت می‌گیرد.

۲) کار کردن روی روش‌های سنتی رمز کردن اطلاعات با استفاده از سیستم‌های آشوبی [۱۱].

۳) ترکیب مناسبی از روش‌های بالا و ارائه یک رهیافت جدید مخابرات امن آشوبی.

[۶] Sliding Mode Control
[۷] Perturbation

## ۱-۱- پیکربندی پایان‌نامه

در این پایان‌نامه به دلیل اهمیت مبحث آشوب، ابتدا به مفهوم آشوب و دینامیک‌های آشوبناک می‌پردازیم و سپس نگاشت‌های آشوبی لاجستیک، چند مدال و خصوصیات آن‌ها مورد ارزیابی قرار می‌گیرد.

در فصل سوم تعریف سنکرون سازی و روش‌های مختلف آن ارائه خواهد شد. به دلیل کاربرد سنکرون سازی در تمامی سیستم‌های مخابرات امن آشوبی تعدادی از این روش‌ها، مزایا و معایب هریک بیان می‌شود.

در فصل چهارم به بررسی مشروح تاریخچه سیستم‌های مخابرات امن آشوبی می‌پردازیم؛ نسل‌های مختلف این سیستم‌ها را بیان نموده و باهم مقایسه می‌کنیم.

درنهایت در فصل پنجم روش پیشنهادی برای افزایش امنیت سیستم‌ها مخابرات امن آشوبی ارائه می‌گردد. در این روش قصد داریم با ترکیب نسل‌های مختلف مخابرات امن آشوبی و ارائه روشی برای همزمانی سیستم‌ها ضریب ایمنی ارسال اطلاعات را در مقایسه با روش‌های بیان‌شده افزایش دهیم. ابتدا استگانوگرافی در تصویر و روش استفاده از آن را بیان کرده و مزایا و معایب آن را با روش‌های معمول رمزنگاری مقایسه می‌کنیم. سپس از نگاشت‌های آشوبی چند مدال به‌عنوان روشی جدید برای جایگذاری اطلاعات در تصویر بهره می‌گیریم. درنهایت با ارائه روش سنکرون سازی جدید و تلفیق آن با استگانوگرافی تصویر امنیت ارسال اطلاعات در سیستم‌های مخابرات امن آشوبی را افزایش می‌دهیم.

# فصل دوم: مفهوم آشوب و دینامیک آشوبناک

آشوب همان‌طور که از نامش پیداست، رفتاری به‌ظاهر تصادفی و بی‌نظم است که در بسیاری از پدیده‌های دنیای واقعی رخ می‌دهد. پدیده‌های معروفی چون اثر پروانه‌ای[۸] از ویژگی‌های خاص آشوب است که در مورد آن توضیح خواهیم داد. در این فصل جز مقدمه‌ای کوتاه و چند تعریف ریاضی، چندان به خود تئوری آشوب نمی‌پردازیم ولی بااین‌حال یادآوری مجدد ویژگی‌های آن بی‌فایده نخواهد بود.

می‌دانیم که ابزار تحلیل پدیده‌ای طبیعی برای فیزیک‌دانان و مهندسان و بقیه علومی که نیاز به مدل‌سازی و تحلیل آن پدیده با استفاده از آن مدل دارند، معادلات دیفرانسیل (معادلات تفاضلی) است. این معادلات که می‌توانند به‌صورت جزئی[۹] یا معمولی[۱۰] باشند، چارچوب تحلیلی قوی برای همه دانشمندان علوم طبیعی فراهم می‌کنند. در بسیاری از موارد برای سادگی تحلیل، مدل‌ها به‌صورت خطی تقریب زده می‌شوند. در این صورت ابزارهای ریاضی کاملی برای تحلیل این‌چنین مسائلی وجود دارد. بااین‌حال به‌محض اینکه چنین ساده‌سازی انجام ندهیم با معادلات غیرخطی مواجه می‌شویم که پدیده‌های جدیدی چون چرخه حدی[۱۱] در آن مشاهده می‌شود؛ اما این تنها رفتار متفاوت دینامیک غیرخطی با خطی نیست. مدت‌ها به دلیل وجود قضیه پوانکاره- بندیکسون تصور می‌شد که سیستم یا دارای نقطه تعادل (چه پایدار و چه ناپایدار) است و یا دارای چرخه حدی است. البته این قضیه تنها برای سیستم‌های مرتبه دوم صادق بود، اما باور عموم بر آن بود که چنین قضیه‌ای برای سیستم‌های مرتبه بالاتر نیز برقرار است. بااین‌حال مشاهده شد که برای سیستم‌های مرتبه سه به بالا، پدیده دیگری نیز علاوه بر این‌ها رخ می‌دهد و آن‌هم آشوب است [۱۲].

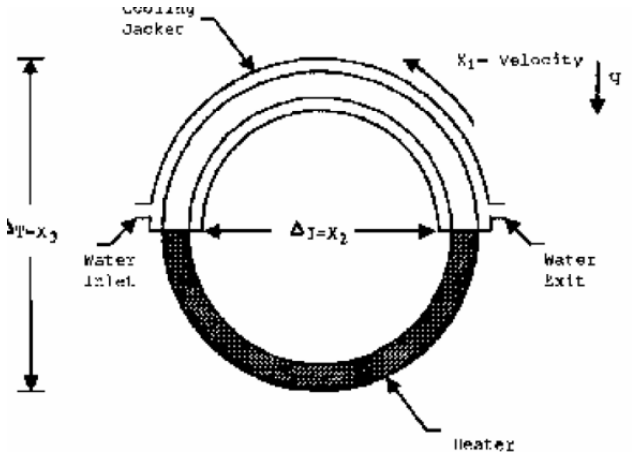
آشوب به مفهوم دقیق و ریاضی آن پدیده است به‌ظاهر تصادفی و پیچیده که در باطن طبیعتی قطعی[۱۲] (در تقابل با تصادفی[۱۳]) دارد. به‌عبارت‌دیگر از یک معادله دیفرانسیل ساده می‌توان رفتارهای

[۸] Butterfly effect
[۹] Partial differential equation(PDE)
[۱۰] Ordinary differential equation(ODE)
[۱۱] Limit cycle
[۱۲] Deterministic

بسیار پیچیده‌ای را انتظار داشت. نمونه از دینامیک مرتبه سوم آشوبناک را که به دینامیک لورنز مشهور است، در زیر می‌بینید.

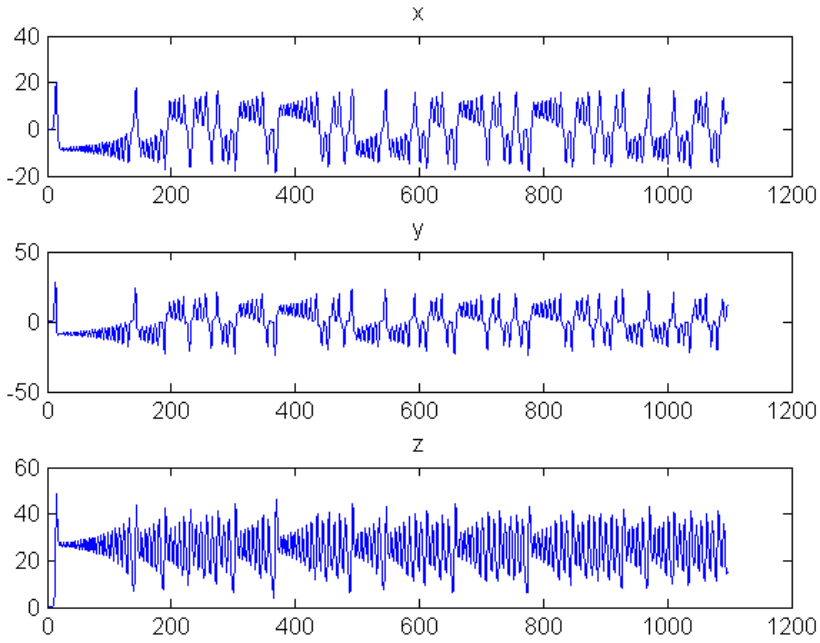
$$\begin{cases} \dot{x} = \sigma(y - x) + u \\ \dot{y} = rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \qquad (۱-۲)$$

دینامیک لورنز توسط هواشناسی به نام ادوارد لورنز[۱۴] در سال ۱۹۶۳ به‌دست‌آمده است، بیان‌گر جریان همرفت در مایعاتی است که گرما از طریق منبعی به آن تزریق می‌شود. نمونه‌ای از ترکیب‌بندی که منجر به دینامیک لورنز می‌شود را در شکل (۲-۱) می‌بینید. لورنز نشان داد که تلاطم[۱۵] در آن مایعات توسط دینامیک ساده‌شده لورنز قابل‌بیان است [۱۳]. نمونه‌ای از رفتار آشوبی این دینامیک را در شکل (۲-۲) می‌بینید.



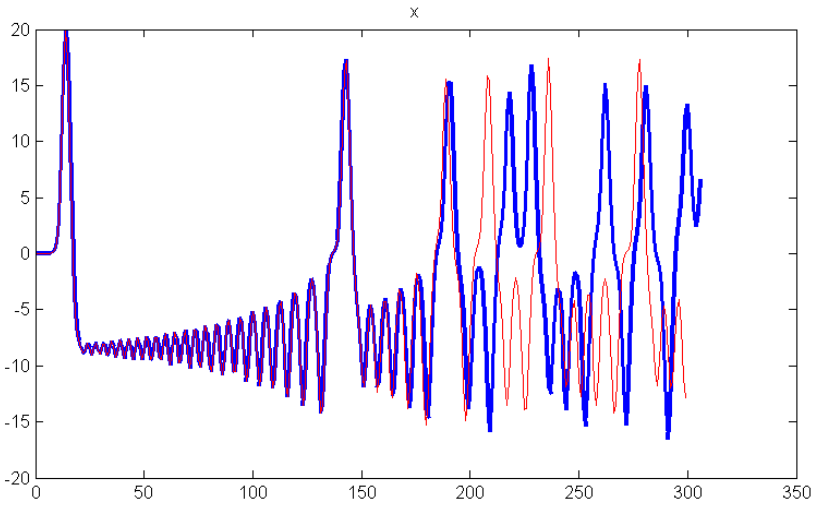

شکل ۲-۱. نمونه‌ای از آزمایشی که منجر به معادلات دیفرانسیل لورنز می‌شود. $x_1$ (نشان داده‌شده با $x$ در معادلات داخل متن) متوسط سرعت چرخش سیال، $x_2$ (نشان داده‌شده با $y$) فاصله تفاوت دمای افقی و $x_3$ (نشان داده‌شده با $z$) تفاوت دمای عمودی است [۱۳].

[۱۳] Stochastic
[۱۴] Edvard Lorenz
[۱۵] Turbulent



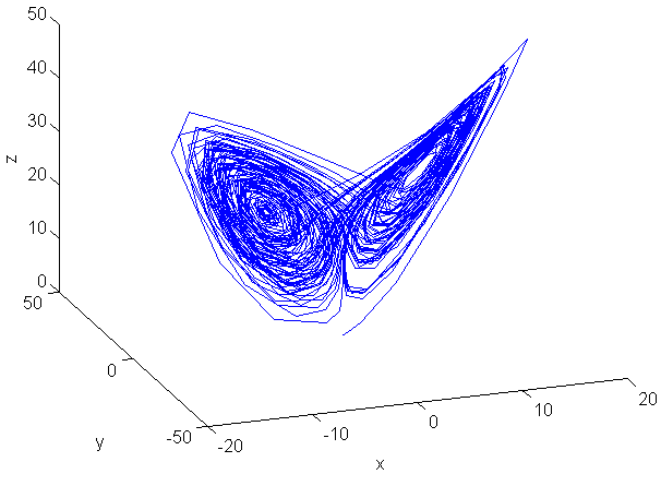

شکل ۲-۲. رفتار آشوبی دینامیک های سیستم لوزنز

یکی از ویژگی‌های سیستم آشوبی، چیزی است که به حساسیت بالا به شرایط اولیه مشهور شده است. یک سیستم آشوبناک- برخلاف سیستم دارای چرخه حدی یا نقطه تعادل پایدار- به تغییرات کوچک حالتش حساس است. تغییر بسیار کوچکی در حالت اولیه باعث تغییرات بسیار قابل‌توجه در شرایط نهایی می‌شود. نمونه معروف چنین پدیده‌ای وضعیت آب‌وهوا و پدیده معروف اثر پروانه ایست. دینامیک غیرخطی چون باعث می‌شود که به دلیل نداشتن همه شرایط اولیه در زمان شروع محاسبات (مثلاً نداشتن و همچنین عدم دقت اندازه‌گیری دما و رطوبت و... در همه‌ی نقاط سطح زمین)، پیش‌بینی طولانی‌مدت امکان‌پذیر نباشد. مثال مشهوری است که می‌گویند بال زدن پروانه‌ای در کشوری دیگر می‌تواند باعث به وجود آمدن یا نیامدن توفان در کشور شما شود. نمونه‌ای از این حساسیت در شکل (۲-۳) می‌بینید. در این شکل، دینامیک لورنز به ازای دو شرایط اولیه بسیار نزدیک به هم (با خطای $|e(0)|=10^{-5}$) مقایسه شده است. مشاهده می‌شود که در ابتدا این دو شکل بسیار شبیه به هم رفتار می‌کنند، بااین‌حال درنهایت رفتار کاملاً متفاوتی دارند.




شکل ۲-۳. دینامیک لورنز به‌ازای دو شرایط اولیه بسیار نزدیک

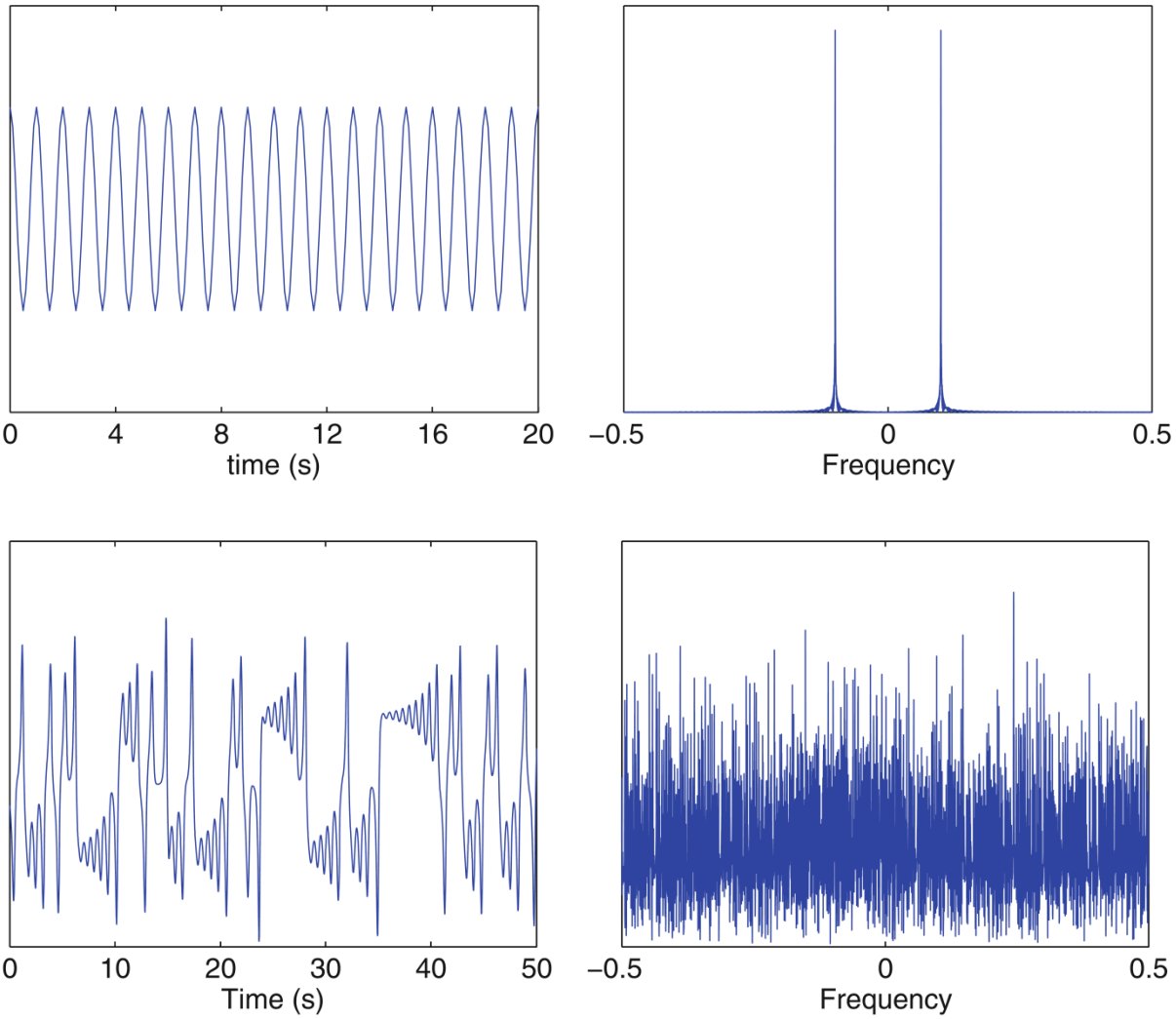
ویژگی دیگر سیستم آشوبی، داشتن جاذب شگفت[۱۶] است. به‌طور کیفی، جاذب‌های شگفت جاذب‌هایی هستند که مسیر حالت به سمت آن‌ها جذب می‌شوند و در همان حال از آن‌ها دور می‌شود. نمونه چنین جاذبی را در شکل (۲-۴) مشاهده می‌کنید که مسیر فاز دینامیک لورنز را نمایش می‌دهد.




شکل ۲-۴. نمونه‌ای از رفتار دینامیک لورنز به ازای $\sigma = 10$، $r = 28$ و $b = 8/3$

[۱۶] Strange attractor

از ویژگی‌های دیگر آشوب، وجود طیف فرکانسی پیوسته است. می‌دانیم اگر سیستمی دارای رفتار تناوبی باشد، دارای طیف گسسته ایست، اما در سیستم‌های آشوبی، طیف پیوسته خواهد بود. مقایسه‌ای بین طیف گسسته رفتاری تناوبی و طیف پیوسته رفتار آشوبی را در شکل (۲-۵) مشاهده می‌کنید.




شکل ۲-۵. مقایسه طیف فرکانسی بین حرکت متناوب و حرکت آشوبی. مشاهده می‌شود که برخلاف دینامیک متناوب، دینامیک آشوبی طیف پیوسته دارد (صفر نبودن و عرض داشتن طیف حرکت تناوبی به دلیل خطای محاسبات عددی و محدود بودن پنجره تبدیل فوریه است) [۱۲].

## ۲-۱- نگاشت‌های آشوبی:

به لحاظ ریاضی و محاسباتی حل معادله دیفرانسیل غیرخطی مشکل است؛ اما حتی مدل‌های ابتدایی می‌توانند شناختی از سازوکار آشوب ارائه دهند. این مدل‌ها به‌جای معادله‌های دیفرانسیل، در قالب معادله‌های تفاضلی بیان می‌شوند. یک نمونه معادله تفاضلی دارای شکل زیر است.

$$x_{n+1} = f(\mu, x_n) \qquad (۲-۲)$$

که در آن $x_n$ عددی حقیقی در بازه (۰،۱) مربوط به $n$امین مقدار $x$ و $\mu$ یک پارامتر است. می‌توان $nT$ را به‌صورت زمان در نظر گرفت که در آن $T$ یک بازه زمانی بنیادی است. پارامتر $\mu$ برحسب مدل تغییر می‌کند و در مثال‌هایی که بررسی می‌کنیم تغییرات آن به شروع یک رفتار آشوبناک می‌انجامد. تابع $f$ نگاشتی است از بازه (۰،۱) به خودش، چراکه $x_{n+1}$ را از $x_n$ تولید می‌کند. تابع $f(\mu, x_n)$ نیز برحسب $x_n$ غیرخطی است. معادله تفاضلی با روش تکرار به‌راحتی قابل‌حل است و حل عددی آن به زمان بسیار کمتری از معادله دیفرانسیل نیاز دارد [۱۴].

### ۲-۱-۱- نگاشت لجستیک:

این نگاشت ساده با معادله تفاضلی

$$x_{n+1} = \mu x_n(1 - x_n), \quad x_n \in [0,1] \qquad (۲-۳)$$

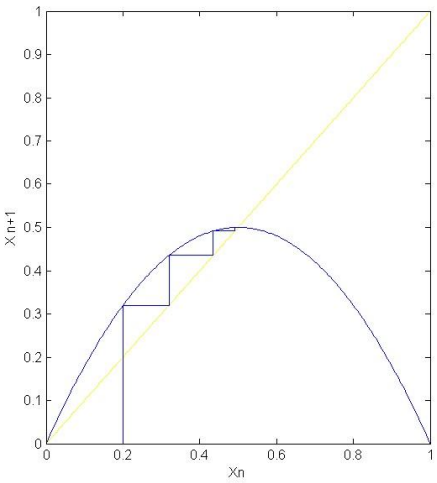
تعریف می‌شود. نام این معادله از معادله دیفرانسیل نظیر آن گرفته‌شده است

$$\frac{dx}{dt} = \mu x(1 - x) \qquad (۲-۴)$$

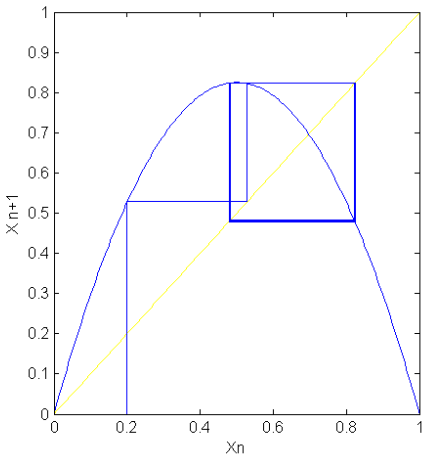
نگاشت لجستیک یک‌بعدی و غیرخطی است و می‌توان آن را به‌صورت شکل نشان داده‌شده در شکل (۲-۶) تصور کرد. نمودار دارای سه قسمت است: سهمی $y = \mu x(1-x)$، خط قطری $x_{n+1} = x_n$ و مجموعه‌ای از خط‌هایی که تکرار پی‌درپی نگاشت را به هم متصل می‌کنند. دنباله زمانی ناشی از نگاشت با انتخاب مقدار $\mu$ (در این مورد $\mu = 2$) به دست می‌آید. ابتدا منحنی درجه دوم نظیر $\mu = 2$ رسم می‌شود، سپس تولید مکرر نقطه‌های بعدی با توجه به یک مقدار اولیه (در این مورد $x_0 = 0.2$) صورت می‌گیرد. اولین نقطه، $x_1$، جایی است که خط $x_0 = 0.2$ منحنی درجه‌دو را قطع می‌کند و پس‌ازآن، مرحله بعدی به‌راحتی با حرکت افقی مشخص می‌شود، یعنی $x_{n+1} = x_n$. این فرآیند تا مرحله‌ای تکرار می‌شود که $x$ به مقدار پایای $x_{n+1} = x_n$ برسد. این نقطه ثابت زمانی حاصل می‌شود که اندازه شیب نگاشت درجایی که خط قطری را قطع می‌کند، کمتر از واحد باشد.

در شکل (۲-۶) دنباله $\{x_n\}$ به یک نقطه ثابت می‌رسد. تجربه نشان می‌دهد که به ازای تمام شرایط اولیه $x_0$ و به ازای $\mu = 2$ به نقطه ثابت قبلی می‌رسیم. مطابق شکل (۲-۷) اگر $\mu$ با مقدار تقریبی ۳/۳ افزایش یابد، وضعیت تغییر می‌کند. مطابق شکل (۲-۷) الف. منحنی درجه‌دو شیب‌دارتر می‌شود و مقدار شیب آن $|f'(x)|$ در نقطه تقاطع بزرگ‌تر از یک می‌شود. درنتیجه نقطه ثابت ناپایدار می‌شود و پس از گذر از مراحل اولیه، $x_n$ بین دو مقدار به‌گونه‌ای نوسان می‌کند که $x_{n+2} = x_n$. مطابق شکل (۲-۷) ب. اینک حرکت دوره‌ای است. مقادیر بالاتر $\mu$ به دوشاخه شدگی‌های[۱۷] بیشتر و حتی رفتار آشوبناک می‌انجامد. شکل (۲-۸) این وضعیت را برای $\mu = 3.9$ نشان می‌دهد. رفتار درازمدت آن‌چنان است که $x_n$ به چند نقطه محدود نمی‌شود بلکه قسمت بیشتر ناحیه مشخصی از منحنی را پر می‌کند و رفتار آن آشفته است.

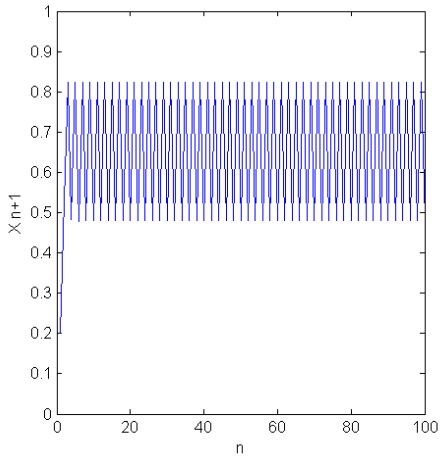
[۱۷] Bifurcation



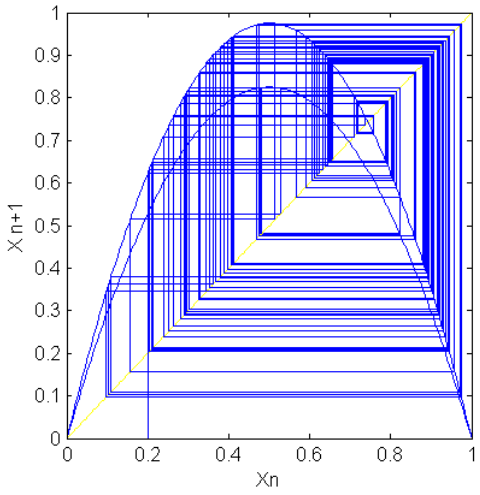

شکل ۲-۶. تحول نگاشت لجستیک به ازای $\mu = 2$. مقدار تعادل $x = 0.5$ است.



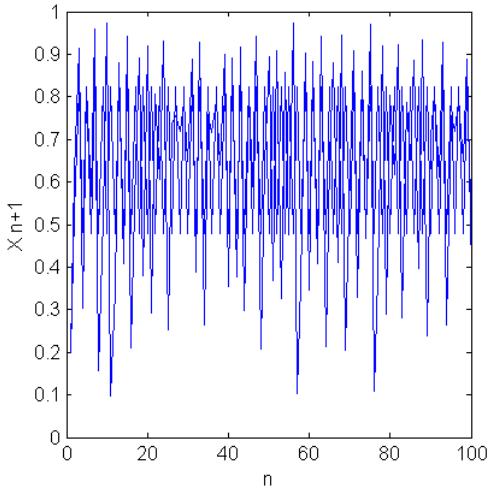

شکل ۲-۷. (الف) نگاشت لجستیک به ازای $\mu = 3.3$ نوسانی را بین دو مقدار $x = 0.48$ و $x = 0.83$ نشان می‌دهد.



شکل ۲-۷. (ب)  حرکت دوره‌ای برحسب شماره تکرار دیده می‌شود.




شکل ۲-۸. (الف) تکرار نگاشت لجستیک، در حالت آشوبناک و به ازای $\mu = 3.9$




شکل ۲-۸. (ب) حرکت آشوبناک برحسب شماره تکرار

### ۲-۱-۲- نگاشت‌های چند مدال[۱۸]:

در این بخش خانواده‌ای از نگاشت‌های چند مدال تک پارامتر معرفی می‌شود که دامنه نگاشت‌ها به زیر دامنه‌هایی بر اساس ماکزیمم تعداد مدال‌های تولیدشده تقسیم می‌شود. هر زیر دامنه شامل یک

[۱۸] Multimodal

نگاشت لجستیک است [۱۵]. نگاشت‌های آشوبی چند مدال را می‌توان برای بالا بردن امنیت سیستم‌های مخابرات آشوبی مورداستفاده قرارداد.

تعریف:

نگاشت $f_\beta$ را $k$ مدال گویند اگر پیوسته و دارای $k$ نقطه بحرانی $c_0, c_1, ..., c_{k-1}$ در بازه $I$ و به‌طور یکنواخت برای هر $(c_i, i = \{0,1,2,...,k\})$، در سمت چپ $c_i$ افزایش و در سمت راست کاهش یابد.

$f$ را یک نگاشت $k$ مدال گویند اگر بتوانیم به‌صورت ترکیبی از نگاشت‌های تک مدال $f_1, f_2, ..., f_k$ با شرایط زیر بنویسیم:

- $f_i : I_i \to I$ نقطه بحرانی یکتا دارد (یک ماکزیمم)
- $f(c_i) = f(c_j), \quad for\ i \neq j$
- $\bigcup_{i=1}^{k} I_i = I$

خانواده پارامتری شده $F$ از نگاشت‌های $f_\beta$ ، توسط تابع تکه‌ای زیر تعریف می‌شود:

$$f_\beta(x) = \beta(d_{r+1} - x)(x - d_r), \quad for\ x \in [d_r, d_{r+1}), \tag{۵-۲}$$

در این تعریف $d_r = r/k (r = \{0,1,2,...,k-1\})$ و $\beta \in J = [0, \alpha k/\gamma]$ است و برای بازه ها داریم:

$$I = \bigcup_{r=0}^{k-1} [d_r, d_{r+1}), \quad \bigcap_{r=0}^{k-1} [d_r, d_{r+1}) = \phi \tag{۶-۲}$$

برای مثال اگر $k=2$ را به عنوان تعداد مدال‌ها درنظر بگیریم، بازه به دو زیربازه $\hat{I}_0=[0,0.5)$ و $\hat{I}_1=[0.5,1]$ با ظرفیت $\gamma=0.5$ تقسیم می‌شود بنابراین $r=0,1$ و خانواده $F$ دارای دو عضو بصورت زیر می‌باشد:

۱) برای یک نگاشت دو مدال[۱۹] با $r=0$ داریم:

$$\beta=\alpha(k-r)/\gamma=(4)(2)/0.5=16$$

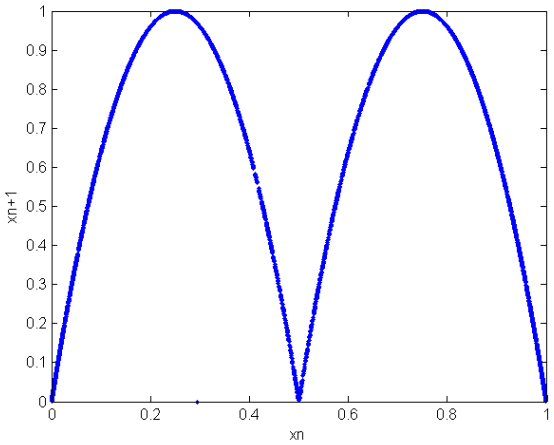
$$f_{16}(x)=16\begin{cases}(1/2-x)x & for\ x\in[0,0.5);\\ (1-x)(x-1/2) & for\ x\in[0.5,1];\end{cases}$$

۲) برای یک نگاشت تک مدال[۲۰] با $r=1$ داریم:

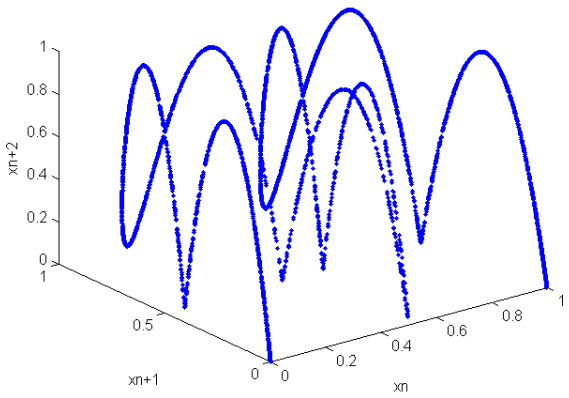
$$\beta=\alpha(k-r)/\gamma=(4)(1)/0.5=8$$

$$f_{8}(x)=8\begin{cases}(1/2-x)x & for\ x\in[0,0.5);\\ (1-x)(x-1/2) & for\ x\in[0.5,1];\end{cases}$$

[۱۹] Bimodal
[۲۰] Unimodal




شکل ۲-۹. (الف) خانواده نگاشت دومدال




شکل ۲-۹. (ب) نمایش سه بعدی دیاگرام فاز خانواده نگاشت دومدال

بدون از دست دادن کلیت مساله، حالت خاص نگاشت آشوبی چهارمدال با $k=4$ را درنظر می‌گیریم.

خانواده تک پارامتری $F$ از نگاشت های آشوبی چند مدال $f_\beta$ بصورت زیر قابل بیان است:

$$f_\beta(x)=\beta\begin{cases}(1/4-x)x & for\ x\in[0,1/4);\\ (1/2-x)(x-1/4) & for\ x\in[1/4,1/2);\\ (3/4-x)(x-1/2) & for\ x\in[1/2,3/4);\\ (1-x)(x-3/4) & for\ x\in[3/4,1];\end{cases}$$

با $k=4$، $r=0,1,2,3$، $\gamma=0.25$ و $\alpha=4$ بازه موردنظر به‌صورت $\beta\in j\in[0,64]$ تعیین می‌شود بنابراین خانواده چهارعضوی $F$ به‌صورت زیر است:

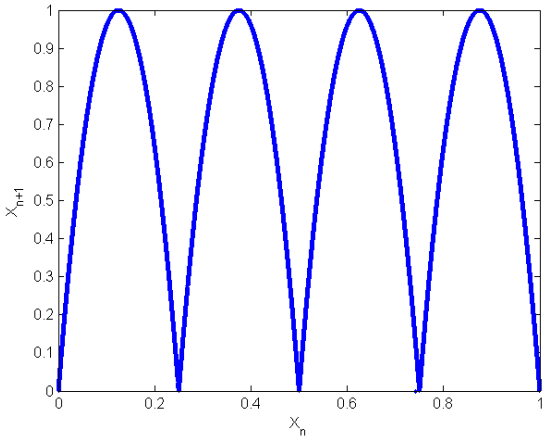
۱) نگاشت چهارمدال $f_{64}$ برای $r=0$.

۲) نگاشت سه‌مدال[۲۱] $f_{48}$ برای $r=1$.

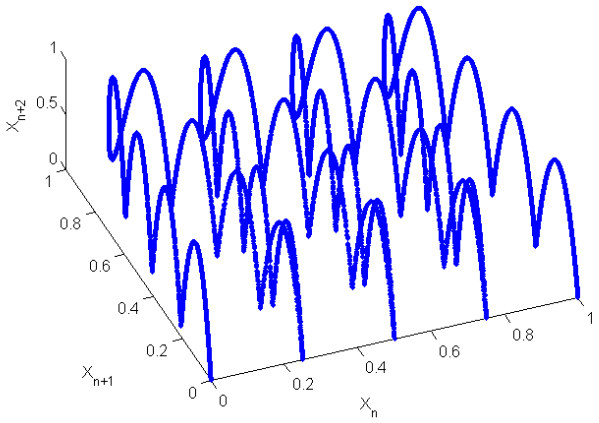
۳) نگاشت دومدال $f_{32}$ برای $r=2$.

۴) نگاشت تک‌مدال $f_{16}$ برای $r=3$.

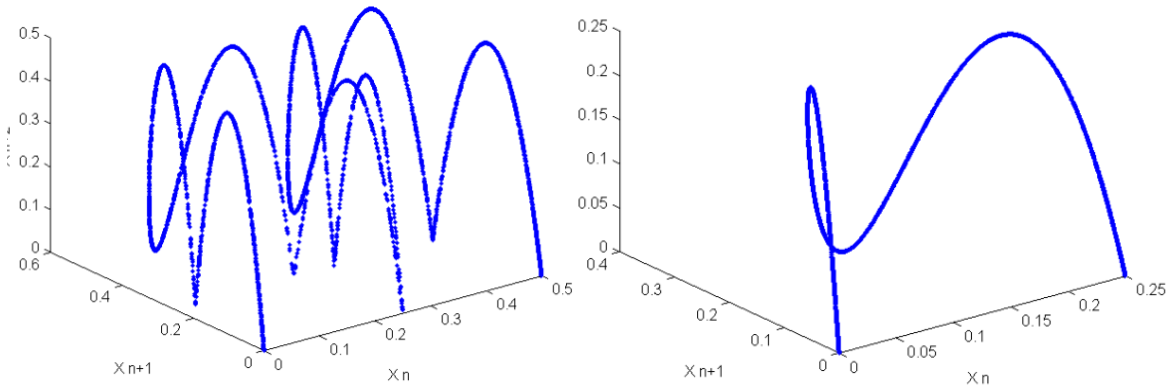
[۲۱] Trimodal



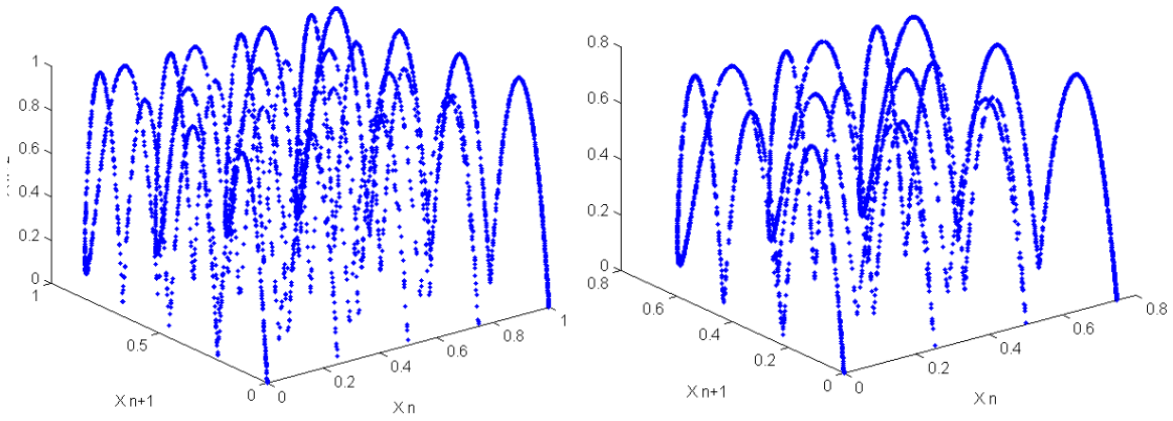

شکل ۲-۱۰. خانواده نگاشت چهارمدال




شکل ۲-۱۱. شکل سه‌بعدی فضای فاز نشان دهنده ساختار کشیدگی و تاشدگی نگاشت آشوبی چهارمدال




(ب) (الف)




(د) (ج)

شکل ۲-۱۲. شکل سه‌بعدی فضای فاز نشان دهنده ساختار کشیدگی و تاشدگی نگاشت آشوبی چهارمدال برای $k=4$: (الف) $r=3$. (ب) $r=2$. (ج) $r=1$. (د) $r=0$.

# فصل سوم: سنکرون سازی سیستم‌های آشوبی

سنکرون‌سازی[۲۲] یا همزمانی سیستم‌های دینامیکی پدیده‌ای است که در سال‌های اخیر توجه بسیاری را به خود جلب کرده است. هم‌زمانی دو سیستم دینامیکی به زبان ساده یعنی اعمال تغییراتی در دو سیستم به‌طوری‌که هردوی آن‌ها یک رفتار از خود نشان دهند. به‌عنوان‌مثال در بسیاری از روش‌های انتقال داده در سیستم‌های مخابراتی، طرف گیرنده و فرستنده هر دو می‌بایست به یک سیگنال حامل[۲۳] یکسان دسترسی داشته باشند. یکسان بودن سیگنال در مخابرات کلاسیک معادل هم فرکانس و هم‌فاز بودن دو سیگنال سینوسی است. از طرف دیگر، همزمانی در سیستم‌های آشوبناک نیز به دلیل کاربردهای متنوعش در مخابرات امن مهم است. در این نوع همزمانی خروجی دو سیستم آشوبناک می‌بایست به‌وسیله کنشی که دو سیستم توسط سیگنال کنترلی بر هم می‌گذارند تا حد ممکن یکسان شود. نکته مهم و قابل‌توجه این است که چنین کاری تا چند سال گذشته غیرممکن تلقی می‌شد. دلیل این تصور، ناپایداری ذاتی سیستم‌های آشوبی است (که با مثبت بودن نمای لیاپانوف آن نمود پیدا می‌کند) که باعث می‌شود برخلاف خیلی از سیستم‌های دیگر تفاوت بسیار جزئی در شرایط اولیه دو سیستم، تغییرات قابل‌توجهی درنتیجه نهایی ایجاد کند. پس سعی در تنظیم دقیق پارامترها و شرایط اولیه دو سیستم آشوبی، محکوم به شکست است. بااین‌حال در سال ۱۹۹۰ پکارو و کارول[۲۴] نشان دادند که در شرایطی با ایجاد سیگنال خطا و اعمال آن به سیستم می‌توان آن‌دو را همزمان کرد [۱۶]. پیش از معرفی این روش خوب است همزمانی را به‌طور ریاضی فرمول‌بندی کنیم [۱۷].

### ۳-۱- فرمول بندی همزمانی

فرض کنید $k$ سیستم متصل‌به‌هم زیر را داشته باشیم:

[۲۲] Synchronization
[۲۳] Carrier signal
[۲۴] Pecaro and Corroll

(۱-۳)

$$S_i : \dot{x}_i = F_i(x_1, x_2, ..., x_k, t) \quad i = 1, ..., k$$

که در آن $F_i : \Re^{n_1} \times \Re^{n_2} \times ... \times \Re^{n_k} \times \Re_+ \to \Re^{n_i}$. برای هر $\tau \in \Re$، اپراتور انتقال زمانی را به‌صورت $(\sigma_\tau x)(t) = x(t+\tau)$ تعریف می‌کنیم [۱۲]. تابع $Q$ را بر روی $x_i(t)$ها تعریف می‌کنیم.

### ۳-۱-۱- تعریف همزمانی

پاسخ $x_1(t)$، $x_2(t)$، ... و $x_k(t)$ سیستم‌های $S_1$، $S_2$، ... و $S_k$ با شرایط اولیه $x_1(0)$، $x_2(0)$، ... و $x_k(0)$ را با توجه به فراتابع[۲۵] $Q_i(x_1, ..., x_k, t)$ همزمان است اگر

$$Q_i(\sigma_{\tau_1} x_1, ..., \sigma_{\tau_k} x_k, t) \equiv 0, \qquad i = 1, ..., k \qquad (۲-۳)$$

رابطه به ازای $\forall t \in \Re$ و مقادیری از $\tau_1, ..., \tau_k$ می‌باشد.

این سیستم‌ها به‌طور تقریبی همزمان‌اند اگر همه‌ی شرایط مانند قبل باشد و همچنین وجود داشته باشد $\varepsilon \in \Re$ که

$$|Q_i(\sigma_{\tau_1} x_1, ..., \sigma_{\tau_k} x_k, t)| < \varepsilon, \quad i = 1, ..., k \qquad (۳-۳)$$

در ضمن $S_1, ..., S_k$ به‌طور مجانبی همزمان است اگر

$$\lim_{t \to \infty} Q_i(\sigma_{\tau_1} x_1, ..., \sigma_{\tau_k} x_k, t) = 0, \quad i = 1, ..., k \qquad (۴-۳)$$

[۲۵] Functional

در همه‌ی این تعارف اگر به‌جای $Q_i(x_1,...,x_k,t)$ها از $Q_i(y_1,...,y_k,t)$ استفاده کنیم که $y_i(t)=h_i(x_i(t))$ خروجی سیستم‌ها باشند به هم‌زمانی خروجی[۲۶] نیز قابل‌تعمیم است [۱۲]. برای تعمیم بیش‌تر می‌توان $\tau_i$ها را نیز متغیر با زمانی گرفت که دارای حد مشخص و ثابتی هستند.

حالت خاص این تعاریف وقتی است که برای ارتباط دو سیستم تعریف کنیم:

$$Q_1(x_1,x_2)=Q_2(x_1,x_2)=Q(x_1,x_2)=|x_1(t)-x_2(t)| \qquad (۵-۳)$$

اینک مسئله همزمان کردن دو سیستم معادل می‌شود با پیدا کردن سیگنال کنترلی که این سیستم‌ها را با توجه به یکی از این شرایط هم‌زمانی، هم‌زمان کند.

### ۳-۲- مروری بر سنکرون سازی های انجام شده

در این بخش تعدادی از سنکرون سازی‌های انجام‌شده به همراه نتایج، مزایا و معایب آن‌ها را مرور می‌کنیم. به‌طورکلی طراحی سیستمی که بتواند رفتار یک سیستم آشوبی را دنبال کند سنکرون سازی گفته می‌شود که بنا به تعریف به سیستم نخست پایه[۲۷] و به سیستم دوم پیرو[۲۸] گویند.

سنکرون سازی سیستم‌های آشوبی در زمینه‌های بسیار زیادی مانند فیزیک، سیستم‌های مهندسی مانند مبدل‌های قدرت، واکنش‌های شیمیایی، سیستم‌های بیولوژیکی، پردازش اطلاعات و به‌خصوص در مخابرات امن کاربرد دارند [۱۸-۲۱]. خصوصیت مشترک سیستم های آشوبی داشتن رفتار غیرقابل پیش بینی و حساسیت بسیار زیاد به شرایط اولیه است بطوریکه با کوچکترین تغییر در شرایط اولیه پاسخ ها بسیار متفاوت خواهند شد [۲۲]. در مدولاسیون آشوبی برای استخراج اطلاعات در گیرنده باید بین گیرنده و فرستنده سنکرون سازی روی دهد. برای سنکرون سازی سیستم‌های آشوبی

[۲۶] Output sychronization
[۲۷] Master
[۲۸] Slave

روش‌های متعددی ارائه‌شده است مانند کنترل مقاوم[۴]، کنترل حالت لغزشی[۲۹][۵]، کنترل تطبیقی [۶-۸]، کنترل بهینه[۹]، و... . در این نوع سنکرون سازی‌ها دو سیستم گیرنده و فرستنده آشوبی باقی می‌مانند ولی یکی با دیگری سنکرون می‌شوند (دو سیستم آشوبی در گیرنده و فرستنده در شرایط اولیه متفاوت کار می‌کنند).

### ۳-۲-۱- سنکرون سازی مقاوم شبه مد لغزشی[۳۰]

در این روش طراحی کنترل‌کننده شبه مد لغزشی برای سنکرون سازی سیستم‌های آشوبی لورنز تعمیم‌یافته بررسی خواهد شد [۴]. این روش برای جلوگیری از پدیده چترینگ که اغلب در کنترل معمولی مد لغزشی ظاهر می‌شود ارائه‌شده است که می‌توان خطای بین سیستم‌های پایه و پیرو را پایدار و به‌صورت دلخواه و قابل پیش‌بینی به همسایگی از صفر هدایت کرد.

یکی از روش‌های موردتوجه به‌منظور سنکرون سازی سیستم‌های آشوبی روش کنترل مد لغزشی است که این روش درواقع یک استراتژی کنترل غیر پیوسته بوده و شامل دو مرحله انتخاب سطح لغزش مناسب به‌منظور قرارگیری حالت‌ها بر آن و سپس طراحی یک قانون کنترل غیر پیوسته برای ماندن مسیر سیستم بر سطح موردنظر و رسیدن به عملکرد کنترلی مطلوب است.

در سیستم‌های کنترل مد لغزشی معمولی اغلب پدیده مخرب چتریگ به وجود می‌آید که روش‌های مختلفی برای غلبه بر این پدیده ارائه‌شده است؛ بنابراین روش کنترل مد لغزشی که نه‌تنها سنکرون سازی بدون چترینگ را نتیجه دهد بلکه بتواند عملکرد کنترلی را پیش‌بینی کند، ضروری است. در ادامه دینامیک سیستم‌های آشوبی لورنز تعمیم‌یافته، تعریف خطا، مسئله سنکرون سازی، تعریف مانیفولد شبه مد لغزشی و دینامیک‌های خطا در مانیفولد شبه مد لغزشی بیان می‌شود. در بخش نهایی هم یک QSMC برای تضمین دقت مانیفولد[۳۱] شبه لغزشی ارائه‌شده است.

---

[۲۹] Sliding Mode Control
[۳۰] Quasi sliding mode control(QSMC)
[۳۱] Manifold

### ۳-۱-۱- توصیف سیستم و معادلات

در این قسمت سنکرون سازی مقاوم دو سیستم لورنز تعمیم یافته [۳۲] یکسان با یک کنترل‌کننده شبه مد لغزشی را بیان می‌کنیم. سیستم‌های لورنز عموماً به‌صورت زیر بیان می‌شوند:

$$\begin{aligned}\dot{x}_1(t) &= (10+\frac{25}{29}k).[x_2(t)-x_1(t)]\\ \dot{x}_2(t) &= (25+\frac{35}{29}k)x_1(t)+(k-1)x_2(t)-x_1(t)x_3(t)\\ \dot{x}_3(t) &= (-\frac{8}{3}-\frac{1}{87}k)x_3(t)+x_1(t)x_2(t)\end{aligned} \qquad (۶-۳)$$

$$[x_1(0)\ x_2(0)\ x_3(0)]^T = [x_{10}\ x_{20}\ x_{30}]^T$$

که $x(t)=[x_1(0)\ x_2(0)\ x_3(0)]^T = R^3$ بردار حالت، $[x_{10}\ x_{20}\ x_{30}]^T$ بردار شرایط اولیه سیستم و $0 \le k < 1$ پارامتر سیستم است. سیستم اصلی لورنز زمانی به دست می‌آید که $k=0.3$ قرار دهیم. رفتار این سیستم به‌طور کامل در [۲۳] به ازای تغییرات مقادیر مختلف $k$ در بازه $0 \le k < 1$ بررسی‌شده است. در این سنکرون سازی دو سیستم آشوبی لورنز تعمیم‌یافته در نظر می‌گیریم و روند طراحی یک کنترل‌کننده شبه مد لغزشی را بیان می‌کنیم.

دو سیستم لورنز با متغیرهای $x$ و $y$ را که به ترتیب سیستم‌های پایه و پیرو هستند را به‌صورت زیر در نظر می‌گیریم:

الف) سیستم پایه:

$$\begin{aligned}\dot{x}_1(t) &= (10+\frac{25}{29}k).[x_2(t)-x_1(t)]\\ \dot{x}_2(t) &= (25+\frac{35}{29}k)x_1(t)+(k-1)x_2(t)-x_1(t)x_3(t)\\ \dot{x}_3(t) &= (-\frac{8}{3}-\frac{1}{87}k)x_3(t)+x_1(t)x_2(t)\end{aligned} \qquad (۷-۳)$$

ب) سیستم پیرو:

[32] Generalized chaotic Lorenz systems

$$\dot{y}_1(t) = (10 + \frac{25}{29}k).[y_2(t) - y_1(t)]$$
$$\dot{y}_2(t) = (25 + \frac{35}{29}k)y_1(t) + (k-1)y_2(t) - y_1(t)y_3(t) + d(t) + u(t) \qquad (۸-۳)$$
$$\dot{y}_3(t) = (-\frac{8}{3} - \frac{1}{87}k)y_3(t) + y_1(t)y_2(t)$$

در حالت کلی عدم قطعیت $d(t)$ را به‌صورت $|d(t)| \le \alpha$ که $\alpha \ge 0$ در نظر می‌گیریم.

به‌منظور سنکرون سازی دو سیستم بیان‌شده، سیگنال کنترلی ورودی $u$ را در معادله دوم سیستم پیرو قرار می‌دهیم و خطای سنکرون سازی را به‌صورت زیر تعریف می‌کنیم:

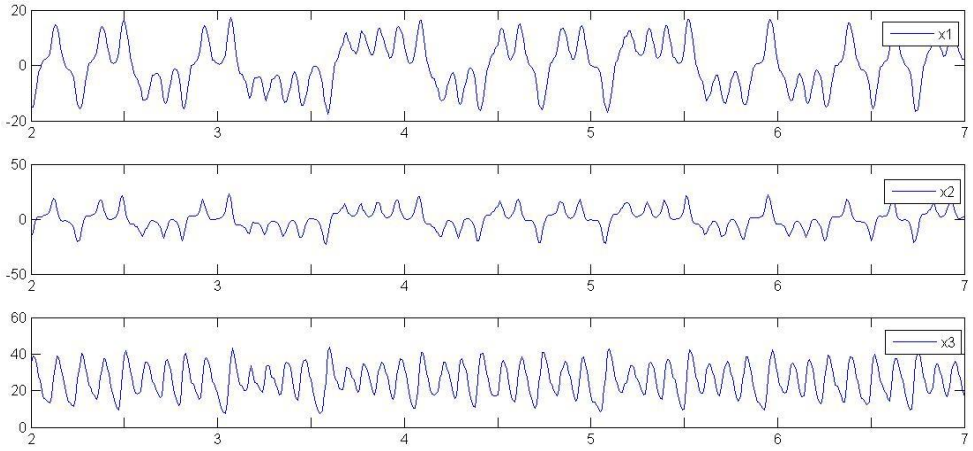
$$E(t) = [e_1(t) \quad e(t)_2 \quad e(t)_3]^T = [y_1(t) - x_1(t) \quad y_2(t) - x_2(t) \quad y_3(t) - x_3(t)]^T \qquad (۹-۳)$$

بنابراین دینامیک خطا سیستم مستقیماً از تفاضل معادلات به‌صورت زیر به دست می‌آید:

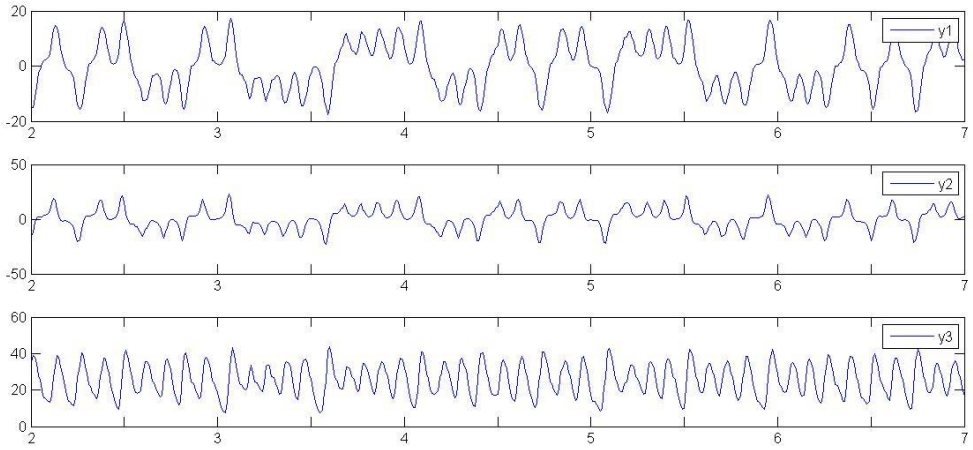
$$\dot{e}_1(t) = (10 + \frac{25}{29}k).[e_2(t) - e_1(t)]$$
$$\dot{e}_2(t) = (25 - \frac{35}{29}k)e_1(t) + (k-1)e_2(t) - y_1(t)y_3(t) + x_1(t)x_3(t) + d(t) + u(t) \qquad (۱۰-۳)$$
$$\dot{e}_3(t) = (-\frac{8}{3} - \frac{1}{87}k)e_3(t) + y_1(t)y_2(t) - x_1(t)x_2(t)$$

هدف از ارائه این روش این است که خطای سنکرون سازی به‌صورت محدود و قابل پیش‌بینی $\lim_{t\to\infty}|e_i| \le \varepsilon_i, i = 1,2,3$ به دست آید. مقادیر ثابت $\varepsilon_i \ge 0$ وابسته به پارامترهای انتخاب‌شده در طراحی کنترل‌کننده شبه مد لغزشی است که در ادامه به آن خواهیم پرداخت.

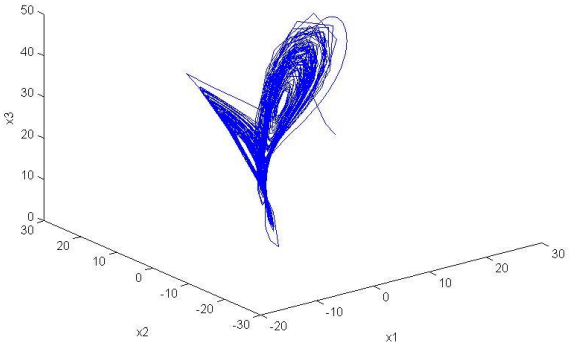
نمودار حالت‌های سیستم‌های پایه و پیرو در شکل ۳-۱ و ۳-۲ نشان داده‌شده است. برای تضمین رفتار آشوبی سیستم لورنز $k = 0.3$ را در نظر گرفته و شرایط اولیه سیستم‌های پایه و پیرو را به ترتیب $x_1(0) = 22$، $x_2(0) = 15$، $x_3(0) = 12$ و $y_1(0) = 20$، $y_2(0) = 13$، $y_3(0) = 12$ انتخاب می‌کنیم. عدم قطعیت یکسان را $d(t) = 0.2\sin(2t) \to |d(t)| \le \alpha$ در نظر می‌گیریم.




شکل ۳-۱. سری‌های زمانی سیستم پایه با شرایط اولیه $x_1(0)=22$، $x_2(0)=15$ و $x_3(0)=12$.




شکل ۳-۲. سری‌های زمانی سیستم پیرو با حضور عدم قطعیت با شرایط اولیه $y_1(0)=20$، $y_2(0)=13$ و $y_3(0)=12$.




شکل ۳-۳. نمودار سه‌بعدی دینامیک‌های سیستم لورنز

### ۳-۱-۲- تعریف مانیفولد شبه لغزشی و طراحی سطح سویچینگ

تابع سویچینگ به‌صورت $s(t)=e_2(t)+\lambda e_1(t)$ تعریف می‌شود که $s\in R$ و $\lambda>-1$ ثابت‌های طراحی هستند.

قبل از ادامه بحث، مانیفولد شبه لغزشی را به‌صورت زیر تعریف می‌کنیم.

**تعریف ۱:**

خطای سیستم در مانیفولد شبه لغزشی قرار دارد اگر $\delta_Q>0$ و $t_Q>0$ وجود داشته باشد بطوریکه هر پاسخ $x(\cdot)$ خطا سیستم (۳-۱۰) در $|s(t)|\le\delta_Q$ برای تمام $t\ge t_Q$ صدق کند.

بنابراین دینامیک خطای $e_1(t)$ به‌صورت زیر به دست می‌آید:

$$\dot{e}_1(t)=(10+\frac{25}{29}k).[s(t)-\lambda e_1(t)-e_1(t)]=-\lambda_1 e_1(t)+(10+\frac{25}{29}k)s(t) \qquad (۱۱-۳)$$

که داریم:

$$\lambda_1=(10+\frac{25}{29}k).[1+\lambda] \qquad (۱۲-۳)$$

با حل معادله دیفرانسیل بالا داریم:

$$e_1(t) = e^{-\lambda_1(t-t_Q)}e_1(t_Q) + \int_{t_Q}^{t} e^{-\lambda_1(t-\tau)}[(10+\frac{25}{29}k).s(\tau)]d\tau \qquad (۱۳-۳)$$

طبق تعریف ۱ وقتی سیستم در مانیفولد شبه لغزشی قرار دارد، $\delta_Q > 0$ است بنابراین کران $e_1(t)$ به‌صورت زیر تخمین زده می‌شود:

$$|e_1(t)| = |e^{-\lambda_1(t-t_Q)}e_1(t_Q) + \int_{t_Q}^{t} e^{-\lambda_1(t-\tau)}[(10+\frac{25}{29}k).s(\tau)]d\tau|$$

$$\le e^{-\lambda_1(t-t_Q)}|e_1(t_Q)| + \int_{t_Q}^{t} e^{-\lambda_1(t-\tau)}|[(10+\frac{25}{29}k).s(\tau)]|d\tau$$

$$\le e^{-\lambda_1(t-t_Q)}|e_1(t_Q)| + [(10+\frac{25}{29}k).\delta_Q]e^{-\lambda_1 t}\int_{t_Q}^{t} e^{-\lambda_1\tau}d\tau$$

$$= e^{-\lambda_1(t-t_Q)}|e_1(t_Q)| + [(10+\frac{25}{29}k).\delta_Q]\frac{1-e^{-\lambda_1(t-t_Q)}}{\lambda_1} \qquad (۱۴-۳)$$

تا هنگامی‌که $\lambda > -1$، داریم $\lambda_1 = \left(10+\frac{25}{29}k\right)(1+\lambda) > 0$ و کران به‌صورت زیر به دست می‌آید:

$$\lim_{t\to\infty}|e_1(t)| \le \varepsilon_1 = \left[\left(10+\frac{25}{29}k\right)\delta_Q\right]/\lambda_1 = \frac{\delta_Q}{1+\lambda} \qquad (۱۵-۳)$$

همچنین می‌توان با استفاده از رابطه $s(t) = e_2(t) + \lambda e_1(t)$ کران $e_2(t)$ زمانی که $t \to \infty$ را محاسبه نمود:

$$\lim_{t\to\infty}|e_2(t)| = \lim_{t\to\infty}|s(t) - \lambda e_1(t)| \le \lim_{t\to\infty}|s(t)| + \lim_{t\to\infty}|\lambda||e_1(t)| \le \varepsilon_2$$
$$= \delta_Q + |\lambda|\varepsilon_1 \qquad (۱۶-۳)$$

همان‌طور که $e_1(t)$ و $e_2(t)$ به ترتیب به $\varepsilon_1$ و $\varepsilon_2$ همگرا می‌شود، $t_\varepsilon$ وجود دارد بطوریکه برای $t \ge t_\varepsilon$ داریم:

$$|e_i| \le \varepsilon_i \, , i = 1,2 \qquad (۱۷-۳)$$

بنابراین با حل معادله دیفرانسیل (۳-۱۰) برای $t \ge t_\varepsilon$ داریم:

$$e_3(t) = e^{-(\frac{8}{3}+\frac{1}{87}k)(t-t_\varepsilon)} e_3(t_\varepsilon) + \int_{t_\varepsilon}^{t} e^{-(\frac{8}{3}+\frac{1}{87}k)(t-\tau)} [y_1(\tau)y_2(\tau) + x_1(\tau)x_2(\tau)]d\tau \qquad (۱۸-۳)$$

برای $t \ge t_\varepsilon$ داریم:

$$\begin{aligned} &| y_1(t)y_2(t) + x_1(t)x_2(t) | \\ &=| x_2(t)e_1(t) + y_1(t)e_2(t) | \\ &=| x_2(t)e_1(t) + (e_1(t)e_2(t) + x_1(t)e_2(t)) | \\ &\le \varepsilon_1\varepsilon_1 + | x_1(t) | \varepsilon_2 + | x_2(t) | \varepsilon_1 \end{aligned} \qquad (۱۹-۳)$$

بعلاوه بر اساس قضیه ۱ در [۲۴] پاسخ حالت سیستم لورنز تعمیم‌یافته در کره $\Omega$ قرار می‌گیرد. داریم:

$$\Omega = \left\{ [x_1, x_2, x_3] \middle| {x_1}^2 + {x_2}^2 + (x_3 - 38 + \frac{10k}{29})^2 = R^2 \right\} \qquad (۲۰-۳)$$

$$R^2 = \frac{(19 - \frac{5k}{29})^2 (8 + \frac{k}{29})^2}{(15 - \frac{264k}{29})(1-k)} \qquad (۲۱-۳)$$

بنابراین با استفاده از رابطه (۳-۱۹)، (۳-۲۰) و (۳-۲۱) برای $t \ge t_\varepsilon$

$$| y_1(t)y_2(t) + x_1(t)x_2(t) | \le R(\varepsilon_1 + \varepsilon_2) + \varepsilon_1\varepsilon_2 \qquad (۲۲-۳)$$

و

(۲۳-۳)

$$|e_3(t)|=|e^{-(\frac{8}{3}+\frac{1}{87}k)(t-t_\varepsilon)}e_3(t_\varepsilon)+\int_{t_\varepsilon}^{t}e^{-(\frac{8}{3}+\frac{1}{87}k)(t-\tau)}[y_1(\tau)y_2(\tau)+x_1(\tau)x_2(\tau)]d\tau|$$

$$\le e^{-(\frac{8}{3}+\frac{1}{87}k)(t-t_\varepsilon)}|e_3(t_\varepsilon)|+(R(\varepsilon_1+\varepsilon_2)+\varepsilon_1\varepsilon_2).e^{-(\frac{8}{3}+\frac{1}{87}k)t}\int_{t_\varepsilon}^{t}e^{-(\frac{8}{3}+\frac{1}{87}k)\tau}d\tau$$

$$=e^{-(\frac{8}{3}+\frac{1}{87}k)(t-t_\varepsilon)}|e_3(t_\varepsilon)|+(R(\varepsilon_1+\varepsilon_2)+\varepsilon_1\varepsilon_2).\frac{1-e^{-(\frac{8}{3}+\frac{1}{87}k)(t-t_\varepsilon)}}{\frac{8}{3}+\frac{1}{87}k}$$

با محاسبات بالا کران $e_3(t)$ زمانی $t\to\infty$ که به‌صورت زیر به دست می‌آید:

$$\lim_{t\to\infty}|e_3(t)|\le\varepsilon_{31}=\frac{[R(\varepsilon_1+\varepsilon_2)+\varepsilon_1\varepsilon_2]}{\left(\frac{8}{3}+\frac{k}{87}\right)} \qquad (۲۴-۳)$$

### ۳-۱-۳- طراحی کنترل‌کننده شبه مد لغزشی برای مانیفولد شبه لغزشی

با محقق ساختن سطح سویچ مناسب و تخمین کران خطای حالت‌های سیستم در مانیفولد شبه لغزشی، این بخش برای رسیدن به طراحی کنترل‌کننده شبه مد لغزشی بیان می‌شود. برای تضمین وقوع مانیفولد شبه لغزشی، کنترل‌کننده شبه مد لغزشی پیوسته زیر پیشنهاد می‌شود [4].

$$u(t)=-w\eta\frac{s}{|s|+\delta} \qquad (۲۵-۳)$$

که

$$\eta=|[(28-\frac{35}{29}k)-\lambda(10+\frac{25}{29}k)e_1(t)+[(k-1)+\lambda(10+\frac{25}{29}k)e_2(t)]-y_1(t)y_3(t)+x_1(t)x_3(t)|+\alpha \qquad (۲۶-۳)$$
$$w>1,\delta>0$$

روش طراحی کنترل ارائه‌شده وقوع مانیفولد شبه لغزشی را برای سیستم (۳-۱۰) تضمین می‌کند (در

پیوست الف اثبات این روش بیان‌شده است).

### ۳-۱-۴- شبیه‌سازی

در این بخش نتایج شبیه‌سازی برای نشان دادن و اثبات مؤثر بودن روش کنترل شبه مد لغزش بیان‌شده است. پارامترهای سیستم را به‌صورت زیر انتخاب می‌کنیم:

برای تضمین رفتار آشوبی سیستم لورنز $k=0.3$ را در نظر گرفته و شرایط اولیه سیستم‌های پایه و پیرو را به ترتیب $x_1(0)=22$، $x_2(0)=15$، $x_3(0)=12$ و $y_1(0)=20$، $y_2(0)=13$، $y_3(0)=12$ انتخاب می‌کنیم. عدم قطعیت یکسان را $d(t)=0.2\sin(2t)\rightarrow|d(t)|\le\alpha$ در نظر می‌گیریم.

**گام اول:** طبق رابطه $s(t)=e_2(t)+\lambda e_1(t)$ پارامتر $\lambda=1>0$ را برای اینکه $\lambda_1=\left(10+\frac{25}{29}k\right)(1+\lambda)>0$ حاصل شود و کران پایدار دینامیک خطای سیستم (۳-۲۵) را تضمین نماید انتخاب می‌کنیم.

**گام دوم:** پارامترهای کنترل در رابطه (۳-۲۵) به‌صورت $\delta=0.03$ و $w=4$ انتخاب کرده و بر اساس قضیه ۱ $\delta_Q=0.04$ به دست می‌آید.

با انتخاب $\lambda$ برای سطح سویچینگ $s(t)$ داریم:

$$s(t)=e_2(t)+e_1(t) \qquad (۳-۲۷)$$

**گام سوم:** با توجه به روابط (۳-۱۵)، (۳-۱۶) و (۳-۲۰) کران قابل پیش‌بینی $\varepsilon_i, i=1,2,3$ را به‌صورت زیر محاسبه می‌کنیم:

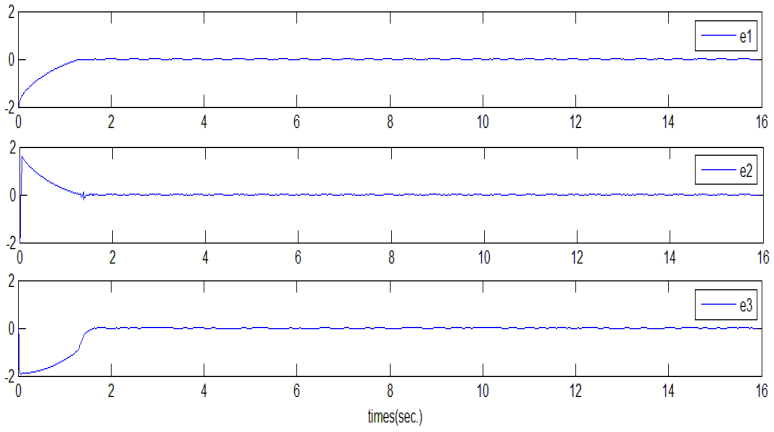
$$|e_1|\le\varepsilon_1=0.02;|e_2|\le\varepsilon_2=0.06;|e_3|\le\varepsilon_3=1.29 \qquad (۳-۲۸)$$

**گام چهارم:** با استفاده از رابطه (۳-۲۷) کنترل‌کننده شبه مد لغزشی به‌صورت زیر حاصل می‌شود:

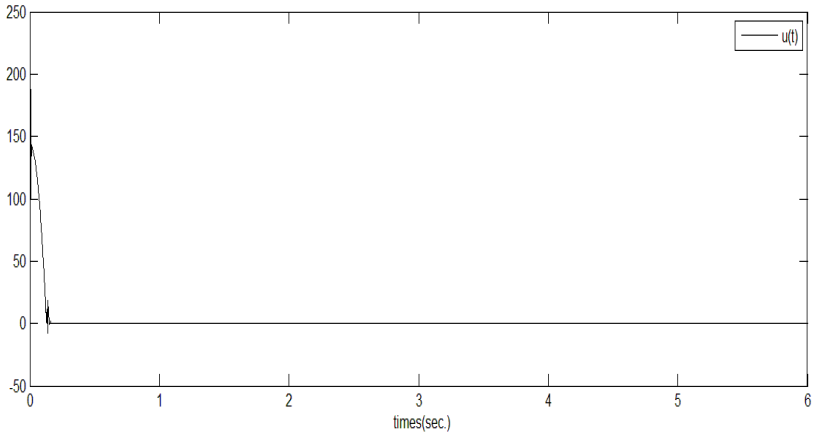
$$u(t) = -4\eta \frac{s}{|s| + 0.03} \qquad (۲۹-۳)$$

$$\eta = |[(28 - \frac{35}{29}k) - \lambda(10 + \frac{25}{29}k)e_1(t) + [(k-1) + \lambda(10 + \frac{25}{29}k)e_2(t)] - y_1(t)y_3(t) + x_1(t)x_3(t)| + 0.2 \qquad (۳۰-۳)$$

نتایج شبیه‌سازی در شکل‌های ۳-۴ و ۳-۵ نشان داده‌شده است. شکل ۳-۴ پاسخ‌های زمانی حالت خطا و این نکته که درنهایت این پاسخ به ناحیه محاسبه‌شده در (۳-۳۰) محدود می‌شود را نشان می‌دهد. شکل ۳-۵ پاسخ کنترل‌کننده شبه مد لغزشی و نشان‌دهنده کارایی مناسب و عدم وجود چترینگ در این کنترل‌کننده است.




شکل ۳-۴. پاسخ‌های زمانی حالت خطا




شکل ۳-۵ پاسخ کنترل‌کننده شبه مد لغزشی

همانطور که در شکل ۳-۴ مشاهده می‌شود در این روش می توان حالت های خطا را پایدار و به‌صورت دلخواه و قابل پیش‌بینی به همسایگی از صفر هدایت کرد.

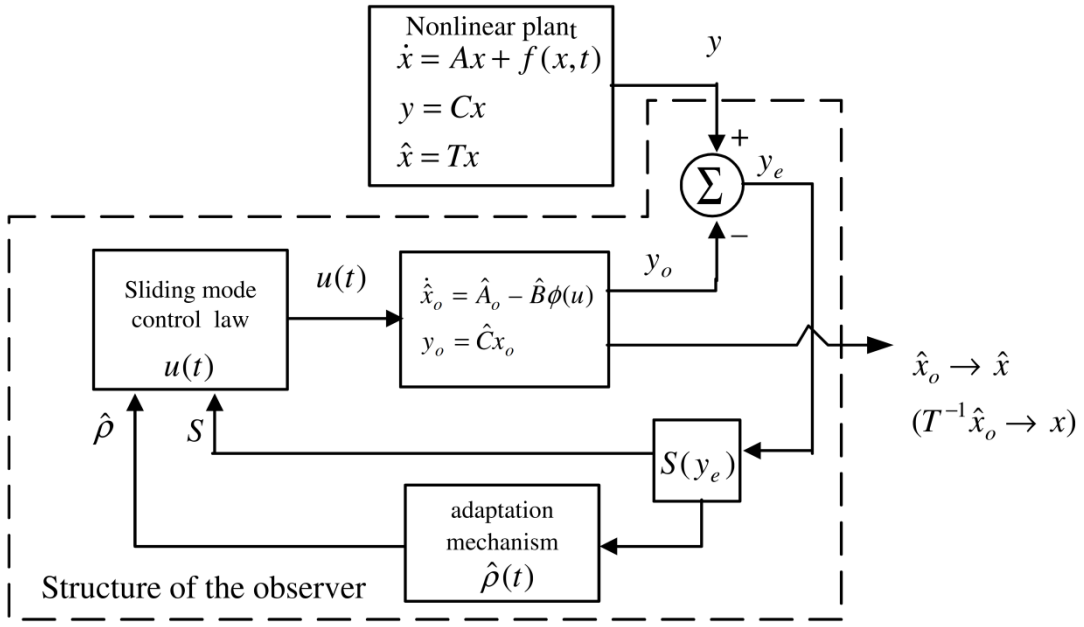
### ۳-۲-۲- سنکرون سازی سیستم‌های فوق آشوب چند متغیره راسلر با استفاده از رویتگر مد لغزشی- تطبیقی

در این شبیه‌سازی سنکرون سازی و کنترل سیستم‌های فوق آشوبی راسلر[۳۳] با ماتریس تبدیل چند متغیره[۳۴] به روش مد لغزشی- تطبیقی ارائه‌شده است. این روش مقاومت بیشتری نسبت به نویز و عدم تطابق پارامتر در دینامیک‌های خطا داشته و نیاز به در نظر گرفتن باندهای بالا[۳۵] در نامعینی‌ها ندارد [۷]. آنالیزهای تئوری و شبیه‌سازی‌های انجام‌شده صحت این روش را تأیید می‌کنند.

### ۳-۲-۱- تعریف مسئله و طراحی رویتگر:

رویتگر مد لغزشی- تطبیقی شامل یک سیستم غیرخطی، کنترلر مد لغزشی و مکانیزم تطبیق نشان داده‌شده در شکل (۳-۶) است.

[۳۳] Rossler hyper chaotic system
[۳۴] Multivariable transmission
[۳۵] Upper bounds




شکل ۳-۶. رویتگر مد لغزشی - تطبیقی فیدبک خروجی[۷].

سیستم غیره خطی زیر را در نظر بگیرید:

$$\dot{x}(t) = Ax + Bf(x,t)$$
$$y(t) = Cx(t) \qquad (۳۱-۳)$$

ماتریس‌های $(A,B)$ کنترل‌پذیر، ماتریس‌های $(A,C)$ روئیت پذیر و $B$ رنک کامل دارد. $p \geq m$ تعداد کانال‌های خروجی بزرگ‌تر یا مساوی تعداد ورودی‌ها است و $rank(CB) = m$.

فرض‌های بالا محدودکننده نمی‌باشند و بسیاری از سیستم‌های غیرخطی آشوبی همانند سیستم راسلر در این موارد صدق می‌کنند [۲۵].

ماتریس تبدیل حالت را به‌صورت زیر در نظر می‌گیریم:

$$\hat{x}(t) = Tx(t) = \left[\frac{T_1}{T_2}\right]x(t) \qquad (۳۲-۳)$$

تبدیل $T$ طوری انتخاب می‌شود که:

$$TB = \begin{bmatrix} T_1 B \\ T_2 B \end{bmatrix} = \begin{matrix} 0 \\ B_1 \end{matrix} \qquad (۳۳-۳)$$

در این تبدیل چون فرض شده که رنک $B$ کامل است، همواره وجود دارد و همچنین $T_1, T_2, B_1$ غیر تکین[۳۶] است.

بنابراین با ماتریس $\hat{x}(t)$ داریم:

$$\begin{aligned} \dot{\hat{x}}(t) &= \hat{A}\hat{x}(t) + \hat{B}f(T^{-1}\hat{x}, t) \\ y(t) &= \hat{C}\hat{x}(t) \end{aligned} \qquad (۳۴-۳)$$

که:

$$\hat{A} \equiv TAT^{-1} = \begin{bmatrix} A_{11}{}_{(n-m)\times(n-m)} & A_{12}{}_{(n-m)\times m} \\ \hat{A}_{21}{}_{m\times(n-m)} & \hat{A}_{22}{}_{m\times m} \end{bmatrix} \qquad (۳۵-۳)$$

$$\hat{B} \equiv TB = \begin{bmatrix} 0_{(n-m)\times m} \\ B_{1m\times n} \end{bmatrix} \qquad (۳۶-۳)$$

$$C \equiv CT^{-1} = [\hat{C}_{1p\times(n-m)} \quad \hat{C}_{2p\times m}] \qquad (۳۷-۳)$$

از رویتگر مد لغزشی که ارائه خواهیم داد برای بازسازی حالت‌های سیستم زیر استفاده می‌کنیم:

[۳۶] Nonsingular

$$\dot{\hat{x}}_0(t) = \hat{A}\hat{x}_0(t) + \hat{B}f(T^{-1}\hat{x}_0, t) - \hat{B}\phi(u(t))$$
$$y_0(t) = \hat{C}\hat{x}_0(t) \qquad (۳۸-۳)$$

$u(t) \in R^m$ کنترل ورودی است و غیرخطی توصیف‌شده به‌صورت $\phi(u(t))$ یک تابع پیوسته در ناحیه $[\beta_1, \beta_2]$ [۲۶, ۲۷].

به‌عنوان‌مثال:

$$\beta_1 u^T(t)u(t) \le u^T(t)\phi(u(t)) \le \beta_2 u^T(t)u(t) \qquad (۳۹-۳)$$

که $\beta_1, \beta_2$ ثابت‌های مثبت غیر صفر هستند و $\phi(0) = 0$.

بردارهای خطا را به‌صورت زیر تعریف می‌کنیم:

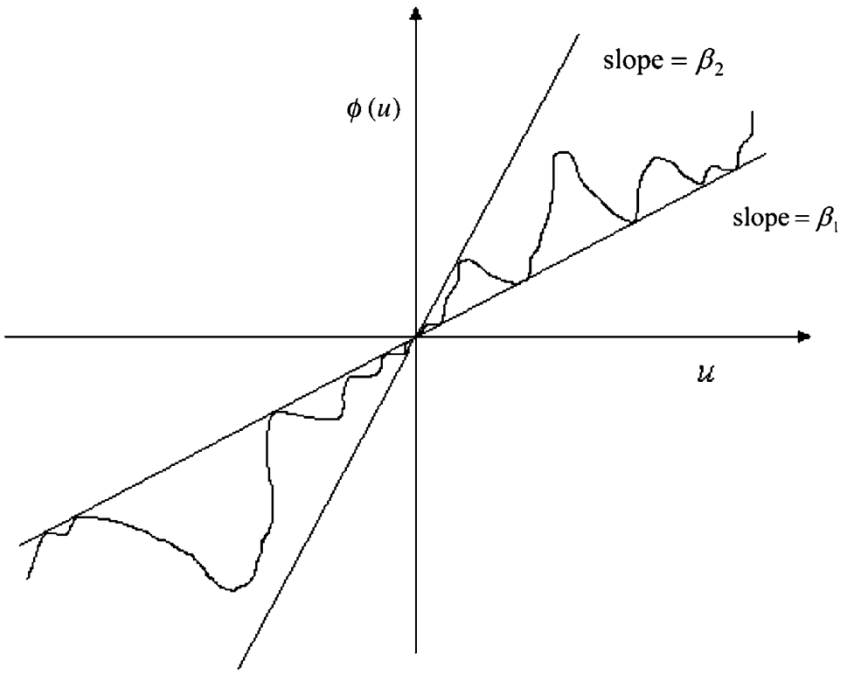
$$e(t) = \hat{x}(t) - \hat{x}_0(t)$$
$$y_e(t) = y(t) - y_0(t) \qquad (۴۰-۳)$$

معادلات دینامیک خطای سیستم به‌صورت زیر به دست می‌آید:

$$\begin{bmatrix} \dot{e}_1(t) \\ \dot{e}_2(t) \end{bmatrix} = \begin{bmatrix} \hat{A}_{11} & \hat{A}_{12} \\ \hat{A}_{21} & \hat{A}_{22} \end{bmatrix} \begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} + \begin{bmatrix} 0 \\ B_1 \end{bmatrix} (f(T^{-1}\hat{x}, t) - f(T^{-1}\hat{x}_0, t)) + \begin{bmatrix} 0 \\ B_1 \end{bmatrix} \phi(u(t))$$
$$y_e(t) = \begin{bmatrix} \hat{C}_1 & \hat{C}_2 \end{bmatrix} \begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} \qquad (۴۱-۳)$$

هدف این است که یک رویتگر با کنترلر تطبیقی با استفاده از اندازه‌گیری خروجی $y(t)$ در دسترس طراحی کنیم بطوریکه حالت‌های رویتگر بتوانند این پلانت غیرخطی را دنبال کنند و داشته باشیم $\lim_{t\to\infty} e(t) = 0$.

بدین منظور احتیاج به انتخاب سطح سویچ مناسبی برای دینامیک‌های خطا داریم، بطوریکه حرکت لغزشی بروی مانیفولد دارای خصوصیات مطلوب باشد و همچنین تعیین کنترل مد لغزشی تطبیقی فیدبک خروجی[۳۷] برای تضمین وجود مد لغزشی حتی تنها با اندازه‌گیری $y(t)$ در دسترس از پلانت، موردنیاز است.




شکل ۳-۷. تابع غیرخطی اسکالر $\phi(u)$ در محدوده $[\beta_1 \quad \beta_2]$ [۷].

### ۳-۲-۲- سطح سویچینگ و طراحی کنترلر:

[۳۷] Adaptive output feedback sliding mode control (AOFSMC)

مزیت کنترل تطبیقی این است که به معادله ریاضی دقیق برای توصیف باندهای بالای عدم قطعیت احتیاجی نیست. کنترل مد لغزشی یک کنترل غیرخطی است که نسبت به نویز و نامعینی پارامترها مقاوم است.

مشابه [۲۸] داریم:

$$S(y_e) = Fy_e = F\hat{C}e(t) \qquad (۴۲-۳)$$

که $F \in R^{m\times p}$ یک ماتریس ثابت و $S(y_e) \in R^{m\times l}$

انتخاب $F$ به طراحی مد لغزشی بستگی دارد.

$$S(y_e) = \sigma e(t) \qquad (۴۳-۳)$$

بدون از دست دادن کلیت مسئله داریم:

$$S(y_e) = \sigma_1 e_1(t) + \sigma_2 e_2(t) \qquad (۴۴-۳)$$

دقت کنید که $\sigma$ قابل‌تغییر و ماتریس $F$ باید طوری انتخاب شود که شرط $\sigma = F\hat{C}$ برآورده سازد.

برای تعیین $\sigma$ همانند [۲۹] طوری انتخاب می‌کنیم که تعداد $(n-m)$ مقدار ویژه مختلط و غیر صفر $\{\lambda_1, \lambda_2, ..., \lambda_{n-m}\}$ دارای قسمت حقیقی منفی باشد.

$e_2$ را برحسب $e_1$ و $S$ بیان می‌کنیم:

$$e_2(t) = \sigma_2^{-1}(-\sigma_1 e_1(t) + S(y_e)) \qquad (۴۵-۳)$$

$$\begin{aligned} \dot{e}_1(t) &= (\hat{A}_{11} - \hat{A}_{12}\sigma_2^{-1}\sigma_1)e_1(t) + \hat{A}_{12}\sigma_2^{-1}S(y_e) \\ \dot{e}_2(t) &= (\hat{A}_{21} - \hat{A}_{22}\sigma_2^{-1}\sigma_1)e_1(t) + \hat{A}_{22}\sigma_2^{-1}S(y_e) + B_1\phi(u(t)) + B_1(f(T^{-1}\hat{x},t) - f(T^{-1}\hat{x}_0,t)) \end{aligned} \qquad (۴۶-۳)$$

مقادیر ویژه $(\hat{A}_{11} - \hat{A}_{12}\sigma_2^{-1}\sigma_1)$ همان $\{\lambda_1, \lambda_2, ..., \lambda_{n-m}\}$ است.

هنگامی‌که سیستم در حالت مد لغزشی است معادلات زیر برآورده می‌شوند:

$$\begin{aligned} S(y_e) &= 0 \\ \dot{S}(y_e) &= 0 \end{aligned} \qquad (۴۷-۳)$$

که به دست می‌آید:

$$\begin{aligned} \dot{e}_1(t) &= (\hat{A}_{11} - \hat{A}_{12}\sigma_2^{-1}\sigma_1)e_1(t) \\ e_2(t) &= -\sigma_2^{-1}\sigma_1 e_1(t) \end{aligned} \qquad (۴۸-۳)$$

تا زمانی که $(\hat{A}_{11} - \hat{A}_{12}\sigma_2^{-1}\sigma_1)$ یک ماتریس پایدار باشد $\|e_1(t)\| \to 0$ و بنابراین $\|e_2(t)\| \to 0$ تضمین خواهد شد.

با انتخاب کنترل ورودی به‌صورت زیر مسیر حالت[۳۸] سیستم به سمت سطح لغزش موردنظر خواهد رفت.

[۳۸] Trajectory

$$u(t) = -\gamma k \hat{\rho}(t) \frac{B_1^T \sigma_2^T S(y_e)}{\left\| B_1^T \sigma_2^T S(y_e) \right\|} \qquad (۴۹-۳)$$

که:

$$k = \max(\left\| \sigma \hat{A} \right\|, \left\| \sigma_2 B_1 \right\|), \gamma > \frac{(B_1^T \sigma_2^T)^{-1}}{\beta_1} \qquad (۵۰-۳)$$

به دلیل اینکه کنترل تطبیقی باند بالای نامعینی را در نظر نمی‌گیرد، طراحی قانون تطبیق را به‌صورت $\dot{\hat{\rho}}(t) = k\left\| S(y_e) \right\|; \hat{\rho}(0) = \hat{\rho}_0$ در نظر می‌گیریم.

که $k > 0$، $\rho_0$ مثبت و مقدار ویژه محدود $\hat{\rho}(t)$ و برای تمام $t > 0$، $\hat{\rho}(t) > 0$.

**قضیه ۱:**

سیستم غیرخطی (۳-۳۳) و سیستم رویتگر (۳-۴۰) با اعمال قانون کنترل (۳-۵۰) و قانون تطبیق (۳-۵۱) در نظر بگیرید. نمودار فضای حالت دینامیک‌های خطا (۳-۴۳) به مانیفولد لغزش $S(y_e) = 0$ میل می‌کنند (اثبات همگرایی در پیوست ب بیان شده است).

### ۳-۲-۳- شبیه‌سازی:

**مثال ۱:**

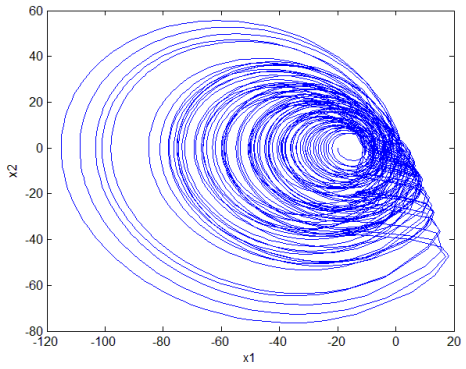
سیستم فوق آشوب راسلر زیر که نشان‌دهنده واکنش شیمیایی ارائه‌شده در [۲۵] است را در نظر بگیرید. این سیستم بااینکه دارای یک ترم غیرخطی است بااین‌حال دارای دو نمای لیاپانف مثبت $\lambda_1 = 0.11$ و $\lambda_1 = 0.02$ است [۳۰].

$$\dot{x}(t)=\begin{bmatrix}\dot{x}_1(t)\\ \dot{x}_2(t)\\ \dot{x}_3(t)\\ \dot{x}_4(t)\end{bmatrix}=\begin{bmatrix}0 & -1 & 0 & -1\\ 1 & a & 1 & 0\\ 0 & 0 & c & -0.5\\ 0 & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}x_1(t)\\ x_2(t)\\ x_3(t)\\ x_4(t)\end{bmatrix}+\begin{bmatrix}0\\ 0\\ 0\\ 1\end{bmatrix}\left[b+x_1(t)x_4(t)\right]$$

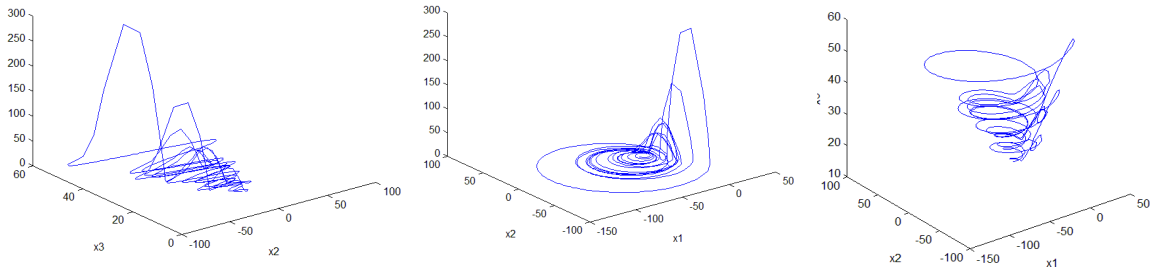
$$y(t)=\begin{bmatrix}0 & 1 & 0 & 1.5\\ 0 & 0 & 1 & -1\end{bmatrix}x(t)$$

$a,b,c$ پارامترهای کنترل برای این اسیلاتور هستند.

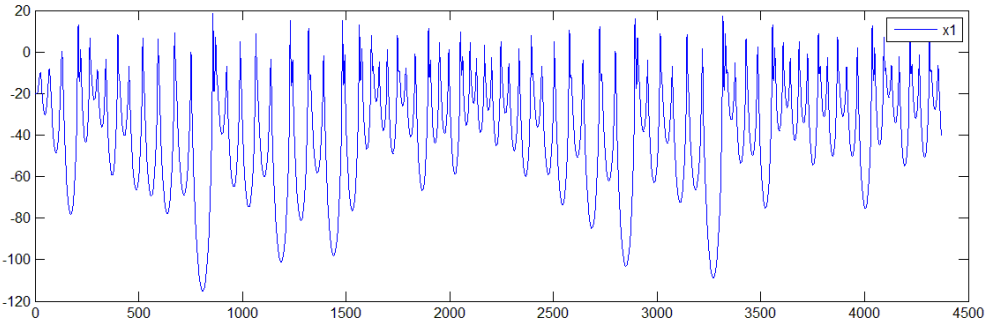
با قرار دادن مقادیر $a=0.25,b=3,c=0.05$ سیستم فوق آشوب راسلر در شکل‌های زیر رسم شده است.

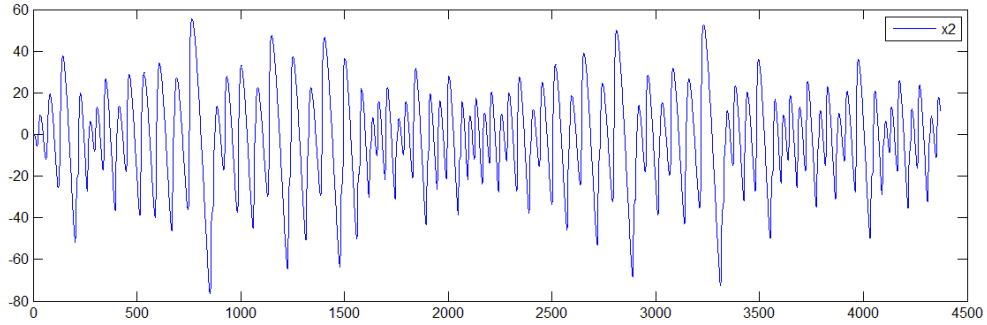


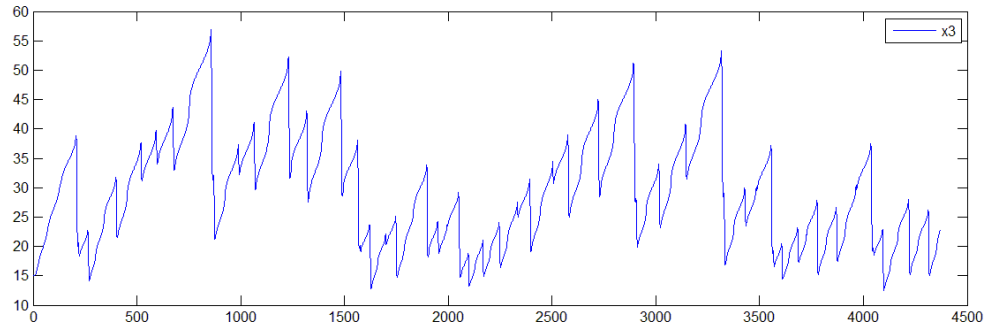

شکل ۳-۸. شکل دو بعدی سیستم فوق آشوب راسلر

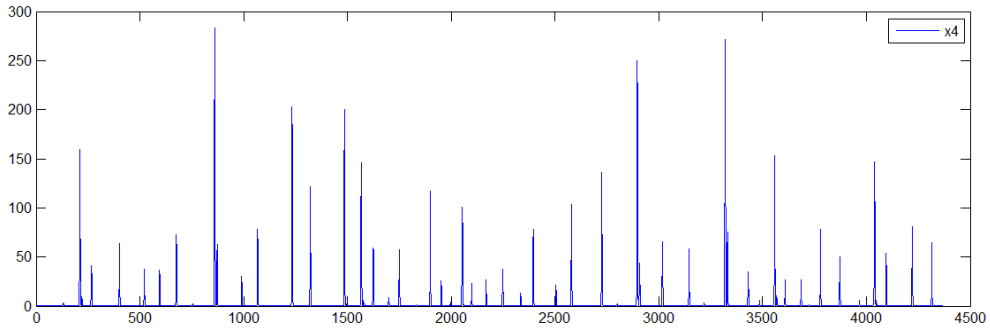



شکل ۳-۹. شکل‌های سه‌بعدی سیستم فوق آشوب راسلر






شکل ۳-۱۰. سری‌های زمانی سیستم راسلر با حضور عدم قطعیت

رویتگر را به‌صورت زیر در نظر می‌گیریم:

$$\dot{\hat{x}}(t)=\begin{bmatrix}\dot{\hat{x}}_{01}(t)\\ \dot{\hat{x}}_{02}(t)\\ \dot{\hat{x}}_{03}(t)\\ \dot{\hat{x}}_{04}(t)\end{bmatrix}=\begin{bmatrix}0 & -1 & 0 & -1\\ 1 & a & 1 & 0\\ 0 & 0 & c & -0.5\\ 0 & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}\hat{x}_{01}(t)\\ \hat{x}_{02}(t)\\ \hat{x}_{03}(t)\\ \hat{x}_{04}(t)\end{bmatrix}+\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\left[3+\hat{x}_{01}(t)\hat{x}_{04}(t)\right]-\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\phi(u(t))$$

$$y_0(t)=\begin{bmatrix}0 & 1 & 0 & 1.5\\ 0 & 0 & 1 & -1\end{bmatrix}\hat{x}_0(t)$$

غیرخطی ورودی را به‌صورت $\phi(u(t))=(0.7+0.2\sin(u))u(t)$ تعریف می‌کنیم.

با توجه به رابطه (۳-۴۱) $\beta_1=0.5$، $\beta_2=0.9$ و از قرار گرفتن مقادیر ویژه $(\hat{A}_{11}-\hat{A}_{12}\sigma_2^{-1}\sigma_1)$ در $\{-0.654 \quad -0.523\pm j1.598\}$ مقدار $\sigma=[0\,2\,4-1]$ و با حل معادله $\sigma=F\hat{C}$ مقدار $F=[2\,4]$ به دست می‌آید.

بنابراین سطح لغزش به‌صورت زیر حاصل می‌شود:

$$S(t)=Fy_e(t)=2y_{e1}(t)+4y_{e2}(t)$$

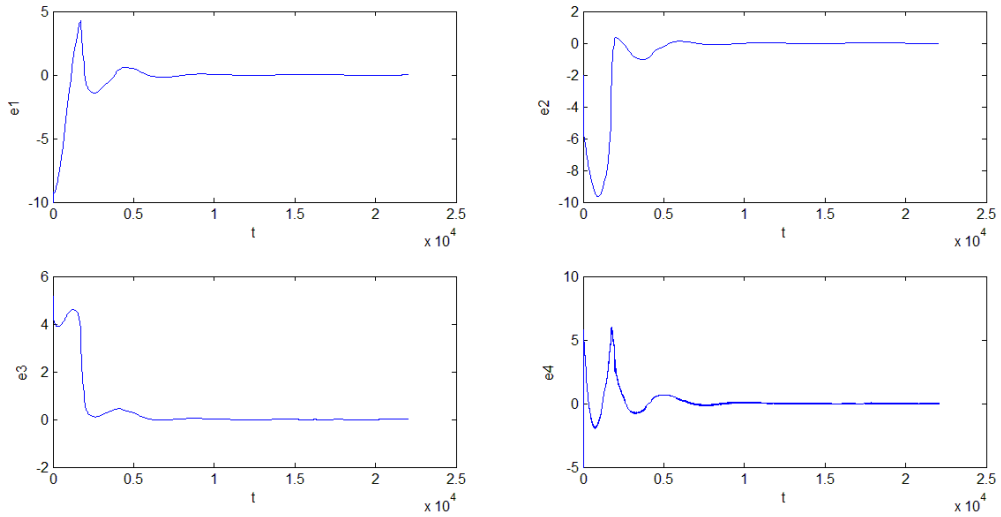
پارامترهای زیر را در نظر می‌گیریم:

$$k=3.62=\max(\|\sigma\hat{A}\|,\|\sigma_2 B_1\|)=\max(3.62,1)\ ,\quad \gamma=2.1>1/\beta_1=2$$

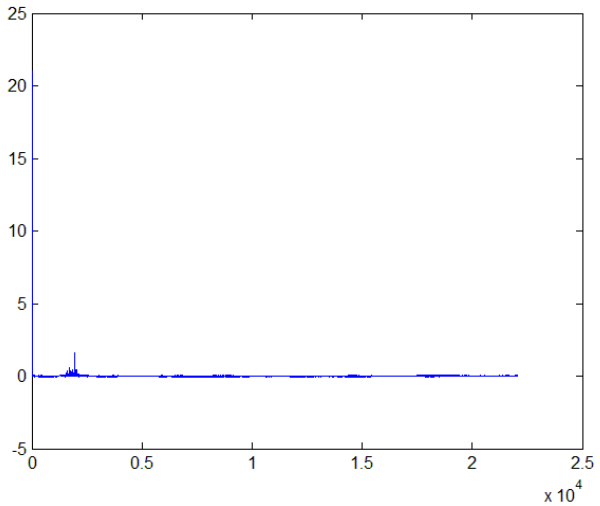
و برای شرایط اولیه داریم:

$$(x_1(0), x_2(0), x_3(0), x_4(0)) = (-20,0,15,0)$$
$$(\hat{x}_{01}(0), \hat{x}_{02}(0), \hat{x}_{02}(0), \hat{x}_{03}(0)) = (-10,2,10,5)$$

نتایج شبیه‌سازی در شکل‌های زیر نشان داده‌شده است.




شکل ۳-۱۱. پاسخ‌های زمانی حالت خطا سیستم فوق آشوب راسلر




شکل ۳-۱۲. پاسخ‌های زمانی $S(y_e)$

**مثال ۲:**

برای اثبات مقاوم بودن روش مد لغزشی تطبیقی، سیستم درایو مثال قبل را با پارامترها و نویز به‌صورت زیر در نظر می‌گیریم:

$$a = 0.255, \quad b = 3.1, \quad c = 0.049, \quad f(t) = 4.6\sin 100t$$

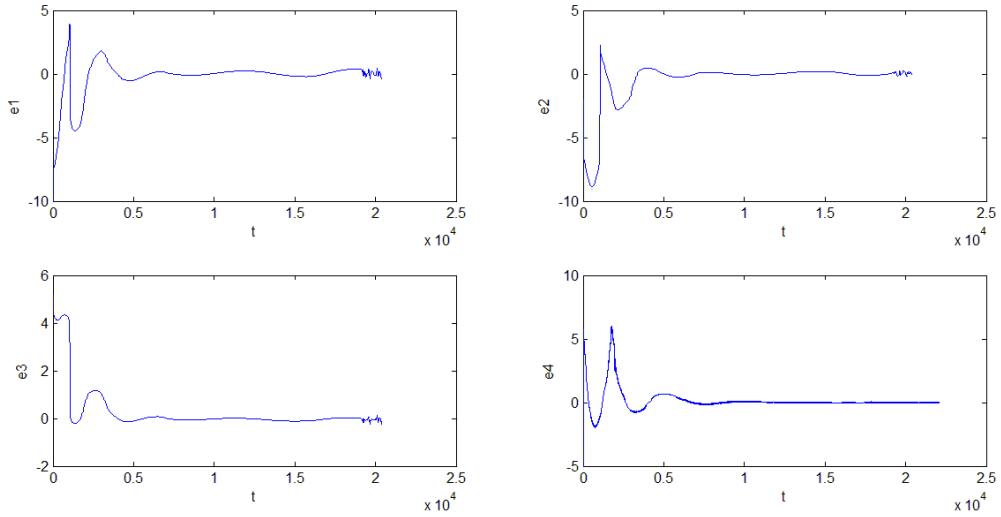
$$\dot{x}(t) = \begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \\ \dot{x}_3(t) \\ \dot{x}_4(t) \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & -1 \\ 1 & 0.255 & 1 & 0 \\ 0 & 0 & 0.049 & -0.5 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \left[3.1 + x_1(t)x_4(t) + 4.6\sin 100t\right]$$

رویتگر را به شکل زیر تشکیل می‌دهیم:

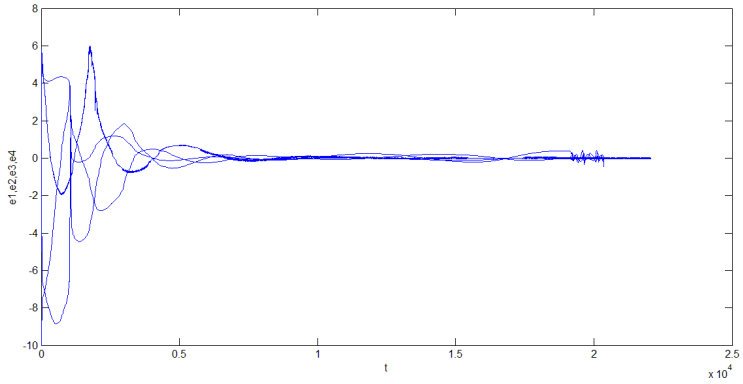
$$\dot{\hat{x}}(t) = \begin{bmatrix} \dot{\hat{x}}_{01}(t) \\ \dot{\hat{x}}_{02}(t) \\ \dot{\hat{x}}_{03}(t) \\ \dot{\hat{x}}_{04}(t) \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & -1 \\ 1 & 0.25 & 1 & 0 \\ 0 & 0 & 0.05 & -0.5 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \hat{x}_{01}(t) \\ \hat{x}_{02}(t) \\ \hat{x}_{03}(t) \\ \hat{x}_{04}(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \left[3 + \hat{x}_{01}(t)\hat{x}_{04}(t) + 4.6\sin 100t\right] - \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \phi(u(t))$$

$$y_0(t) = \begin{bmatrix} 0 & 1 & 0 & 1.5 \\ 0 & 0 & 1 & -1 \end{bmatrix} \hat{x}_0(t)$$

نتایج شبیه‌سازی در شکل‌های زیر نشان داده‌شده است.




شکل ۳-۱۳. پاسخ‌های زمانی حالت خطا سیستم فوق آشوب راسلر




شکل ۳-۱۴. نمایش همزمان پاسخ‌های زمانی حالت خطا سیستم فوق آشوب راسلر

از نتایج شبیه‌سازی به دست می‌آید که هرگاه عدم تطابق پارامتری و نویز وجود ندارد هنگامی‌که کنترلر عمل می‌کند سطح لغزش $S(y_e)$ به‌سرعت به سمت صفر میل می‌کند و سیستم‌های درایو و پاسخ باهم سنکرون می‌شوند و همچنین زمانی که عدم تطابق پارامتری و نویز وجود دارند نیز این سنکرون سازی به‌خوبی انجام می‌شود.

### ۳-۲-۳- کنترل تطبیقی سیستم غیرخطی مرتبه دوم اسیلاتور دافینگ

در این بخش سنکرون سازی به روش کنترل تطبیقی برای سیستم غیرخطی مرتبه دوم اسیلاتور دافینگ[۳۹] موردبررسی قرار می‌گیرد. غیرخطی یک ورودی مرتبه $n$ با ساختار کلی زیر را در نظر می‌گیریم:

$$\dot{x}_1 = x_2,$$
$$\dot{x}_2 = x_3,$$
$$.$$
$$.$$
$$.$$

$$\dot{x}_n = \sum_{k=1}^{N} \theta_k^{*} f_k(x) + u \qquad (۵۱-۳)$$

که در آن $x = [x_1 ... x_n]^T$ حالت‌ها، $u$ ورودی و $\theta^* = [\theta_1^* ... \theta_1^*]$ پارامترهای نامشخص سیستم هستند بطوریکه بازه‌های هرکدام از $\theta_k^*$ها معین و در محدوده $(\theta^k{}_{\min}, \theta^k{}_{\max})$ است. $f_k(x)$ تابع‌های غیر خطی‌های منظم و یکنواختی به‌صورت $f_k(x) = a(x)/b(x)$ در نظر گرفته می‌شود که $a(x)$ برای $x$ های محدود، محدود بوده و همچنین دارای شرط $b(x) \neq 0$ است.

هدف طراحی کنترلر تطبیقی برای اطمینان از پایداری مجانبی همه‌جایی برای سنکرون سازی متغیرهای حالت $x(x)$ با متغیرهای حالت سیستم ثانویه $x_m(x)$ است.

برای به دست آوردن کنترلر تطبیقی خطای دینامیکی سیستم را به‌صورت زیر تعریف می‌کنیم:

$$e(t) = x(t) - x_m(t) \qquad (۵۲-۳)$$

[۳۹] Duffing osilator

داریم:

$$\dot{e}_1 = e_2,$$
$$\dot{e}_2 = e_3,$$
.
.
.

$$\dot{e}_n = \sum_{k=1}^{N} \theta_k^{*} f_k(x) + u - \dot{x}_{m,n}. \qquad (۵۳-۳)$$

برای اثبات پایداری و به دست آوردن قوانین تطبیق از تابع لیاپانوف زیر استفاده می‌کنیم:

$$V = \frac{1}{2}(e_2 + \alpha e_1)^2 + \frac{1}{2\gamma}(\hat{\theta} - \theta^*)^2 \qquad (۵۴-۳)$$

همگرایی پارامتر $\hat{\theta}$ به مقدار واقعی $\theta^*$ زمانی اتفاق می‌افتد که مسیر حالت[۴۰] مرجع $x_m(x)$ تحریک پایا[۴۱] باشد. می‌توان نشان داد برای اطمینان از همگرایی و سنکرون سازی سیستم و صفر شدن خطا داریم [۳۱, ۳۲]:

$$u = \dot{x}_{m,2} - \alpha e_2 - (e_2 + \alpha e_1) - \hat{\theta}(t) f(x_1, x_2) \qquad (۵۵-۳)$$

$$\dot{\hat{\theta}} = \gamma(e_2 + \alpha e_1) f(x_1, x_2) \qquad (۵۶-۳)$$

(برای تمام $\alpha$ها و $\gamma$های مثبت)

[۴۰] Trajectory
[۴۱] Persistently exciting

مقدار اولیه $\hat{\theta}(0)$ را می‌توانیم به‌صورت دلخواه در نظر بگیریم اما برای اطمینان از حاصل شدن پایداری مجانبی منطقی است که این مقدار را از $(\theta_{\min}, \theta_{\max})$ انتخاب کنیم.

گاهی مواقع ممکن است با انتخاب یک مقدار اولیه برای پارامتر، مقدار نهایی حاصله در بازه محدود موردنظر قرار نگیرد. برای اینکه تخمین پارامترها به‌طورقطع در محدوده موردنظر قرار بگیرد قانون تطبیق پارامتر را اصلاح می‌کنیم [۳۳]. همانند قبل برای به دست آوردن قوانین فوق از تابع لیاپانوف به‌صورت زیر استفاده می‌کنیم:

$$V = \frac{1}{2}(e_2 + \alpha e_1)^2 + \frac{1}{2\gamma}[(\bar{\theta} - \theta^*)^2 - (\bar{\theta} - \hat{\theta})^2] \qquad (۵۷-۳)$$

بنابراین داریم:

$$u = \dot{x}_{m,2} - \alpha e_2 - (e_2 + \alpha e_1) - \hat{\theta}(t) f(x_1, x_2) \qquad (۵۸-۳)$$

$$\dot{\hat{\theta}} = \gamma(e_2 + \alpha e_1) f(x_1, x_2) - \sigma(\bar{\theta} - \hat{\theta}) \qquad (۵۹-۳)$$

$$\hat{\theta} = \begin{cases} \bar{\theta} & if\ \bar{\theta} \in (\theta_{\min}, \theta_{\max}) \\ \theta_{\min} & if\ \bar{\theta} \le \theta_{\min} \\ \theta_{\max} & if\ \bar{\theta} \ge \theta_{\max} \end{cases} \qquad (۶۰-۳)$$

حال برای بررسی صحت سنکرون سازی و قوانین تطبیق موردنظر معادله درجه دوم اوسیلاتور دافینگ را به‌صورت زیر در نظر می‌گیریم:

$$\dot{x}_1 = x_2$$
$$\dot{x}_2 = -\theta_1^* x_1 - \theta_2^* x_2 - \theta_3^* x_1^3 + u$$

مقدار صحیح پارامترهای نامعین را به‌صورت زیر در نظر می‌گیریم:

$$\theta_1^* = -0.8, \quad \theta_2^* = -0.4, \quad \theta_3^* = -1.8$$

بازه هرکدام از پارامترها به‌صورت زیر است:

$$\theta_1^* \in (-2.0,1.0), \quad \theta_2^* \in (-0.5,-0.1), \quad \theta_3^* \in (-1.2,1-2.0)$$

مقدار اولیه پارامترها:

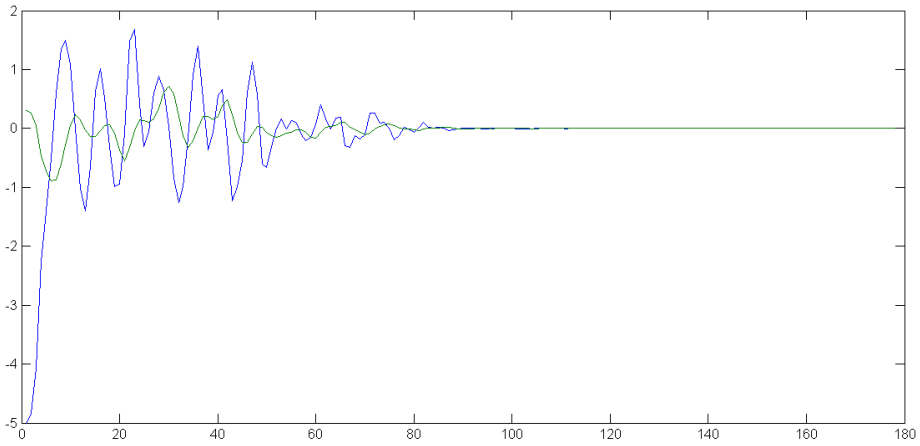
$$\theta_1(0) = -1.5, \quad \theta_2(0) = -0.2, \quad \theta_3(0) = -1.75$$

$$x(0) = [0.5,-2]^T, \quad x_m(0) = [0.2,3.0]^T$$

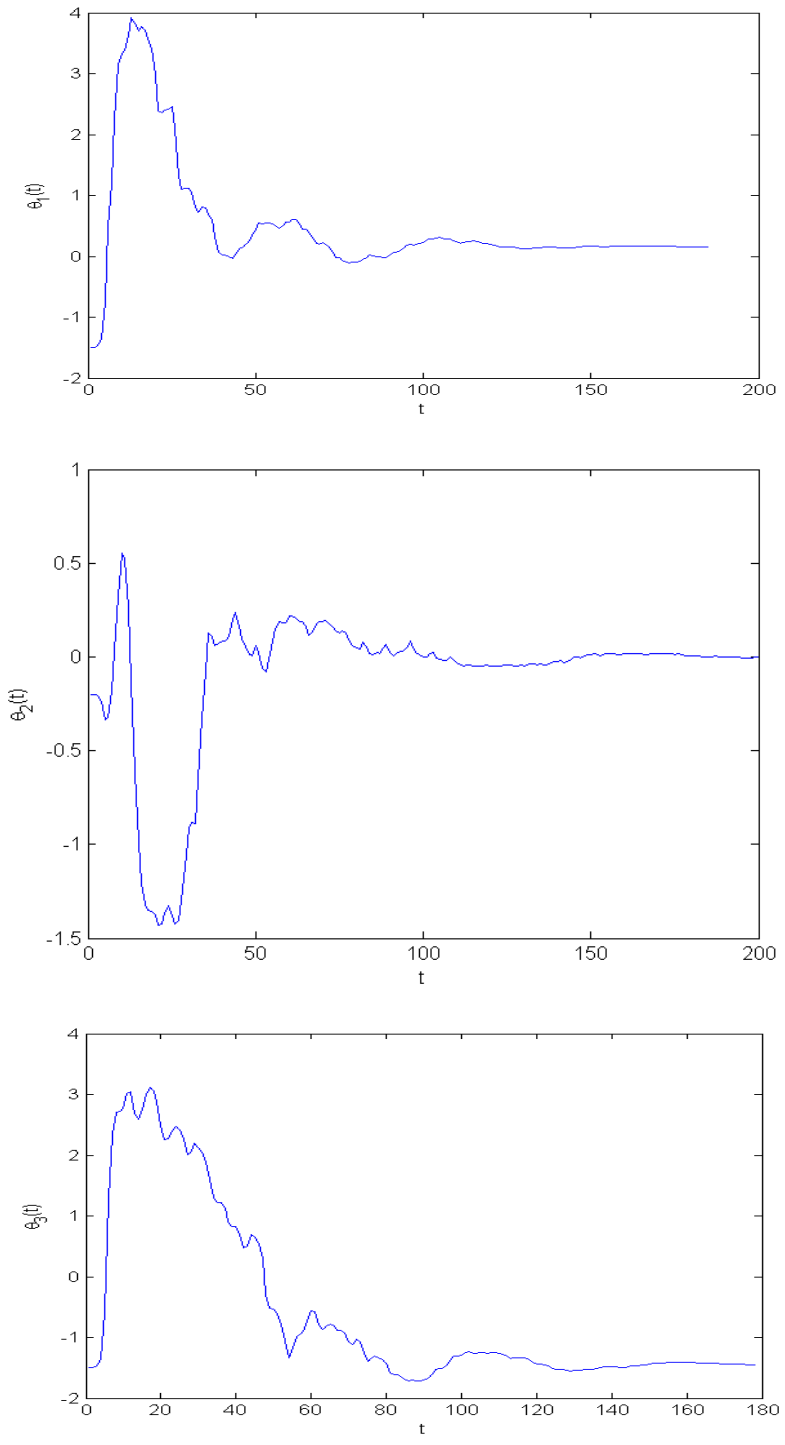
مسیر حالت سیستم مرجع (تحریک کامل) یک اوسیلاتور دافینگ را به‌صورت زیر در نظر می‌گیریم:

$$\dot{x}_{m,1} = x_{m,2}$$
$$\dot{x}_{m,2} = -3x_{m,1} - 0.2x_{m,2} - 1.2x_{m,1}^3 + 2.2\cos(1.3t) + 5.0\sin(2t)$$

پس اعمال قوانین موردنظر و شبیه‌سازی سیستم، نمودار همگرایی پارامترها در شکل ۳-۱۶ و نمودار خطاهای سیستم و همگرایی آن‌ها در شکل ۳-۱۵ نشان داده‌شده است.




شکل ۳-۱۵. نمودار همگرایی خطاهای سیستم $e_1, e_2$.




شکل ۳-۱۶. نمودار همگرایی پارامترهای $\theta_3(t),\theta_2(t),\theta_1(t)$.

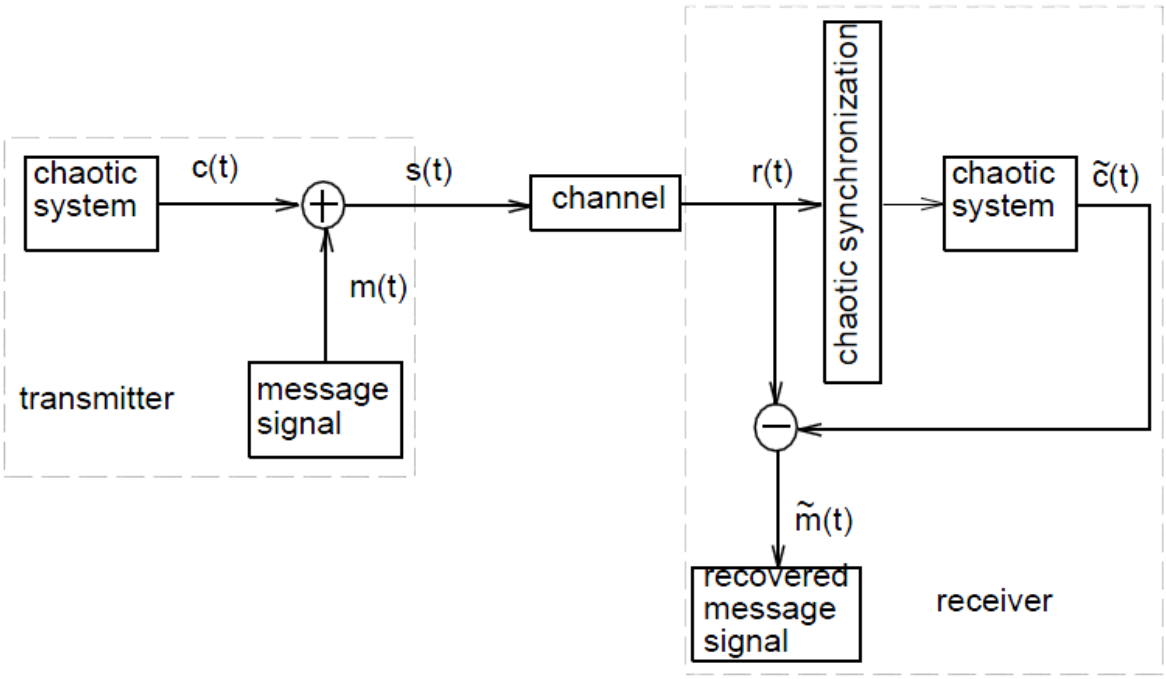
همان‌طور که مشاهده می‌شود خطاهای سیستم بعد از گذشت مدت‌زمانی به صفر همگرا می‌شود و پارامترهای نامعین سیستم نیز تقریبا به مقادیر موردنظر تطبیق پیداکرده‌اند.

# فصل چهارم: مطالعه سیستم‌های مخابرات‌امن آشوبی

در این بخش به بررسی نسل‌های مختلف سیستم‌های مخابرات امن آشوبی می‌پردازیم و مزایا و معایب هرکدام را بررسی کرده و اهمیت سنکرون سازی در مخابرات امن آشوبی به‌عنوان مهم‌ترین بخش از سیستم مورد ارزیابی قرار می‌گیرد.

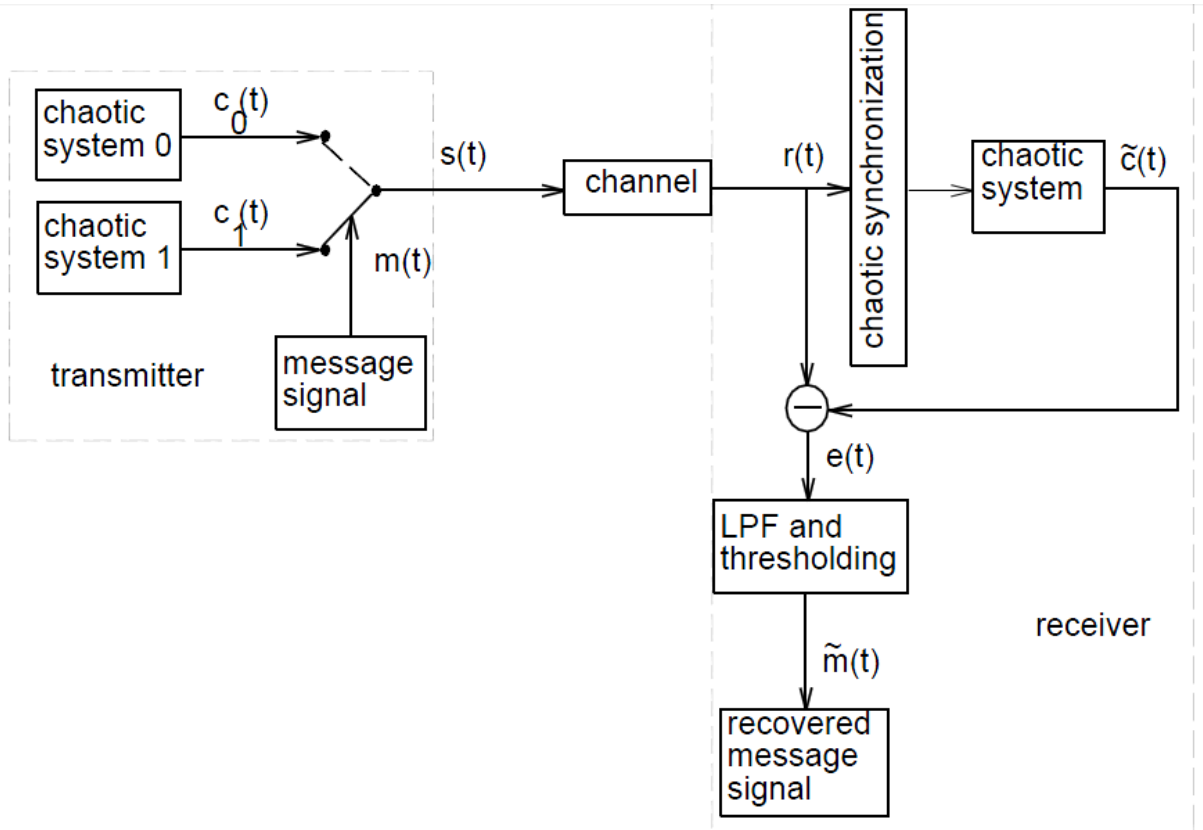
### ۴-۱- نسل اول

نسل اول در سال ۱۹۹۳ معرفی شد که شامل پوشاندن جمع شونده آشوب[۴۲] [۳]، نشان داده‌شده در شکل (۴-۱-الف) و کلید زنی آشوبی[۴۳] [۳۴]، نشان داده‌شده در شکل (۴-۱-ب) است. رهیافت پوشاندن جمع شونده که در شکل (۴-۱) نشان داده‌شده است شامل دو سیستم آشوبی یکسان در گیرنده و فرستنده است. پوشاننده آشوبی که با $c(t)$ نشان داده می‌شود یکی از متغیرهای حالت سیستم آشوبی فرستنده است. سیگنال پیام $m(t)$ که معمولاً بین ۲۰ تا ۳۰ دسی‌بل ضعیف‌تر از $c(t)$ است، بسیار پیچیده بوده و سیگنال پیام $m(t)$ بسیار کوچک‌تر از $c(t)$ است، می‌توان امیدوار بود که سیگنال پیام $m(t)$ را نتوان از $s(t)$ بدون دانستن دقیق $c(t)$ به دست آورد.




(الف)

[۴۲] Additive chaos masking
[۴۳] Chaotic shift keying

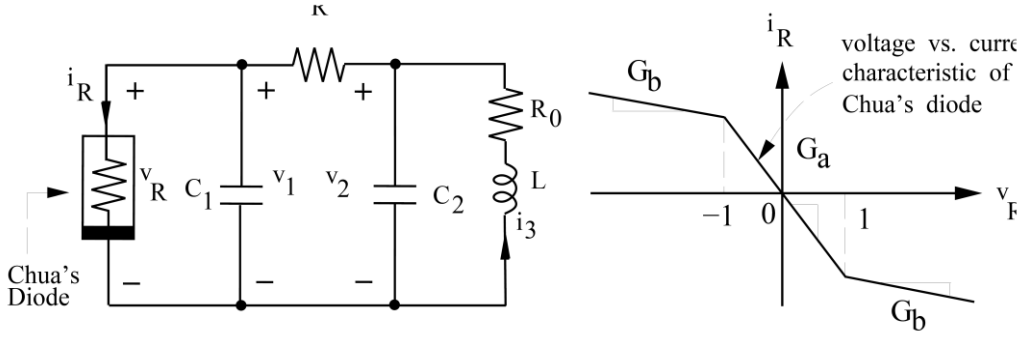



(ب)

شکل ۴-۱. بلوک دیاگرام نسل اول سیستم‌های مخابرات امن آشوبی. (الف) رهیافت پوشاندن جمع شونده آشوبی (ب) رهیافت کلید زنی آشوبی که رهیافت سوئیپچینگ آشوبی هم نامیده می‌شود [۳].

یک مثال از مخابرات امن آشوبی در زیر آمده است همان‌گونه که در شکل (۴-۱-الف) مشاهده می‌شود، در گیرنده به بلوک همزمانی آشوب نیازمندیم و همزمان‌سازی آشوبی تعمیمی از همزمان‌سازی حامل در مخابرات معمول است ولی با آن تفاوت زیادی دارد.

برای نشان دادن همزمانی آشوب از نوسان‌سازهای Chua استفاده می‌نماییم. نوسان‌ساز Chua در شکل (۴-۲) نشان داده‌شده است.




شکل ۴-۲. نوسان‌ساز و مشخصات دیود Chua

معادلات حالت نوسان‌ساز Chua به شرح زیر است.

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{c_1}[G(v_2 - v_1) - f(v_1)] \\ \dfrac{dv_2}{dt} = \dfrac{1}{c_2}[G(v_1 - v_2) + i_3] \\ \dfrac{di_3}{dt} = \dfrac{1}{L}[-v_2 - R_0 i_3] \end{cases} \qquad (۱-۴)$$

که در آن $v_1$، $v_2$ و $i_3$ به ترتیب ولتاژهای $c_1$ و $c_2$ و جریان گذرنده از $L$ است. $G = \dfrac{1}{R}$ قرار می‌دهیم درنتیجه جمله $R_0 i_3$ با توجه به مقاومت کوچک سلف در مدار عملی قابل‌توجه خواهد بود. معادله مشخصه $v - i$ دیود Chua، $f(v_1)$ پیوسته قطعه‌ای و به‌صورت زیر است.

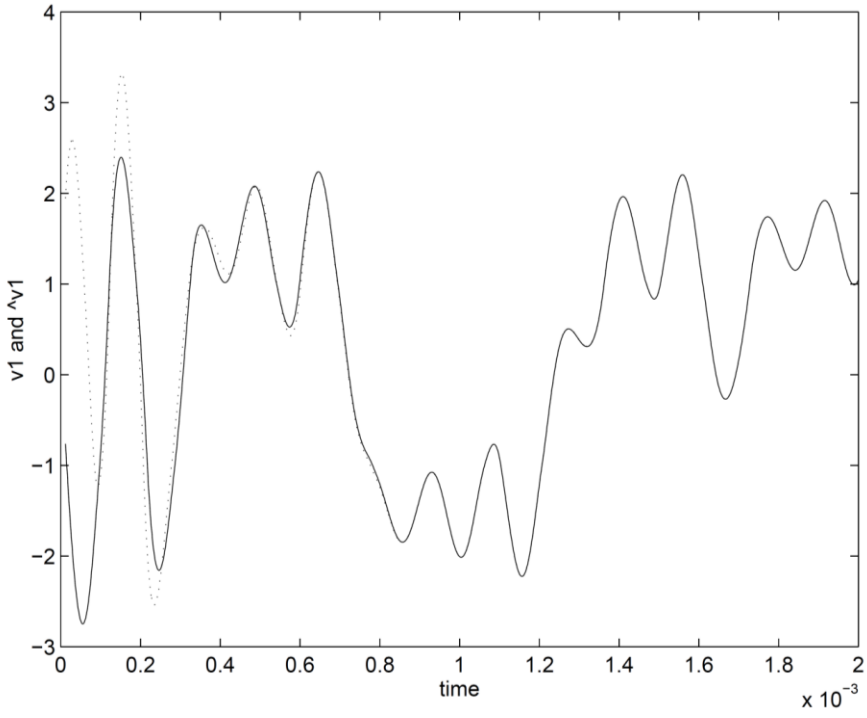
$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|) \qquad (۲-۴)$$

که در آن $E$ ولتاژ شکست دیود Chua همان‌گونه که در شکل (۴-۲) نشان داده‌شده است. اگر اسیلاتور Chua داده‌شده توسط معادله ۴-۱ به‌عنوان فرستنده استفاده نماییم، اسیلاتور Chua زیر به‌عنوان گیرنده خواهد بود.

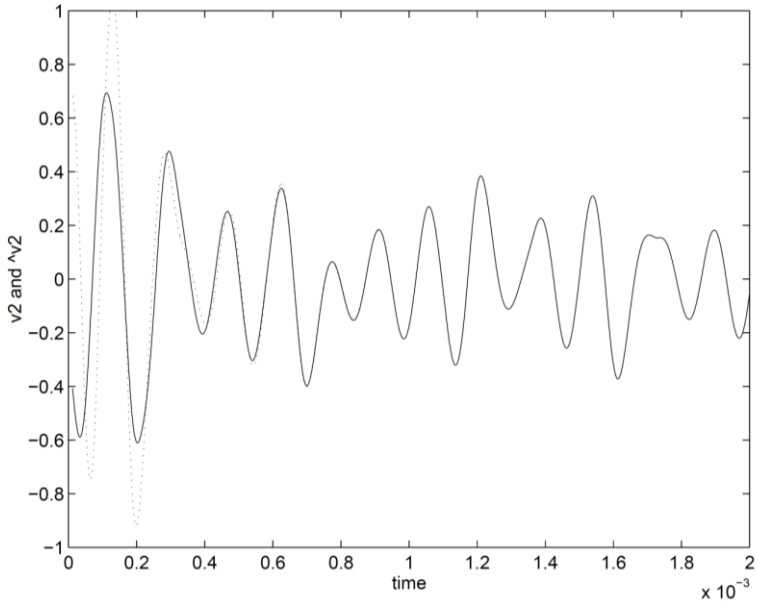
$$\begin{cases} \dfrac{d\tilde{v}_1}{dt} = \dfrac{1}{c_1}[G(\tilde{v}_2 - \tilde{v}_1) - f(\tilde{v}_1)] \\ \dfrac{d\tilde{v}_2}{dt} = \dfrac{1}{c_2}[G(v_1 - \tilde{v}_2) + \tilde{i}_3] \\ \dfrac{d\tilde{i}_3}{dt} = \dfrac{1}{L}[-\tilde{v}_2 - R_0\tilde{i}_3] \end{cases} \qquad (۳-۴)$$

که در آن $\tilde{v}_1$، $\tilde{v}_2$ و $\tilde{i}_3$ متغیرهای حالت گیرنده است.

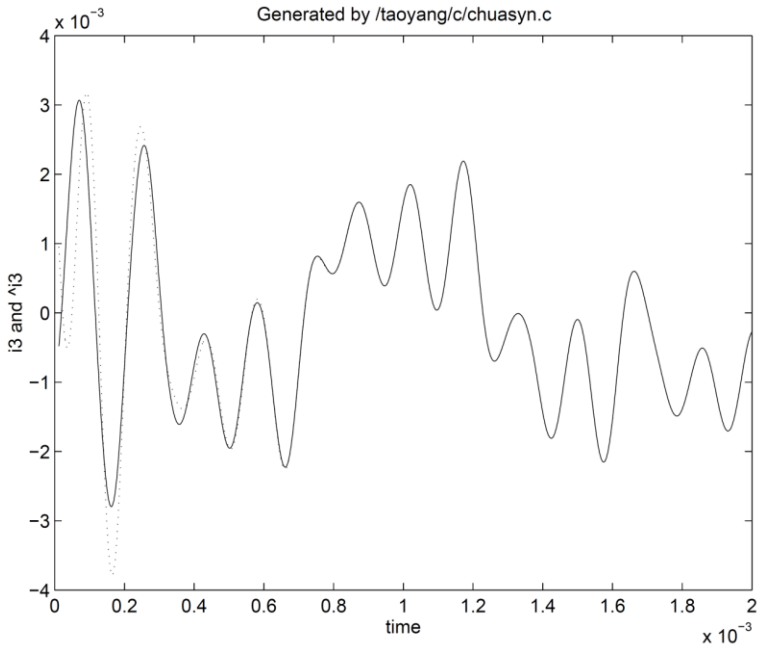
توجه کنید که در قسمت دوم معادله ۴-۳، $\tilde{v}_1$ را با $v_1$ جایگزین کرده‌ایم. در این حالت $v_1$ سیگنال ارسال‌شده است. می‌توان اثبات نمود که در شرایط خاص می‌توان نوسانات Chua بیان‌شده در معادلات ۴-۱ و ۴-۳ را همزمان نمود [۳۵]. نتایج شبیه‌سازی در شکل ۴-۳ نشان داده‌شده است. خطوط پیوسته نشان‌دهنده متغیرهای حالت فرستنده و خطوط مقطع نشان‌دهنده متغیرهای حالت گیرنده است. می‌بینیم که متغیرهای حالت گیرنده به متغیرهای حالت فرستنده در حدود ۰٫۵ میلی‌ثانیه میل می‌نمایند هرچند که حالت اولیه آن‌ها بسیار متفاوت است.




(الف)




(ب)




(ج)

شکل ۴-۳. همزمان سازی دو نوسان‌ساز Chua. (الف) فرآیند همزمان سازی $v_1$ و $\tilde{v}_1$ (ب) فرآیند همزمان سازی $v_2$ و $\tilde{v}_2$ (ج) فرآیند همزمان سازی $i_3$ و $\tilde{i}_3$

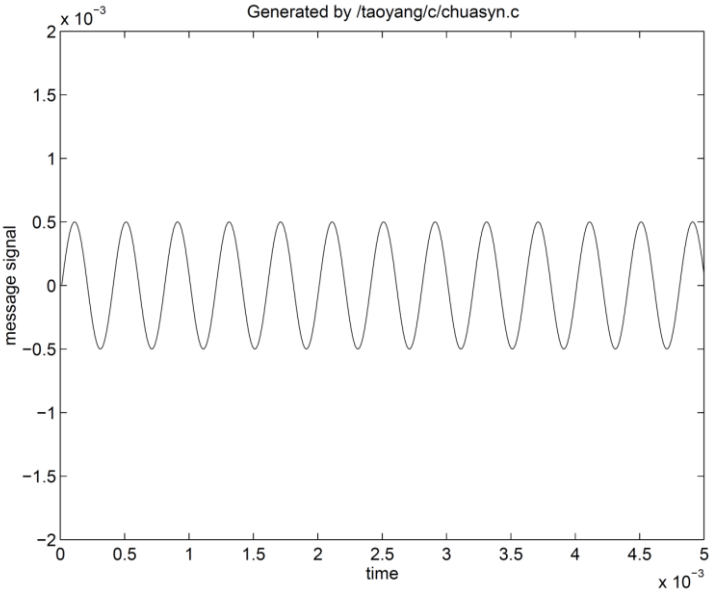
بعد از درک مفهوم هم‌زمان‌سازی آشوب، می‌توان یک سیگنال کوچک پیام $m(t)$ را در سیگنال فرستاده‌شده $s(t)$ پنهان کرد.

گیرنده در معادله ۴-۳ را می‌توان به‌صورت زیر نوشت:

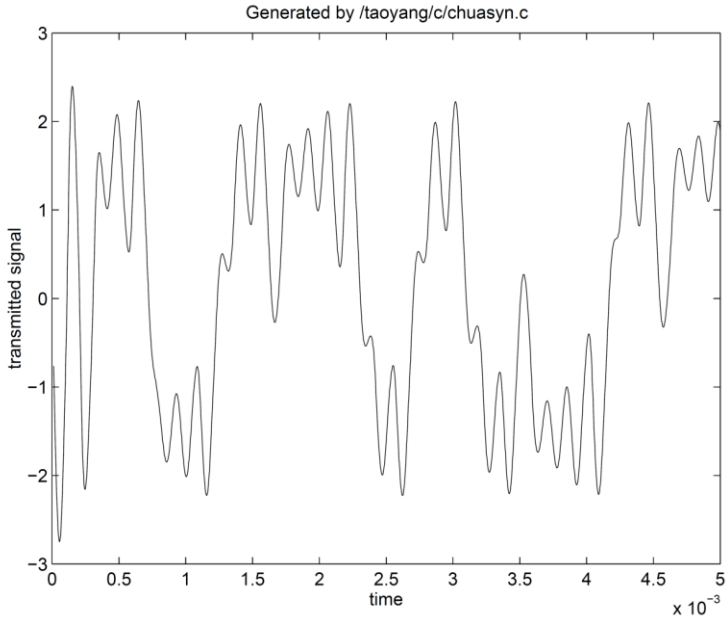
$$\begin{cases} \dfrac{d\tilde{v}_1}{dt} = \dfrac{1}{c_1}[G(\tilde{v}_2 - \tilde{v}_1) - f(\tilde{v}_1)] \\ \dfrac{d\tilde{v}_2}{dt} = \dfrac{1}{c_2}[G(v_1 + m(t) - \tilde{v}_2) + \tilde{i}_3] \\ \dfrac{d\tilde{i}_3}{dt} = \dfrac{1}{L}[-\tilde{v}_2 - R_0\tilde{i}_3] \end{cases} \qquad (۴-۴)$$

در این حالت در نظر می‌گیریم که کانال بدون نویز است و معادله $r(t) = s(t) = v_1(t) + m(t)$ برقرار است. هم‌زمان‌سازی هنگامی‌که $m(t)$ به‌اندازه کافی کوچک باشد قابل‌دستیابی است. در شکل (۴-۴) نتایج شبیه‌سازی برای رهیافت پوشاندن جمع شونده آشوب ارائه‌شده است. شکل (۴-۴-الف) پیام ضعیف را نشان می‌دهد و شکل (۴-۴-ب) سیگنال فرستاده‌شده را نشان می‌دهد. ازآنجایی‌که سیگنال پیام بسیار ضعیف است نمی‌توان اثری از آن در سیگنال فرستاده‌شده دید، در این حالت سیگنال پیام در سیگنال شبه نویز آشوبی پنهان‌شده است. نتایج بازیابی شده در شکل (۴-۴-ب) نشان داده‌شده است. همان‌گونه که مشاهده می‌شود بعد از گذشت حالت گذرا همزمانی ناقص انجام‌شده و سیگنال پیام به همراه نویز زیادی بازیابی شده است.

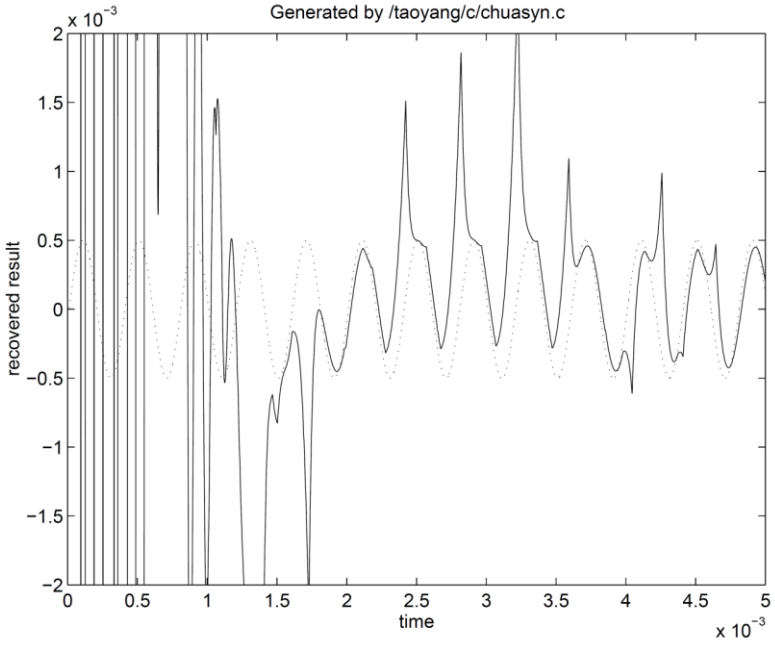
اثبات‌شده است که این رهیافت در کاربردهای عملی به علت محدودیت‌هایی که در زیر به آن‌ها اشاره می‌شود قابل‌استفاده نیست. ازآنجایی‌که سیگنال پیام حدود ۲۰ تا ۳۰ دسی‌بل ضعیف‌تر از سیگنال آشوبی است، این روش بسیار به نویز کانال و عدم تطبیق پارامترها بین سیستم‌های آشوبی در فرستنده و گیرنده حساس است. به‌علاوه، این روش دارای درجه امنیت بسیار کمی می‌باشد [۳۶].




(الف)




(ب)




(ج)

شکل ۴-۴. نتیجه شبیه‌سازی رهیافت پوشاندن جمع شونده آشوب با استفاده از دو نوسان‌ساز Chua. (لف) سیگنال پیام ضعیف $m(t)$. (ب) سیگنال فرستاده‌شده $s(t)$. (ج) سیگنال بازیابی شده $\tilde{m}(t)$ [۳۶].

کلید زنی آشوبی که در شکل (۴-۱-ب) نشان داده‌شده است، سوئیچینگ آشوبی هم نامیده می‌شود و برای ارسال سیگنال پیام دیجیتال طراحی‌شده است. در این رهیافت، سیگنال پیام که سیگنالی

دیجیتال است برای سوئیچ کردن سیگنال ارسالی بین دو جاذب آشوبی با مشخصات آماری مشابه که برای کد کردن بیت‌های صفر و یک سیگنال پیام بکار می‌رود، استفاده می‌شود. این دو جاذب به‌وسیله دو سیستم آشوبی با ساختار یکسان ولی پارامترهای متفاوت ایجاد می‌گردد. در سمت گیرنده، سیگنال دریافتی برای تحریک یک سیستم آشوبی که معادل یکی از سیستم‌های آشوبی در فرستنده است، مورداستفاده قرار می‌گیرد. سیگنال دریافتی به‌وسیله یک فیلتر پایین گذر و سپس استفاده از سطح آستانه برای خطای هم‌زمان‌سازی سیگنال $e(t)$ که در شکل (۴-۱-ب) نشان داده‌شده است، بازیابی می‌شود.

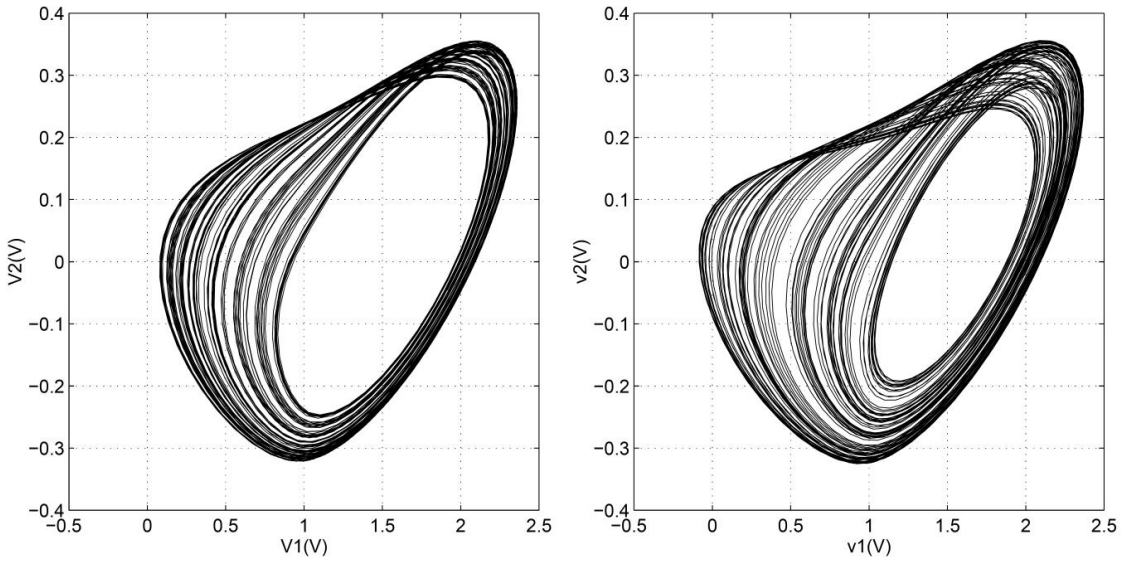
برای نشان دادن این رهیافت نیز از نوسان‌سازهای Chua در فرستنده و گیرنده استفاده می‌کنیم. در فرستنده از دو جاذب آشوبی شبیه راسلر برای کد کردن بیت‌های صفر و یک بکار می‌رود. پارامترهای بکار رفته برای کد کردن بیت یک عبارت‌اند از:

$$R = 1000\Omega, R_0 = 20\Omega, G_a = -1.139mS, G_b = -0.71mS, E = 1v, L = 12.5mH, c_1 = 17nF, c_2 = 187nF$$

جاذب آشوبی مربوطه در شکل (۴-۵-الف) نشان داده‌شده است. پارامترهای بکار رفته برای کد کردن بیت صفر به شرح زیرند:

$$R = 1000\Omega, R_0 = 20\Omega, G_a = -1.139mS, G_b = -0.71mS, E = 1v, L = 12.5mH, c_1 = 17.5nF, c_2 = 197nF$$

جاذب آشوبی مربوطه در شکل (۴-۵-ب) نشان داده‌شده است. این دودسته پارامتر دو جاذب آشوبی متفاوت ولی ازنظر آماری مشابه را تولید می‌نمایند. ولتاژ $v_1$ به گیرنده فرستاده می‌شود بلوک همزمان سازی آشوب چیزی شبیه و نه لزوماً معادل آنچه در شکل (۴-۱-الف) نشان داده شد است.

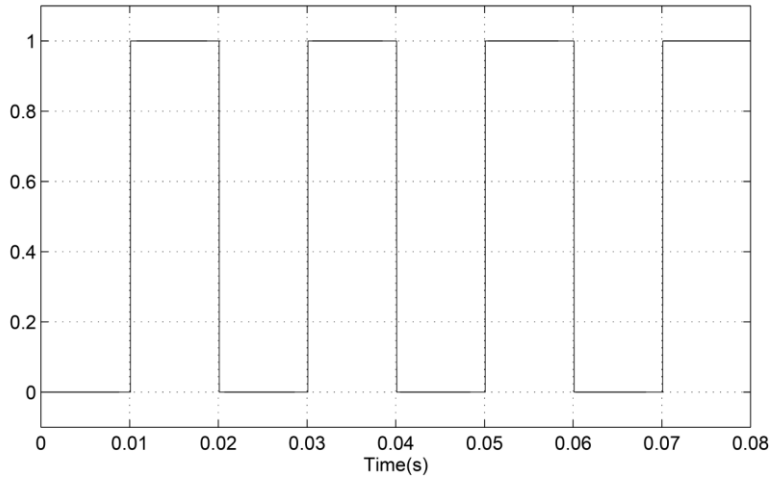



(ب) (الف)

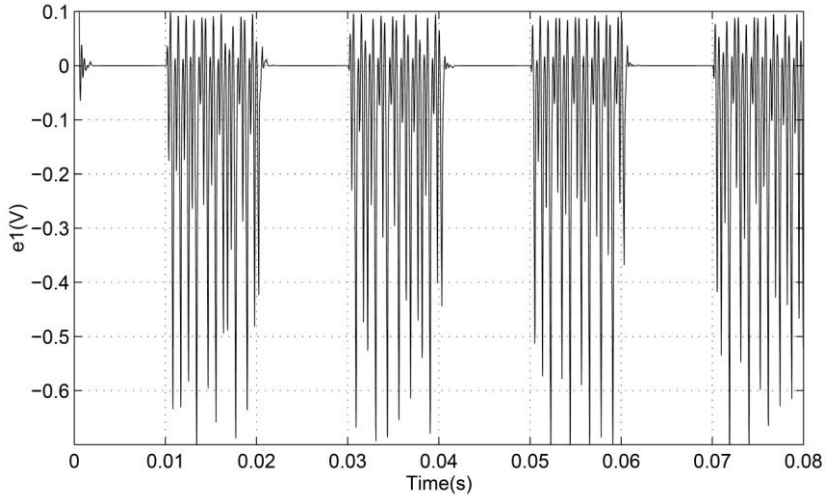
شکل ۴-۵. جاذب‌های آشوبی نوسان‌ساز Chua که در رهیافت کلید زنی آشوبی بکار رفته‌اند. هردو در صفحه $v_1 - v_2$ نشان داده‌شده‌اند. (الف) جاذب آشوبی برای کد کردن بیت یک (ب) جاذب آشوبی برای کد کردن بیت صفر.

نتایج شبیه‌سازی در شکل (۴-۶) نشان داده‌شده است. شکل (۴-۶-الف) نشانگر سیگنال پیام دودویی با دوره ۱۰ میلی‌ثانیه است. شکل (۴-۶-ب) نشانگر خطای همزمان سازی گیرنده مجاز مربوط به بیت صفر است. شکل (۴-۶-ج) نشانگر خطای همزمان سازی گیرنده مجاز مربوط به بیت یک است. می‌توان سیگنال دودویی الف را با انتقال میانگین‌گیری و اعمال حد آستانه به ب یا ج بازیابی کرد.

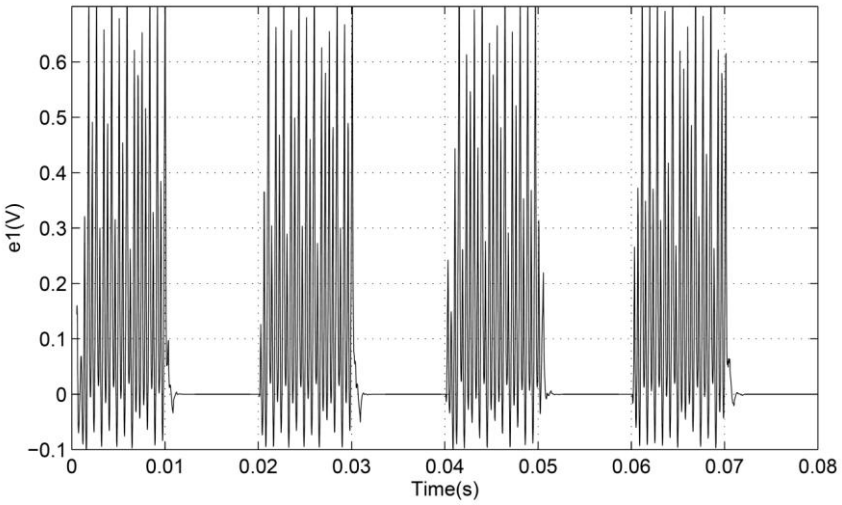
این رهیافت از خود در برابر نویز و عدم تطبیق پارامتر مقاومت نشان می‌دهد. اگر جاذب‌های آشوبی مربوطه از هم در فضای دوشاخگی بسیار دور باشند، این رهیافت دارای درجه پایینی از امنیت است [۳۷]. به‌هرحال ازآنجایی‌که این اولین رهیافت مخابرات امن آشوبی بوده است، هم‌اکنون نیز امکان زیادی برای بهتر شدن دارد.


1
0.8
0.6
0.4
0.2
0
0
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
Time(s)

(الف)


0.1
0
−0.1
−0.2
−0.3
−0.4
−0.5
−0.6
e1(V)
0
0.01
0.02
0.03
0.04
0.05
0.06
0.07
0.08
Time(s)

(ب)

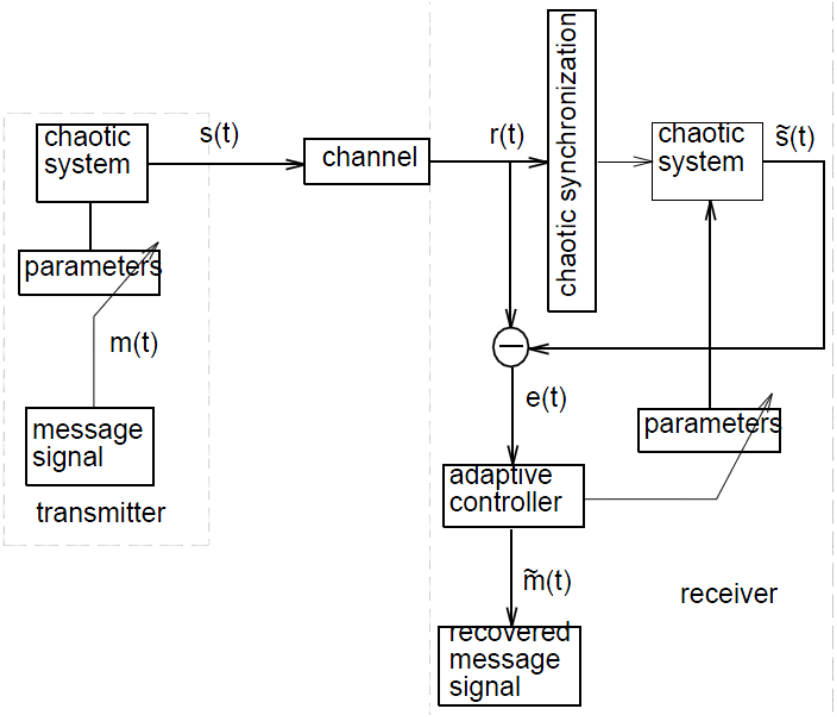



(ج)

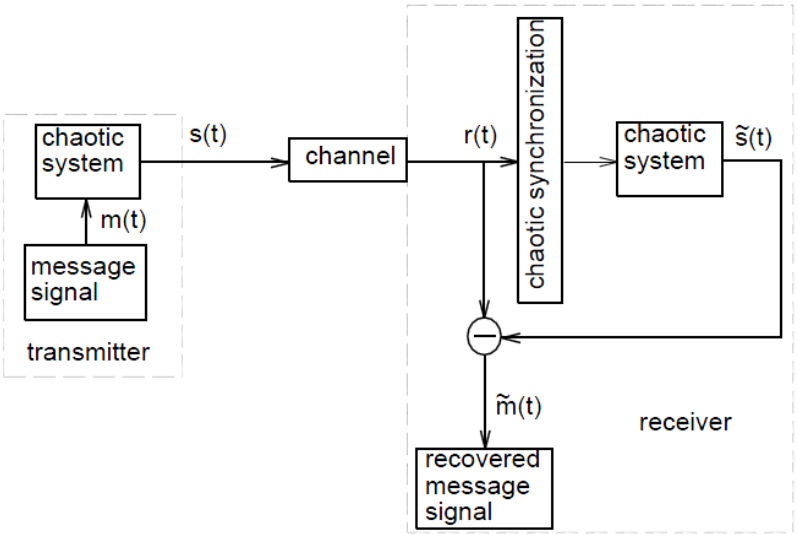
شکل ۴-۶. نتایج شبیه‌سازی برای کلید زنی آشوبی. (الف) سیگنال پیام باینری $m(t)$. (ب) خطای همزمان سازی نوسان‌ساز Chua با پارامتر مربوط به بیت صفر. (ج) خطای همزمان سازی نوسان‌ساز Chua با پارامتر مربوط به بیت یک.

### ۴-۲- نسل دوم

نسل دوم سیستم‌های مخابرات امن آشوبی در طی سال‌های ۱۹۹۳ تا ۱۹۹۵ با نام مدولاسیون آشوبی ارائه شد. این نسل از دو روش مختلف برای مدولاسیون پیام بر روی حامل آشوبی سود می‌جست. اولین روش مدولاسیون پارامتر آشوبی نام دارد و در شکل (۴-۷-الف) نشان داده‌شده است. در این روش از سیگنال پیام برای تغییر پارامترهای فرستنده آشوبی استفاده می‌شود [۱۰]. روش دوم که روش مدولاسیون غیر خودکار آشوبی نامیده می‌شود و در شکل (۴-۷-ب) نشان داده‌شده است، از سیگنال پیام برای تغییر دادن صفحه فاز فرستنده آشوبی استفاده می‌نماید [۳۸].




(الف)

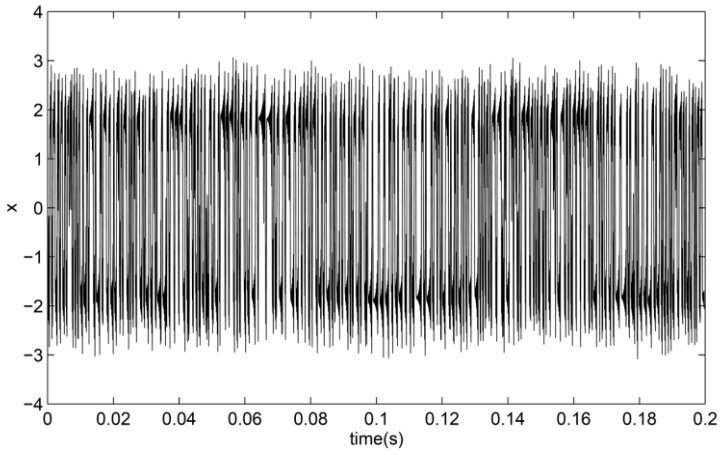



(ب)

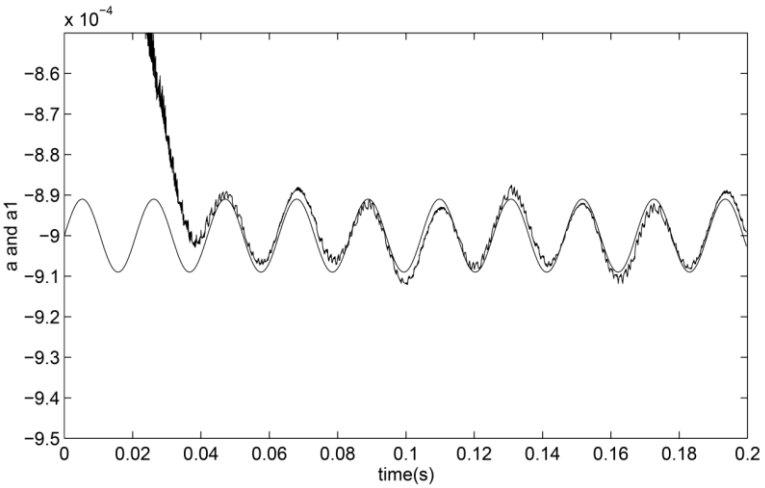
شکل ۴-۷. بلوک دیاگرام نسل دوم سیستم‌های مخابرات امن آشوبی. (الف) مدولاسیون پارامتر آشوبی. (ب) مدولاسیون غیر خودکار آشوبی [۱۰].

در شکل (۴-۷-الف) سیگنال پیام $m(t)$ به‌منظور مدوله کردن تعدادی از پارامترهای سیستم آشوبی فرستنده به‌نحوی‌که مسیرهایشان در بین جاذب‌های مختلف آشوبی تغییر نماید به کار می‌رود. در سمت گیرنده از یک کنترل‌کننده تطبیقی برای تنظیم وفقی پارامترهای سیستم آشوبی به‌نحوی‌که

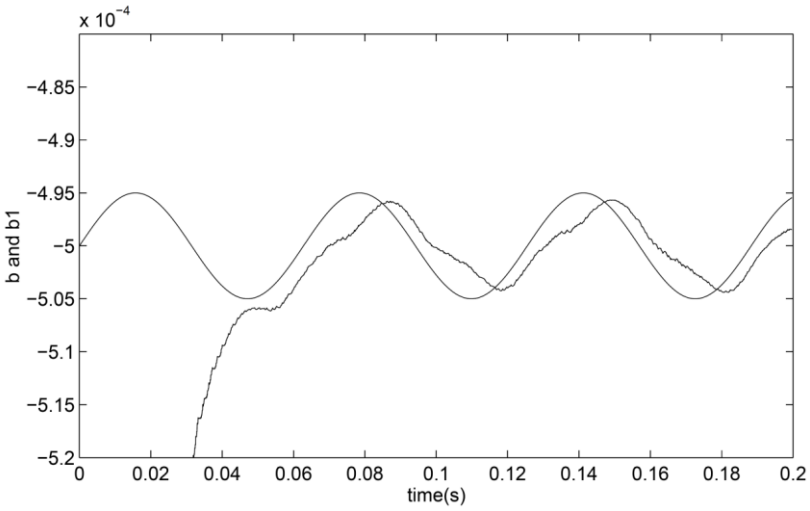
خطای هم‌زمان‌سازی به صفر میل نماید استفاده می‌گردد. با انجام این عمل، خروجی کنترل‌کننده تطبیقی می‌تواند سیگنال پیام را بازیابی کند. نتایج شبیه‌سازی در شکل (۴-۸) نشان داده‌شده است. در این شبیه‌سازی از سه سیگنال پیام برای تنظیم سه پارامتر مختلف سیستم آشوبی فرستنده استفاده‌شده است. ازآنجایی‌که سیستم آشوبی دائماً جاذب‌هایش را تغییر می‌دهد، شکل موج سیگنال فرستاده‌شده همان‌گونه که در شکل (۴-۸-الف) نشان داده‌شده است نسبت به سیگنال‌های آشوبی معمولی پیچیده‌تر است. در شکل‌های (۴-۸-ب) تا (۴-۸-د) سه سیگنال پیام اصلی و بازیابی شده را نمایش می‌دهیم. مشاهده می‌شود که بعد از زمان گذرای هم‌زمان‌سازی، سیگنال‌های پیام باوجود مقداری cross talk و مقدار کمی تاخیر بازیابی شده‌اند. به‌جای تغییر پارامترهای فرستنده آشوبی، رهیافت مدولاسیون غیر خودکار نشان داده‌شده در شکل (۴-۷-ب) از سیگنال پیام برای تغییر دادن جزئی جاذب آشوبی مستقیماً در صفحه فاز استفاده می‌شود. برخلاف مدولاسیون پارامتر آشوبی که در آن فرستنده بین مسیرهای مختلف در جاذب‌های گوناگون آشوبی سوئیچ می‌نماید. در تئوری، رهیافت مدولاسیون غیر خودکار یک رهیافت بی‌خطا است. نسل دوم درجه امنیت را تا حدی بالا می‌برد اما هنوز این درجه از امنیت رضایت‌بخش نبود [۳۶].



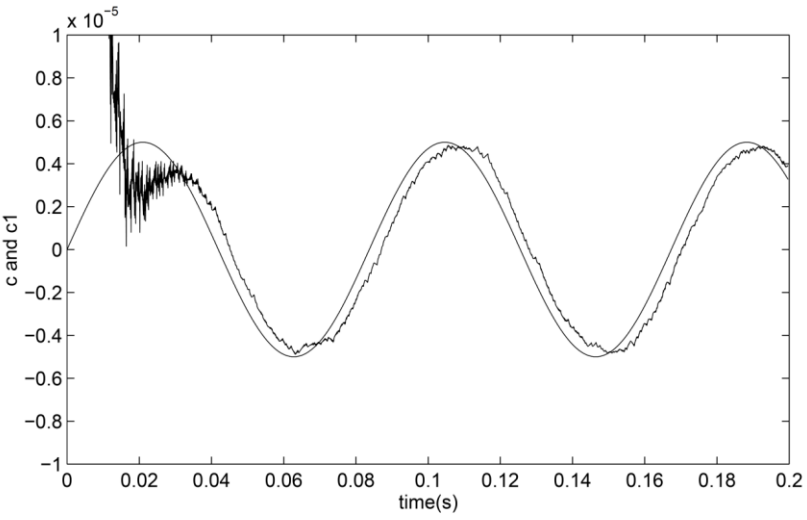

(الف)




(ب)




(ج)



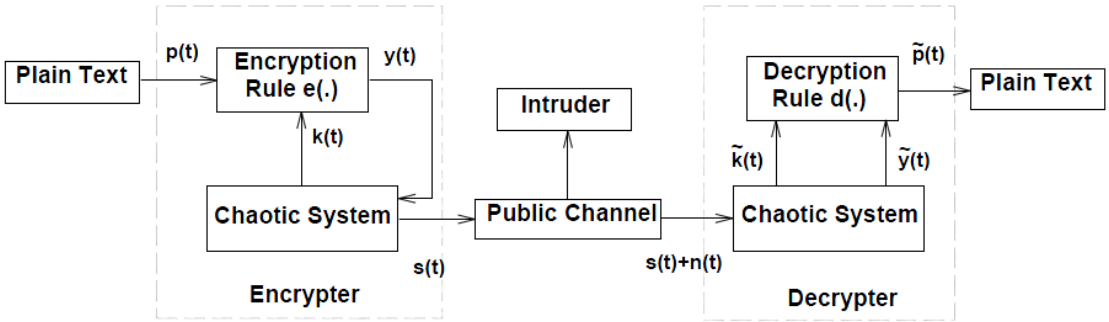

(د)

شکل ۴-۸. استفاده از مدولاسیون پارامتر آشوبی برای ارسال سه سیگنال پیام به‌صورت همزمان. (الف) سیگنال فرستاده‌شده $s(t)$. (ب) اولین سیگنال پیام و نسخه بازیابی شده آن. (ج) دومین سیگنال پیام و نسخه بازیابی شده آن. (د) سومین سیگنال پیام و نسخه بازیابی شده آن [۱۰].

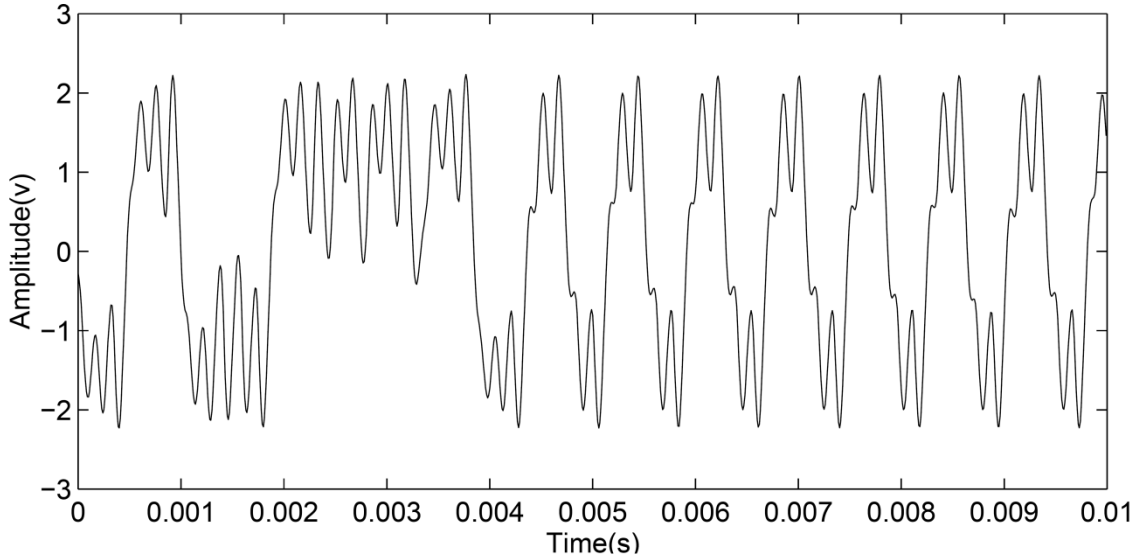
### ۴-۳- نسل سوم

نسل سوم سیستم‌های مخابرات امن آشوبی که در شکل (۴-۹) نشان داده‌شده است در سال ۱۹۹۷ باهدف افزایش درجه امنیت سیستم به حدی فراتر از دو نسل قبلی پیشنهاد شد [۳۹]. به این نسل سیستم رمزنگاری آشوبی می‌گوییم. در این نسل از ترکیب تکنیک‌های رمزنگاری کلاسیک و هم‌زمان‌سازی آشوب برای بهبود درجه امنیت استفاده می‌گردد. تاکنون این نسل سیستم‌های مخابرات امن آشوبی در بین تمامی نسل‌ها دارای امنیت بیشتری بوده و تابه‌حال شکسته نشده است. در سیستم رمزنگاری آشوبی سیگنال متن اصلی $p(t)$ توسط الگوریتم رمزنگاری با کلید $k(t)$ که توسط سیستم آشوبی در فرستنده تولید می‌شود، رمز می‌گردد. سیگنال مخلوط شده به‌منظور تحریک سیستم آشوبی به‌نحوی‌که دینامیک‌های آشوبی به‌صورت پیوسته و با الگویی بسیار پیچیده تغییر نمایند، به کار می‌رود. سپس یک متغیر حالت دیگر سیستم آشوبی فرستنده از طریق کانال عمومی که در دسترس دشمن است، فرستاده می‌شود. ازآنجاکه دشمن به کلید سخت‌افزاری آشوبی دسترسی ندارد، پیدا کردن $p(t)$ از روی $s(t)$ بسیار دشوار می‌شود. در گیرنده، سیگنال دریافت شده

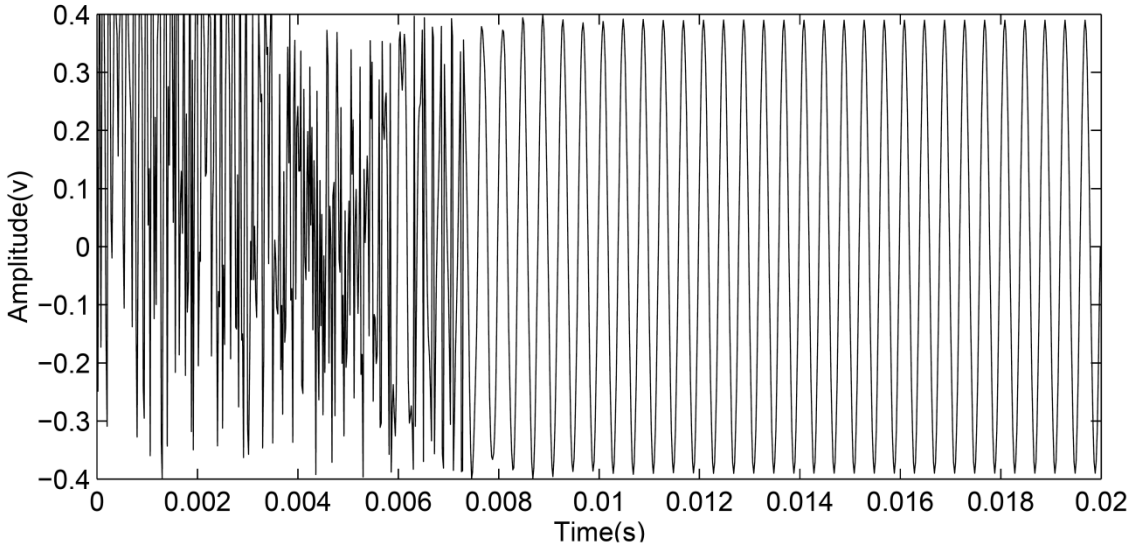
$r(t)=s(t)+n(t)$ است که در آن $n(t)$ نویز کانال است، به‌منظور هم‌زمان‌سازی هر دو سیستم آشوبی در فرستنده و گیرنده به کار می‌رود. بعد از هم‌زمان‌شدن دو سیستم آشوبی فرستنده و گیرنده، سیگنال‌های $k(t)$ و $y(t)$ در گیرنده می‌توانند با مقداری نویز بازسازی شوند. بدین منظور آن‌ها را با $\tilde{k}(t)$ و $\tilde{y}(t)$ نمایش می‌دهیم. با واردکردن $\tilde{k}(t)$ و $\tilde{y}(t)$ در قانون رمزگشایی، متن اصلی به همراه مقداری نویز قابل بازیابی است که با $\tilde{p}(t)$ نمایش داده می‌شود. نتایج شبیه‌سازی در شکل (۴-۱۰) نشان داده‌شده است. شکل (۴-۱۰-الف) نشانگر سیگنال ارسالی $s(t)$ است که همان‌گونه که مشاهده می‌شود از روی آن نمی‌توان سیگنال پیام را تشخیص داد. شکل (۴-۱۰-ب) نشانگر سیگنال‌های بازیابی شده و رمزگشایی‌شده در گیرنده است. مشاهده می‌شود که پس از گذشت زمان گذرای هم‌زمان‌سازی، سیگنال متن اصلی بازیابی شده است. به‌منظور نشان دادن امنیت بالای این رهیافت، روش مطرح‌شده در [۳۶] برای کد برداری سیگنال متن اصلی به‌کاررفته است. شکل (۴-۱۰-ج) سیگنال بازیابی شده توسط دشمن $\tilde{y}(t)$ را نشان می‌دهد. همان‌گونه که در شکل (۴-۱۰-د) نشان داده‌شده است، از روی $\tilde{y}(t)$ به‌هیچ‌وجه نمی‌توان سیگنال پیام اصلی را بازیابی نمود.



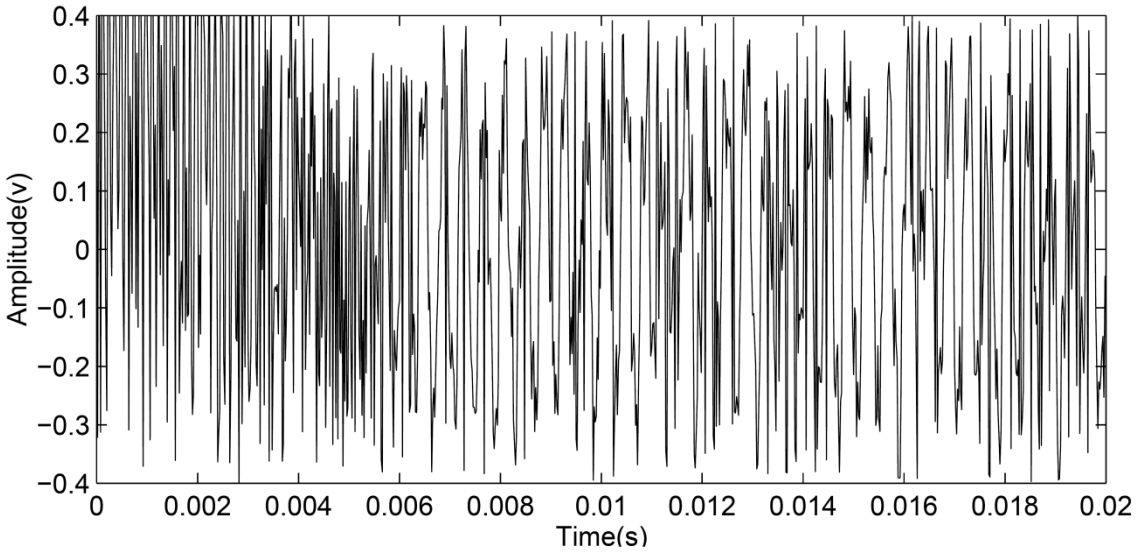

شکل ۴-۹. بلوک دیاگرام نسل سوم سیستم مخابرات امن آشوبی


Amplitude(v)
Time(s)
3
2
1
0
−1
−2
−3
0
0.001
0.002
0.003
0.004
0.005
0.006
0.007
0.008
0.009
0.01

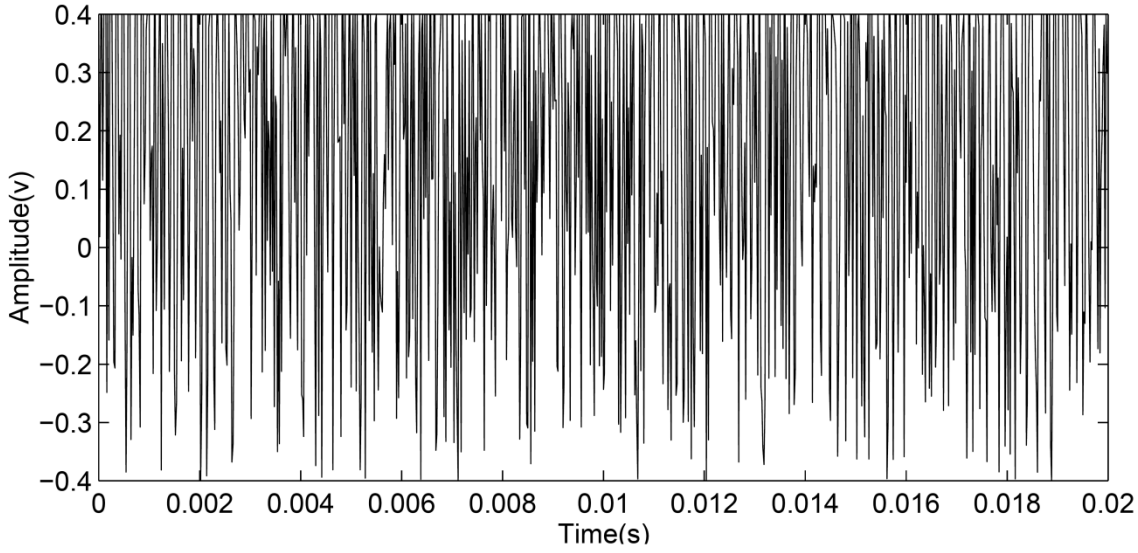
(الف)


Amplitude(v)
Time(s)
0.4
0.3
0.2
0.1
0
−0.1
−0.2
−0.3
−0.4
0
0.002
0.004
0.006
0.008
0.01
0.012
0.014
0.016
0.018
0.02

(ب)




(ج)




(د)

شکل ۴-۱۰. نتایج شبیه‌سازی سیستم رمزنگاری آشوبی. (الف) سیگنال فرستاده‌شده $s(t)$. (ب) سیگنال بازیابی شده سپس رمزگشایی‌شده $p(t)$. (ج) سیگنال رمز شده بازیابی شده با استفاده از روش مطرح در [۳۶]. (د) نتیجه رمزگشایی سیگنال مرحله (ج)

## ۴-۴- نتیجه‌گیری:

به‌منظور پیاده‌سازی عملی سیستم‌های مخابرات امن آشوبی، دو مشکل اساسی و تکنیکی باید حل شود تا بتوانیم سیستم‌های آشوبی را همزمان نماییم. اولین مشکل، مشکل عدم تطبیق پارامترها بین

سیستم‌های آشوبی فرستنده و گیرنده است. این مشکل به‌وسیله همزمان سازی تطبیقی حل‌شده است [۵]. مشکل دیگر خاصیت غیرخطی بودن کانال است. که این مشکل در [۳۵] حل شده است.

به‌منظور ساده‌سازی تمامی مثال‌ها در ساختار مخابرات آنالوگ ارائه شدند. در پیاده‌سازی‌های عملی مخابرات امن آشوبی به شکل سیستم‌های مخابرات امن دیجیتال با حامل‌های آشوبی صورت می‌پذیرد. اولین رهیافت رقومی کردن سیگنال ارسالی s(t) و سپس ارسال آن از طریق تکنیک‌های کلاسیک مخابرات دیجیتال بود. بر اساس مقاومت همزمان سازی تطبیقی استفاده‌شده در نسل‌های دوم و سوم، خطای رقومی کردن تنها می‌تواند قسمت کوچک از تمام نویزهای موجود در سیگنال بازیابی شده را تشکیل دهند. رهیافت دوم به ارسال سیگنال‌های اطلاعات دیجیتال در نسل سوم بر اساس همزمان سازی تطبیقی سیستم‌های آشوبی که بر اساس تئوری کنترل تطبیقی انجام می‌شود تخصیص داده شد. در اصل همزمان سازی سیستم‌های آشوبی بکار رفته در سه نسل اول همزمان سازی پیوسته است.

نسل‌های ارائه‌شده دارای درجه امنیت پایین هستند بنابراین می بایست رهیافتی جدید و دارای امنیت بیشتر ارائه شود بدین منظور در فصل بعد روشی جدید برای سیستم‌های مخابرات امن آشوبی با ترکیبی از نسل سوم، نگاشت های آشوبی چند مدال و استگانوگرافی[۴۴] در تصویر ارائه خواهد شد.

[۴۴] Steganography

# فصل پنجم: ارائه رهیافت جدید مخابرات امن آشوبی

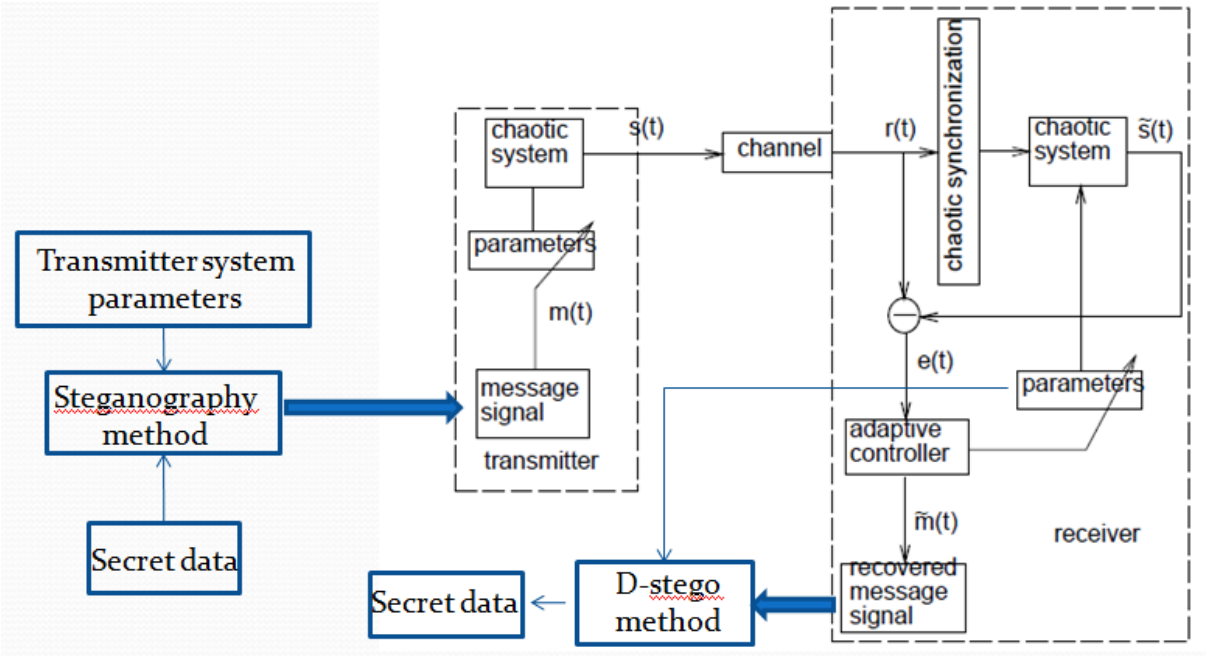
از وقتی نتایج بررسی‌های انجام‌شده برای به‌کارگیری آشوب در رمزنگاری منجر به سیستم‌های مخابراتی امن آشوبی از مرتبه پایین شد [۳۶, ۳۷]، نگرانی‌هایی در مورد اینکه این رهیافت‌ها ممکن است به‌اندازه کافی امن نباشد به وجود آمد. به‌منظور رفع این نگرانی یک راه استفاده از سیستم‌های مخابرات امن فوق آشوب[۴۵] است اما همزمان سازی این سیستم‌ها دارای مشکلات بسیار بیشتری است. از سویی دیگر می‌توانیم امنیت سیستم‌های مخابرات امن آشوبی مرتبه پایین را با استفاده از ترکیب سیستم‌های رمزنگاری معمول با سیستم‌های آشوبی افزایش دهیم [۳۹]. برای رفع مشکل امنیت پایین سیستم‌های مخابرات امن آشوبی پیوسته مرتبه پایین، می‌توان یکی از دو روش زیر را بکار برد. اولین روش افزایش پیچیدگی سیگنال ارسالی و روش دوم کاهش افزونگی[۴۶] در سیگنال ارسالی است[۴۰, ۴۱]. در این پایان‌نامه از ترکیب روش‌ها و نسل‌های مختلف سیستم‌های مخابرات امن آشوبی برای افزایش پیچیدگی سیگنال ارسالی با بهره‌گیری از نگاشت‌های آشوبی چند مدال و استگانوگرافی در تصویر استفاده‌شده است. همچنین لازم به ذکر است که برای کاهش افزونگی سیگنال ارسالی می‌توان از روش‌های سنکرون سازی غیر پیوسته ضربه‌ای استفاده نمود [۴۲].

نسل دوم درجه امنیت را تا حدی بالا می‌برد اما هنوز این درجه از امنیت رضایت‌بخش نیست به همین دلیل برای افزایش امنیت این نوع سیستم‌ها به ارائه رهیافتی ترکیبی می‌پردازیم. در این روش از مدولاسیون پارامتر آشوبی (نسل دوم)، استگانوگرافی در اطلاعات (مشابه نسل سوم) و نگاشت‌های آشوبی چند مدال استفاده خواهیم نمود. از نگاشت‌های آشوبی چند مدال برای بالا بردن امنیت سیستم‌های مخابرات آشوبی استفاده می‌شود. به‌طورکلی یکی از روش‌های بالا بردن امنیت در سیستم‌های مخابرات امن آشوبی ارسال اطلاعات رمز شده به‌وسیله این سیستم‌ها است. سیستم‌های آشوبی به دلیل دارا بودن ماهیت شبه نویز کاربردهای بسیار زیادی در این زمینه دارند و معمولاً نسل‌های مختلف سیستم‌های امن آشوبی به‌تنهایی از امنیت بالایی برخوردار نمی‌باشند.

[۴۵] Hyper chaos
[۴۶] Redundancy

استگانوگرافی برخلاف رمزنگاری که در آن فرد مزاحم از ارسال اطلاعات رمز شده اطلاع داشته ولی قادر به شناسایی رمز آن نیست؛ ارسال اطلاعات مخفی را بدون اطلاع از فرد مزاحم انجام می‌دهد بطوریکه آن فرد از ارسال اطلاعات مخفی مطلع نیست. به دلیل همین خصوصیات استگانوگرافی یکی از مواردی است که می‌توان از آن سود جست.

در رهیافت ارائه‌شده ابتدا سیگنال پیام را با استفاده از نگاشت آشوبی چند مدال با روش اصلاح مقادیر پیکسل‌ها[۴۷] استگانوگرافی[۴۸] نموده و با مدولاسیون پارامتر آشوبی ارسال می‌کنیم. سپس با سنکرون سازی انجام‌شده در گیرنده و تعیین پارامترهای نامعین سیستم و مشخص نمودن خانواده نگاشت، تصویر بازیابی می‌شود. در شکل ۵-۱ بلوک دیاگرام این رهیافت را مشاهده می‌کنید.




شکل ۵-۱. بلوک دیاگرام رهیافت جدید مخابرات امن آشوبی

[۴۷] Gray level modification(GLM)
[۴۸] Steganography

همان‌طور که در شکل ۵-۱ مشاهده می‌شود رهیافت ارائه‌شده دارای دو بخش فرستنده[۴۹] و گیرنده[۵۰] است. برای نشان دادن نحوه عملکرد این روش هر یک از این بخش‌ها را به‌طور مجزا بیان می‌کنیم. پیش از بیان نحوه عملکرد در فرستنده و گیرنده باید تعریف پنهان نگاری[۵۱]، اهمیت استفاده از پنهان نگاری و تفاوت آن با رمزنگاری موردبررسی قرار گیرد. همچنین در این بخش روش اصلاح مقادیر پیکسل‌ها[۵۲] که در این رهیافت مورداستفاده قرارگرفته است به‌صورت مشروح توضیح داده خواهد شد.

### ۵-۱- پنهان نگاری

پنهان نگاری یا استگانوگرافی هنر مخفی کردن یک پیام در یک کانال یا معبر ارتباطی است به‌طوری‌که نوع خاصی از اطلاعات موردنظر در سایر انواع اطلاعات نهفته می‌شود. حامل‌های متعددی برای این موضوع همچون متن، موسیقی و ویدیو، تصویر و غیره قابل‌طرح است ولی تصاویر دیجیتال به دلیل کثرت استفاده آن‌ها در حوزه اینترنت از عمومیت قابل‌تأملی برخوردار هستند.

اصلاح مقادیر پیکسل‌ها یک روش برای نگاشت اطلاعات با استفاده از مفهوم زوج و فرد بودن اعداد برای نگاشت اطلاعات در داخل تصویر استفاده می‌کند. این روش یک نگاشت یک‌به‌یک بین اطلاعات باینری و پیکسل انتخاب‌شده در تصویر است. ابتدا پیکسل‌های خاصی از تصویر با استفاده از یک تابع ریاضی تصادفی (در اینجا نگاشت آشوبی چند مدال) انتخاب می‌شود و مقادیر شدت روشنایی[۵۳] این پیکسل‌ها مشخص‌شده و با رشته بیتی که می‌خواهد در تصویر نگاشته شود مقایسه می‌شود. در ابتدا مقادیر شدت روشنایی تمامی پیکسل‌های انتخاب‌شده ازلحاظ زوج یا فرد بودن بررسی می‌شود. در صورت فرد بودن با تغییر یک واحد از آن این مقدار زوج می‌شود و در صورت زوج بودن بدون تغییر باقی می‌ماند. حال اگر بیتی که می‌خواهیم در پیکسل پنهان کنیم زوج باشد (یعنی ۰) پیکسل موردنظر دست‌نخورده باقی می‌ماند اما اگر بیت موردنظر فرد باشد (یعنی ۱) مقدار شدت روشنایی

---

[۴۹] Transmitter
[۵۰] Reciver
[۵۱] Steganography
[۵۲] Gray level modification (GLM)
[۵۳] Gray level

پیکسل یک واحد کم می‌شود تا آن پیکسل زوج شود. با این روش در هر پیکسل فقط یک بیت از اطلاعات را می‌توان پنهان کرد. این عمل روی تمام پیکسل‌های انتخاب‌شده تکرار می‌شود تا رشته بیت پیام به‌طور کامل نگاشته شود

این روش را می‌توان طی گام‌های زیر انجام داد:

گام اول: پیام موردنظر که می‌تواند به‌صورت عکس، متن و یا صوت باشد، به‌صورت یک‌رشته بیت درمی‌آوریم و ابعاد آن را در ۳۲ بیت اول این رشته قرار می‌دهیم.

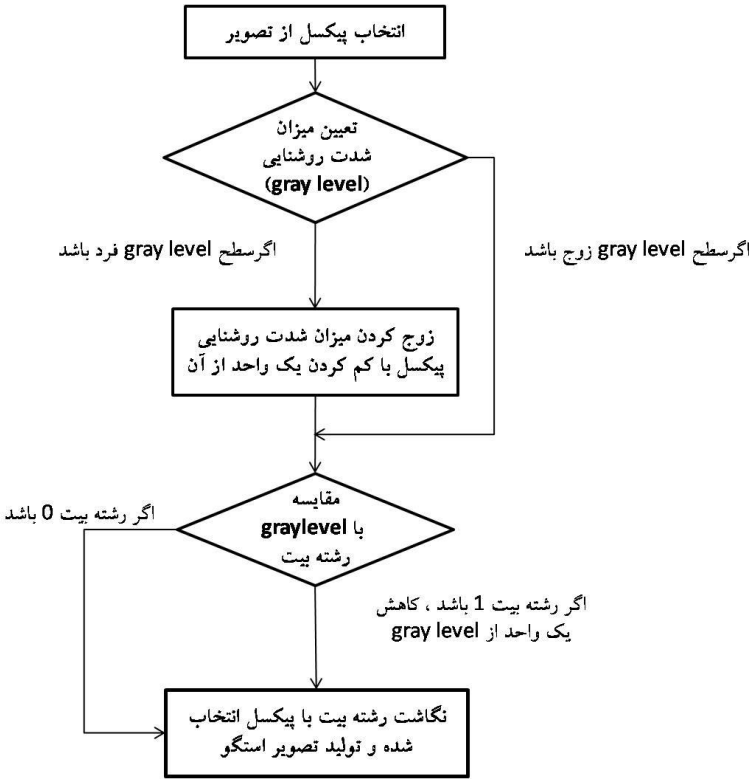
گام دوم: با استفاده از تابعی (نگاشت آشوبی چند مدال) که دو عدد را به‌عنوان کلید دریافت می‌کند، پیکسل‌هایی از تصویر به‌طور تصادفی انتخاب می‌شود.

گام سوم: مقادیر شدت روشنایی پیکسل‌های انتخاب‌شده را بررسی می‌کنیم؛ اگر فرد بودند مقدار آن‌ها را به‌اندازه یک واحد کاهش می‌دهیم تا همه آن‌ها زوج شوند.

گام چهارم: هر پیکسل را با رشته بیت حاصله مقایسه می‌کنیم. اگر مقدار آن بیت فرد بود (یعنی ۱) یک واحد از شدت روشنایی پیکسل موردنظر کم می‌کنیم و اگر بیت موردنظر زوج بود (یعنی ۰) پیکسل مربوطه بدون تغییر می‌ماند (زوج باقی می‌ماند).

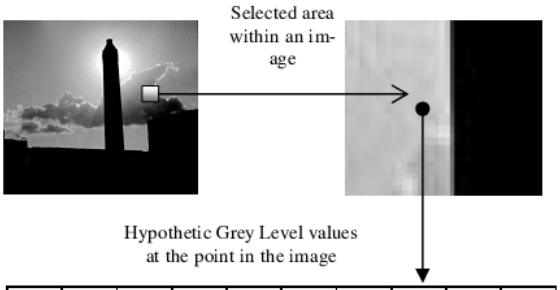
مراحل فوق را تا جایی که همه رشته بیت در داخل تصویر جای گیرد انجام می‌دهیم. بدین ترتیب روی هرکدام از پیکسل‌های انتخاب‌شده یک بیت نگاشته شده است.

فلوچارت کلی فرآیند پنهان‌سازی اطلاعات درروش GLM به‌صورت شکل (۵-۲) زیر است:




شکل ۵-۲. فلوچارت فرآیند پنهان‌سازی اطلاعات در روش GLM

به‌عنوان‌مثال بخشی از تصویر را انتخاب نموده و مقدار پیکسل‌های آن را مشخص می‌کنیم. قاعده انتخاب پیکسل‌ها می‌تواند به‌صورت معادله ساده خطی $2x+0.5w$ باشد که در آن $w$ عرض ناحیه موردنظر و $x$ سطرهای تصویر است. در شکل (۵-۳)، $w=10$ و $x=[0-9]$ است. معمولاً از یک معادله ریاضی برای انتخاب محل پیکسل‌ها برای جای دادن اطلاعات مخفی استفاده می‌شود اما در رهیافت ارائه‌شده از روش جدیدی برای انتخاب محل پیکسل‌ها استفاده می‌کنیم. در اینجا صرفاً برای سادگی توضیح مفهوم اصلاح مقادیر پیکسل‌ها از این معادله ساده خطی استفاده‌شده است.



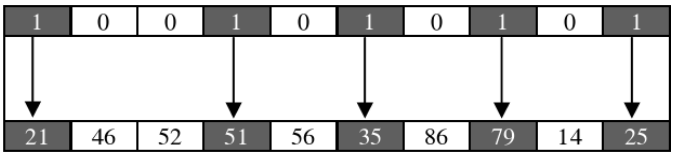

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 13 | 15 | 16 | 18 | 21 | 23 | 14 | 78 | 79 | 81 |
| 14 | 30 | 31 | 26 | 57 | 51 | 45 | 57 | 69 | 76 |
| 13 | 37 | 26 | 48 | 84 | 47 | 95 | 48 | 52 | 65 |
| 52 | 35 | 65 | 84 | 57 | 92 | 58 | 51 | 45 | 75 |
| 82 | 21 | 56 | 58 | 64 | 67 | 25 | 51 | 41 | 74 |
| 84 | 9 | 21 | 32 | 35 | 84 | 76 | 95 | 56 | 54 |
| 98 | 12 | 84 | 91 | 19 | 99 | 86 | 98 | 7 | 2 |
| 13 | 15 | 16 | 18 | 21 | 23 | 14 | 78 | 79 | 81 |
| 14 | 30 | 31 | 26 | 57 | 51 | 45 | 57 | 69 | 76 |
| 13 | 37 | 26 | 48 | 84 | 47 | 95 | 48 | 52 | 65 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 13 | 15 | 16 | 18 | 21 | 23 | 14 | 78 | 79 | 81 |
| 14 | 30 | 31 | 26 | 57 | 51 | 45 | 57 | 69 | 76 |
| 13 | 37 | 26 | 48 | 84 | 47 | 95 | 48 | 52 | 65 |
| 52 | 35 | 65 | 84 | 57 | 92 | 58 | 51 | 45 | 75 |
| 82 | 21 | 56 | 58 | 64 | 67 | 25 | 51 | 41 | 74 |
| 84 | 9 | 21 | 32 | 35 | 84 | 76 | 95 | 56 | 54 |
| 98 | 12 | 84 | 91 | 19 | 99 | 86 | 98 | 7 | 2 |
| 13 | 15 | 16 | 18 | 21 | 23 | 14 | 78 | 79 | 81 |
| 14 | 30 | 31 | 26 | 57 | 51 | 45 | 57 | 69 | 76 |
| 13 | 37 | 26 | 48 | 84 | 47 | 95 | 48 | 52 | 65 |

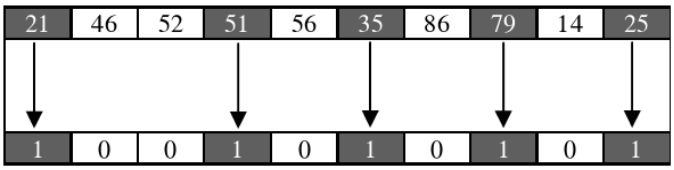
شکل ۵-۳ قاعده انتخاب پیکسل‌ها [۴۳]

۱۰ پیکسل را برای قرار دادن یک‌رشته بیت ۱۰ تایی انتخاب می‌کنیم و سپس gray level آن را طبق قاعده بالا تغییر می‌دهیم:

مسیر رفت (رمزنگاری):




مسیر برگشت (رمزگشایی):



مراحل بازیابی اطلاعات را می‌توان طی مراحل زیر انجام داد:

گام اول: با استفاده از تابعی که در مرحله مخفی سازی اطلاعات استفاده شد و کلید، محل پیکسل‌های حاوی اطلاعات را مشخص می‌کنیم.

گام دوم: مقادیر شدت روشنایی پیکسل‌های انتخاب‌شده را بررسی می‌کنیم. اگر مقدار موردنظر فرد باشد در رشته بیت ۱ را قرار می‌دهیم و اگر زوج بود در رشته بیت ۰ را قرار می‌دهیم. (برای افزایش سرعت با دستیابی به ۳۲ بیت اول طول پیام را تشخیص می‌دهیم و به‌اندازه همین طول در مسیر پیکسل‌های انتخاب‌شده تصویر جلو می‌رویم تا عملیات اضافه انجام نشود).

گام سوم: رشته بیت حاصله را به‌صورت یک رشته عدد ۸ بیتی مبنای ۱۰ درمی‌آوریم.

گام چهارم: با استفاده از ابعاد رشته عدد را به‌صورت ماتریس پیام درمی‌آوریم.

### ۵-۱-۱-معیار بررسی کیفیت تصویر استگانوگرافی

هنگام مخفی کردن اطلاعات در داخل تصویر کاور، جزییات تصویر کاور را طوری حفظ کنیم که تفاوت تصویر استگو تصویر کاور قابل‌درک و تشخیص با چشم انسان نباشد. این مسئله مهمی است که استگانوگرافی با آن مواجه است. همان‌طور که همه ما می‌دانیم کیفیت تصویر استگو بالاتر، متضمن غیرقابل ادراک تر بودن پیام پنهان‌سازی شده است. ما می‌توانیم با استفاده از معیارهای نسبت سیگنال به نویز و میزان شباهت این مسئله را ارزیابی می‌کنیم.

- **نسبت سیگنال به نویز[۵۴]:**

PSNR برای مقادیر ۸ بیتی از رابطه زیر محاسبه می‌شود:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\ dB$$

[۵۴] PSNR

$$MSE = \left(\frac{1}{M \times N}\right)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(P_{(x,y)} - P'_{(x,y)}\right)^2$$

M و N سایز تصویر،P(x,y) مقادیر پیکسل تصویر اصلی و P'(x,y)مقدار پیکسل تصویر پنهان نگاری شده را در مکان x,y نشان می‌دهد. مقادیر بزرگ‌تر PSNR نشان‌دهنده‌ی درجه کمتر اعوجاج ایجادشده بعد از پنهان‌سازی اطلاعات و مقادیر کمتر بیانگر اعوجاج بیشتر است به‌طوری‌که مقدار PSNR زیر 30dB نشان‌دهنده کیفیت خیلی پایین است؛ یعنی اعوجاج ایجادشده کاملاً قابل‌مشاهده است. برای مقادیر بالای 40dB کیفیت بالایی برای تصاویر استگو داریم.

- **میزان شباهت[۵۵]:**

این عدد میزان شباهت بین دو سیگنال را نشان می‌دهد و می‌تواند مقادیر بین ۰ و ۱ را اختیار کند. مقدار r=1 یعنی دو سیگنال دقیقا یکی هستند.

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2}\sqrt{\sum(y_i - \bar{y})^2}}$$

### ۵-۲- فرستنده

در رهیافت ارائه‌شده سیگنال اطلاعات (تصویر) با روش مدولاسیون آشوبی از طریق جمع با پارامترهای سیستم راسلر ارسال می‌شود. همان‌طور که بیان شد برای بالا بردن امنیت ارسال اطلاعات باید سیگنال اطلاعات ارسالی را پیچیده‌تر نماییم به همین دلیل ابتدا پیش‌پردازشی بر روی اطلاعات انجام می‌دهیم. این پیش‌پردازش شامل پنهان‌سازی اطلاعات مخفی درون سیگنال ارسالی (تصویر) با روش اصلاح مقادیر پیکسل‌ها است؛ بنابراین ابتدا می‌بایست محل مناسب پیکسل‌ها در تصویر برای پنهان‌سازی اطلاعات انتخاب شود.

[۵۵] similarity measure

در روش‌های مختلف استگانوگرافی برای پنهان‌سازی اطلاعات، پیکسل‌های مناسب باید طوری انتخاب شوند که هم کاملاً تصادفی و غیرقابل‌شناسایی باشند و هم حداقل تأثیر را در خصوصیات ظاهری تصویر ایجاد نمایند.

در روش ارائه‌شده از نگاشت‌های آشوبی چند مدال (فصل دوم بخش ۲-۱-۲) برای تعیین محل مناسب پیکسل‌های تصویر استفاده می‌شود. برای انتخاب نوع خانواده و عضو نگاشت چند مدال در تعیین محل پیکسل‌ها، به دو عدد $k$ و $r$ نیازمندیم. این دو عدد در فرستنده و از روی پارامترهای فرستنده طبق جداول تناظر ۵-۱ و ۵-۲ انتخاب می‌شوند. در این جداول تناظر طوری برقرارشده است که تغییر پارامترهای سیستم فرستنده، این سیستم را از حالت آشوبی خارج نمی‌کند.

دینامیک سیستم آشوبی راسلر (فرستنده) به‌صورت زیر است:

$$\begin{aligned}\dot{x}_1 &= -y_1 - z_1 \\ \dot{y}_1 &= x_1 + a y_1 \\ \dot{z}_1 &= b + z_1(x_1 - c)\end{aligned} \qquad (۱-۵)$$

این سیستم برای همسایگی پارامترهای $c \in [3,11]$، $a = b = 0.2$ و مجموعه بزرگی از شرایط اولیه رفتار آشوبی خواهد داشت. از دو پارامتر سیستم آشوبی راسلر $c_i$ و $a_j$ برای تنظیم جدول تناظر بهره می‌گیریم.

جدول ۵-۱. تناظر بین $c_i$ها و $K_i$ها

| $K_i$ | $c_i$ |
|---|---|
| $K_1 = 1$ | $c_1 = 3$ |
| $K_2 = 2$ | $c_2 = 4$ |
| $K_3 = 3$ | $c_3 = 5$ |
| $K_4 = 4$ | $c_4 = 6$ |

جدول ۵-۲. تناظر بین $a_j$ها و $r_j$ها

| $r_j$ | $a_j$ |
|---|---|
| $r_1 = 0$ | $a_1 = 0.2$ |
| $r_2 = 1$ | $a_2 = 0.3$ |
| $r_3 = 2$ | $a_3 = 0.4$ |
| $r_4 = 3$ | $a_4 = 0.5$ |

بنابراین با انتخاب پارامترهای سیستم راسلر می‌توان $c_i = k_i,\ i = 1,2,3,4$ را به‌عنوان مشخص‌کننده خانواده نگاشت آشوبی چند مدال و $a_j = r_j,\ j = 1,2,3,4$ به‌عنوان تعیین‌کننده عضو این خانواده در نظر گرفت.

با انتخاب این پارامترها، خانواده نگاشت‌های آشوبی چند مدال با توجه به رابطه (۲-۵) به‌صورت زیر قابل حصول است:

$$f_\beta(x) = \beta \begin{cases} (1/4 - x)x & for\ x \in [0,1/4); \\ (1/2 - x)(x - 1/4) & for\ x \in [1/4,1/2); \\ (3/4 - x)(x - 1/2) & for\ x \in [1/2,3/4); \\ (1 - x)(x - 3/4) & for\ x \in [3/4,1]; \end{cases}$$

که به‌عنوان‌مثال با انتخاب $c_1 = 4 \leftarrow k_1 = 4$ و داشتن $\gamma = 0.25$ برای هریک از عضوهای این خانواده داریم:

۱- نگاشت چهارمدال[۵۶] $f_{64}$ برای $r = 0$.

۲- نگاشت سه‌مدال[۵۷] $f_{48}$ برای $r = 1$.

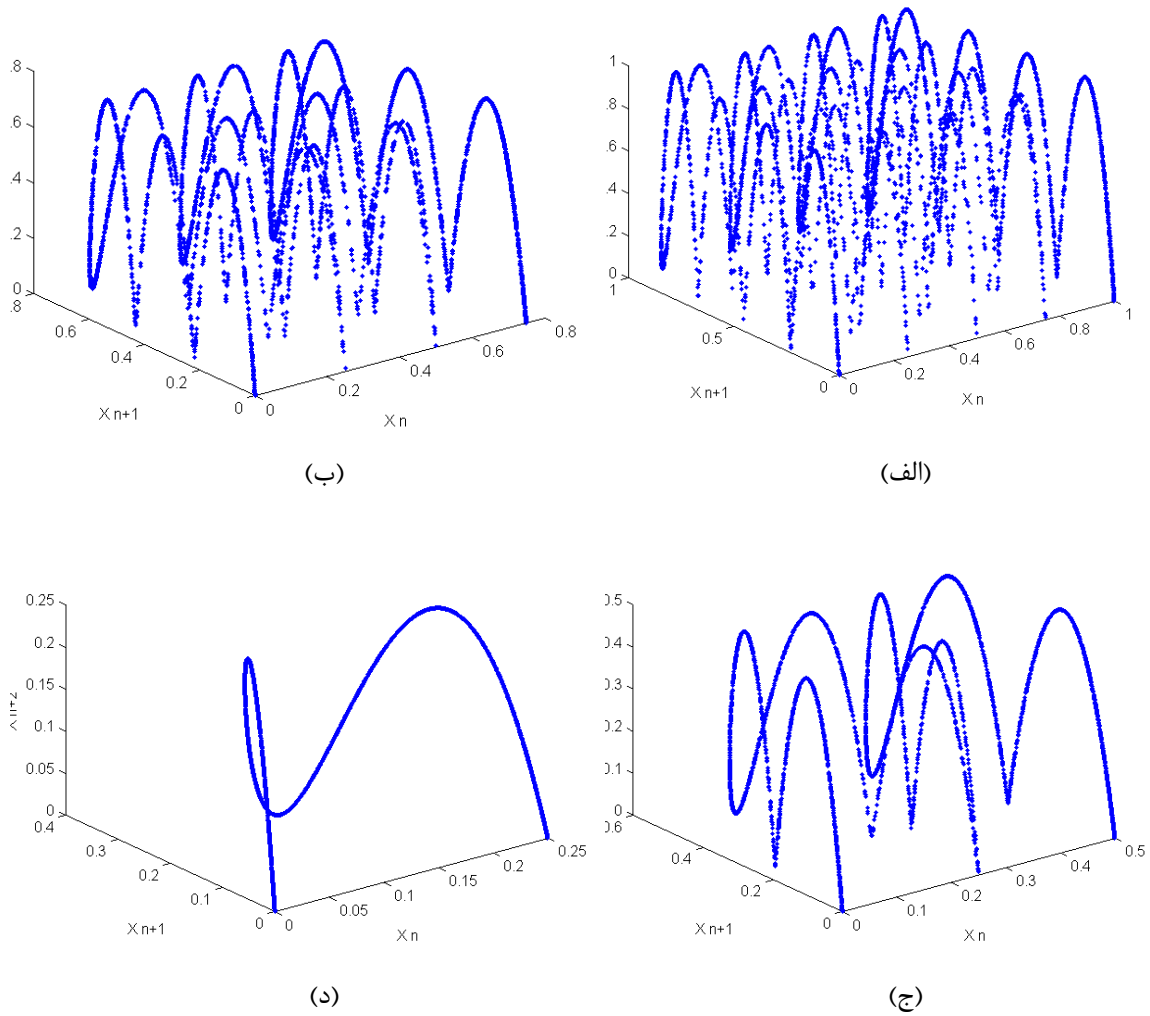
۳- نگاشت دومدال[۵۸] $f_{32}$ برای $r = 2$.

[۵۶] Quadmodal
[۵۷] Trimodal
[۵۸] Bimodal

۴- نگاشت تک‌مدال[۵۹] $f_{16}$ برای $r=3$.

حال با انتخاب هریک از $a_j \leftarrow r_j$ ها یکی از شکل‌های الف تا ج در شکل (۵-۴) حاصل می‌شود که این انتخاب به تنظیم فرستنده بستگی دارد.

شکل دیاگرام فاز ساختار کشیدگی و تاشدگی[۶۰] برای عضوهای مختلف این خانواده را نشان می‌دهد.



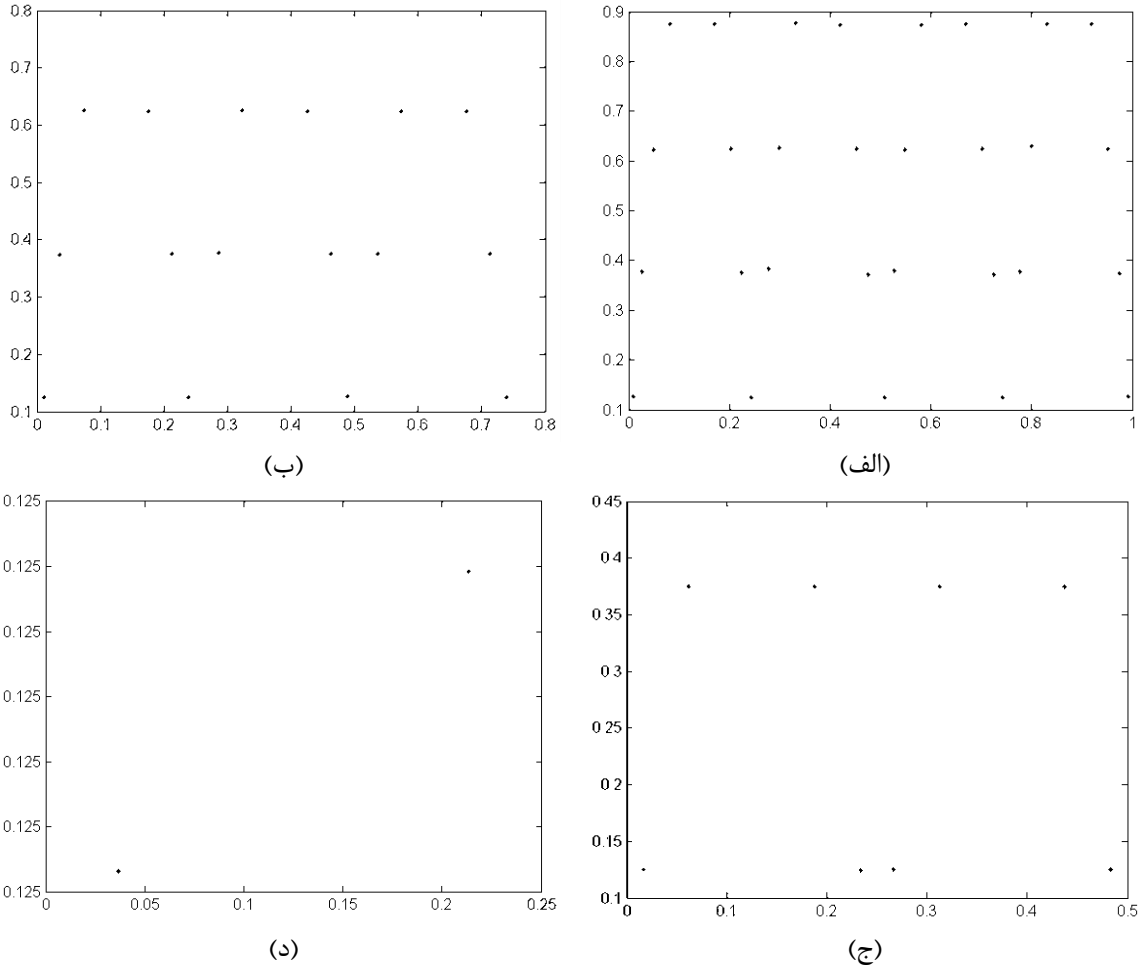

(ب) (الف)

(د) (ج)

شکل ۵-۴. دیاگرام فاز سه‌بعدی کشیدگی و تاشدگی نگاشت آشوبی چهار مدال برای $k=4$: (الف) $r=0$ (ب) $r=1$ (ج) $r=2$ (د) $r=3$.

[۵۹] Unimodal
[۶۰] Stretching and Folding

حال با منطبق کردن محورهای $x_n$ و $x_{n+1}$ نشان داده‌شده در دیاگرام کشیدگی و تاشدگی شکل (۵-۴) با محورهای $x$ و $y$ تصویر کاور[۶۱] (همان تصویری که ارسال خواهد شد)، مقدار ماکزیمم $x_{n+2}$ را به‌عنوان محل مناسب برای جایگذاری اطلاعات انتخاب می‌کنیم. شکل (۵-۵) پیکسل‌های انتخاب‌شده با توجه به شکل‌های (۵-۴) را نشان می‌دهد.




شکل ۵-۵. پیکسل‌های انتخاب‌شده به‌عنوان کاندیدای مناسب برای جایگذاری اطلاعات مطابق با شکل (۵-۴)

بنابراین با استفاده از نگاشت آشوبی چند مدال که دو عدد (دو پارامتر سیستم فرستنده طبق جداول تناظر) را به‌عنوان کلید دریافت می‌کند، پیکسل‌های مناسب برای جای دادن اطلاعات انتخاب شد.

[۶۱] Cover image

مقادیر شدت روشنایی این پیکسل‌های انتخاب‌شده با رشته بیت موردنظر (پیام مخفی) مقایسه می‌شود و از طریق روش GLM اطلاعات جایگذاری شده و تصویر استگو[۶۲] ایجاد می‌شود.

حال از قانون مدولاسیون زیر برای مدوله کردن اطلاعات $I_1(t)$ و $I_2(t)$ در پارامترهای سیستم فرستنده (۵-۱) استفاده می‌کنیم:

$$\begin{aligned} a(t) &= a + I_1(t), \quad \hat{a}(t) = \hat{a} + \hat{I}_1(t), \\ c(t) &= c + I_2(t), \quad \hat{c}(t) = \hat{c} + \hat{I}_2(t), \end{aligned} \qquad (۲-۵)$$

که $\hat{I}_1(t)$ و $\hat{I}_2(t)$ سیگنال‌های بازیابی شده می‌باشند. در مثالی که ارائه خواهد شد تنها از سیگنال $I_1(t)$ برای ارسال تصویر استگو استفاده می‌کنیم. بدهی است که می‌توان اطلاعات دیگری را نیز با $I_2(t)$ مخابره نمود.

### ۵-۳- گیرنده

پس از ارسال تصویر توسط مدولاسیون پارامتر آشوبی که درون آن پیام مخفی ذخیره‌شده است؛ برای بازیابی پیام باید ابتدا تصویر به‌درستی دریافت شود که این عمل با سنکرون سازی تطبیقی صورت می‌پذیرد. پس از سنکرون سازی صورت گرفته و تطبیق پارامترهای نامعین سیستم در گیرنده می‌توان خانواده و عضو نگاشت را با توجه به جداول تناظر مشخص نمود؛ تصویر استگو[۶۳] ایجادشده را دریافت و پیام مخفی موردنظر را بازیابی کنیم.

#### ۵-۳-۱- روش سنکرون سازی ارائه‌شده

برای انجام سنکرون سازی ارائه‌شده ابتدا لازم است تعاریف زیر بیان شود [۵]:

تعریف ۱: سیستم غیرخطی یکنواخت با بردار حالت $X = \{x_i\}_1^{i=n} \in R^n$ و بردار خروجی $G = \{g_i\}_1^{i=m} \in R^m$ به‌صورت:

[۶۲] Stego image
[۶۳] Stego image

(۳-۵)

$$\dot{X} = f(X,P), G = h(X)$$

$h(.)$ تابع بردار یکنواخت

$p \in R^l$ بردار پارامترهای ثابت و $l < n$

$G^{(j)}$ $j$ امین مشتق زمانی بردار $G$

بردار حالت $X$ را ازلحاظ جبری مشاهده‌پذیر گویند اگر برای برخی از توابع یکنواخت $\Phi$ و $j$ به‌صورت یکتا وجود داشته باشد:

(۴-۵)

$$X = \Phi(G, G^{(1)},...,G^{(j)})$$

تعریف ۲: برای برخی از شرایط تعریف ۱ اگر بردار پارامترهای $P$ رابطه زیر را برآورده کند:

(۵-۵)

$$\Omega_1(G,...,G^{(j)}) = \Omega_2(Y,...,Y^{(j)})P$$

که $\Omega_1(.)$ و $\Omega_2(.)$ به ترتیب ماتریس‌های یکنواخت $n\times 1$ و $n \times n$ هستند. $P$ از دیدگاه $G$ به‌صورت جبری قابل‌شناسایی گفته می‌شود.

بر اساس تعاریف صورت گرفته سیستم (۵-۱) به‌صورت جبری مشاهده‌پذیر خواهد بود و با در نظر $g_1 = y_1$ و $g_2 = z_1$ حالت $x_1$ را می‌توان به‌صورت زیر نوشت:

$$x_1 = \dot{g}_1 - ag_1 \qquad (۶-۵)$$

بنابراین با انتخاب این خروجی‌ها، سیستم راسلر مشاهده‌پذیر جبری است و با جایگزینی در معادله دیفرانسیل (۵-۱) داریم:

$$b + \dot{g}_1 g_2 - \dot{g}_2 = ag_1 g_2 + cg_2 \qquad (۷-۵)$$

بنابراین بردار پارامترهای $p=(a,c)$ و حالت خارج از دسترس $x_1$ با تعاریف صورت گرفته قابل حصول خواهند بود.

با تعاریف صورت گرفته مسئله سنکرون سازی سیستم راسلر با پارامترهای نامعین بطوریکه حالت‌های $y_1$ و $z_1$ در دسترس می‌باشند قابل انجام است و پارامترهای نامعین $c$ و $a$ به دست خواهند آمد.

سیستم نامعین راسلر (۵-۱) را با حالت‌های خروجی معین $z_1$ و $y_1$ به‌عنوان فرستنده در نظر گرفته و برای سیستم گیرنده داریم:

$$\begin{aligned}\dot{x}_2 &= -y_1 - z_1 + u_1\\ \dot{y}_2 &= x_2 + \hat{a}y_1 + u_2\\ \dot{z}_2 &= b + z_1(x_2 - \hat{c}) + u_3\end{aligned} \qquad (۵-۸)$$

هدف کنترلی پیدا کردن $u=(u_1,u_2,u_3)$ و $\hat{p}=(\hat{a},\hat{c})$ بطوریکه سیستم‌های فرستنده و گیرنده سنکرون شده و $\hat{p}$ به مقدار واقعی $(a,c)$ همگرا شود به‌عبارت‌دیگر با انتخاب مناسب $u$ و $\hat{p}$ برای سیستم (۲) داشته باشیم:

$$(w_1,\hat{p}) \to (w_2,p), \quad t\to\infty$$

$w_1$ و $w_2$ به ترتیب بردارهای حالت فرستنده و گیرنده هستند و $w_i^T=(x_i,y_i,z_i);\ for\, i=\{1,2\}$.

در این مقاله از هردو پارامتر سیستم برای ارسال سیگنال‌های $I_1(t)$ و $I_2(t)$ استفاده می‌شود. از قانون مدولاسیون زیر برای مدوله کردن $I_1(t)$ و $I_2(t)$ در پارامترهای سیستم فرستنده (۵-۱) استفاده می‌کنیم:

$$\begin{aligned}a(t) &= a + I_1(t), \quad \hat{a}(t) = \hat{a} + \hat{I}_1(t),\\ c(t) &= c + I_2(t), \quad \hat{c}(t) = \hat{c} + \hat{I}_2(t),\end{aligned}$$

که $\hat{I}_1(t)$ و $\hat{I}_2(t)$ سیگنال‌های بازیابی شده می‌باشند.

حال خطاهای سیستم را به‌صورت زیر تعریف می‌کنیم:

$$e_x = x_1 - x_2; \quad e_y = y_1 - y_2; \quad e_z = z_1 - z_2; \tag{۹-۵}$$

$$\begin{aligned} &\tilde{a} = a - \hat{a}; \quad \tilde{c} = c - \hat{c}; \\ &\hat{I}_1 = I_1 - \hat{I}_1; \quad \hat{I}_2 = I_2 - \hat{I}_2; \end{aligned} \tag{۱۰-۵}$$

بنابراین داریم:

$$e^T = (e_x, e_y, e_z); \quad \tilde{p}^T = (\tilde{a}, \tilde{c}); \quad \tilde{I}^T = (\tilde{I}_1, \tilde{I}_2) \tag{۱۱-۵}$$

با توجه به روابط ارائه‌شده داریم:

$$\dot{e} = \begin{bmatrix} \dot{e}_x \\ \dot{e}_y \\ \dot{e}_z \end{bmatrix} = \begin{bmatrix} -u_1 \\ ex + \tilde{a}y + \tilde{I}_1 y - u_2 \\ ze_x - \tilde{c}z - \tilde{I}_2 z - u_3 \end{bmatrix} \tag{۱۲-۵}$$

برای ساده‌سازی $y = y_1$ و $x = x_1$ در نظر می‌گیریم. همان‌طور که مشاهده می‌شود در این مسئله کنترلی بردارهای ورودی $u$ و $\tilde{p}$ طوری باید طراحی شوند که $e$ به‌صورت مجانبی به سمت صفر میل کند.

### ۵-۳-۲- طراحی کنترل‌کننده

در این بخش کنترل‌کننده برای ردیابی پیوسته تغییرات پارامترهای مدوله‌شده در گیرنده بیان می‌شود و سپس $I_1(t)$ و $I_2(t)$ با استفاده از این کنترل‌کننده بازیابی خواهند شد. مسئله کنترل را با استفاده از روش لیاپانوف حل می‌کنیم و بر اساس تابع لیاپانوف تخمینگر موردنظر را برای تضمین سنکرون سازی دو سیستم ارائه می‌دهیم.

تابع لیاپانوف زیر را در نظر می‌گیریم:

$$V = \frac{1}{2}e^T e + \frac{1}{2}\tilde{p}^T \tilde{p} + \frac{1}{2}\tilde{I}^T \tilde{I} \qquad (۱۳-۵)$$

مشتق تابع لیاپانوف به‌صورت زیر است:

$$\begin{aligned} \dot{V} &= \tilde{a}\dot{\tilde{a}} + \tilde{c}\dot{\tilde{c}} - e_x u_1 + e_x e_y + \tilde{a} y e_y + \tilde{I}_1 y e_y - e_y u_2 \\ &+ z e_x e_z - \tilde{c} z e_z - \tilde{I}_2 z e_z - e_z u_3 + \tilde{I}_1 \dot{\tilde{I}}_1 + \tilde{I}_2 \dot{\tilde{I}}_2 \end{aligned} \qquad (۱۴-۵)$$

برای آن‌که $\dot{V}$ منفی معین باشد جملات مثبت آن را مساوی صفر قرار داده و بقیه جملات آن را به نحوی انتخاب می‌کنیم که کل $\dot{V}$ منفی معین شود آنگاه برای $\dot{\tilde{p}}$، $u$ و $\dot{\tilde{I}}$ داریم:

$$u = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} e_y + z e_z \\ k_1 e_y^d \times sign(e_y) \\ k_2 e_z^d \times sign(e_z) \end{bmatrix} \qquad (۱۵-۵)$$

$$\dot{\tilde{p}} = \begin{bmatrix} \dot{\tilde{a}} \\ \dot{\tilde{c}} \end{bmatrix} = \begin{bmatrix} -y e_y \\ z e_z \end{bmatrix} \qquad (۱۶-۵)$$

$$\dot{\tilde{I}} = \begin{bmatrix} \dot{\tilde{I}}_1 \\ \dot{\tilde{I}}_2 \end{bmatrix} = \begin{bmatrix} -y e_y \\ z e_z \end{bmatrix} \qquad (۱۷-۵)$$

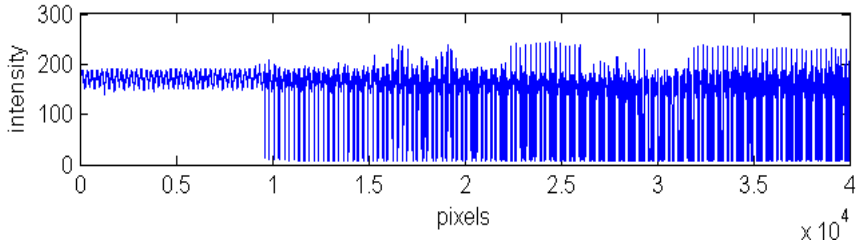
$k_1$ و $k_2$ ثابت‌های مثبت مطلق و $d$ هر عدد مثبت صحیح

## ۵-۴- شبیه‌سازی

برای نشان دادن نتیجه روش پیشنهادی از تصویرکاور نمونه شکل (۵-۶-الف) با سایز 256×256 استفاده می‌کنیم. شبیه‌سازی انجام‌شده صحت روش ارائه‌شده را نشان می‌دهد. تصویر موردنظر را به

بردار تبدیل کرده تا بتوانیم این تصویر را به‌عنوان اطلاعات $I_1(t)$ در سیستم ارسال کنیم. شکل (۵-۶) تصویر اصلی و بردار تصویر را نشان می‌دهد.

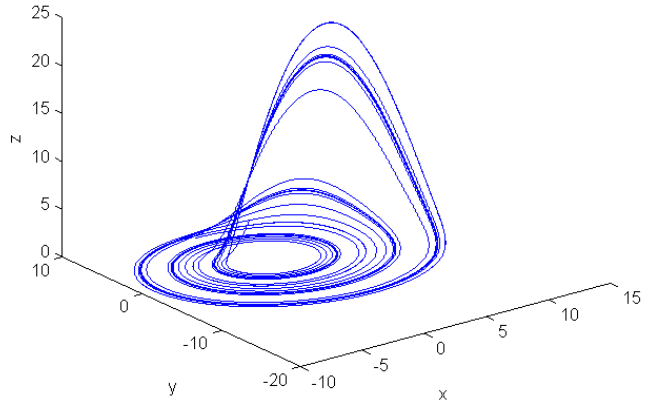
(الف)



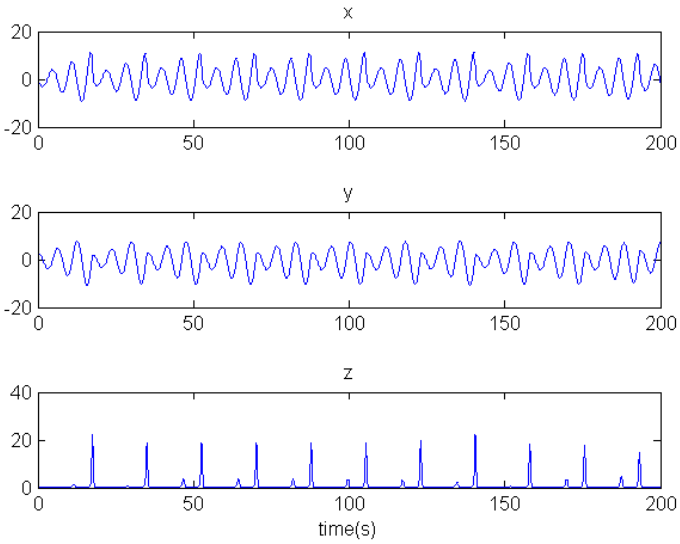

(ب)

شکل ۵-۶. (الف) تصویر اصلی مورداستفاده برای استگانوگرافی (ب) بردار پیکسل‌های تصویر

پارامترهای سیستم فرستنده $p=(a=0.2,c=5.7)$ و شرایط اولیه آن را $x_1(0)=1, y_1(0)=-1, z_1(0)=1$ در نظر می‌گیریم. شکل (۵-۷) جاذب آشوبی و رفتار همه‌ی حالت‌های سیستم راسلر را نشان می‌دهد.




(الف)



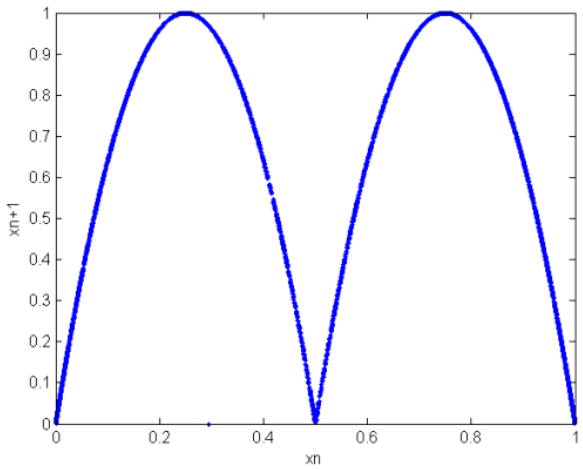

(ب)

شکل ۵-۷.(الف) جاذب آشوبی سیستم راسلر (ب) رفتار همه‌ی حالت‌های سیستم آشوبی راسلر

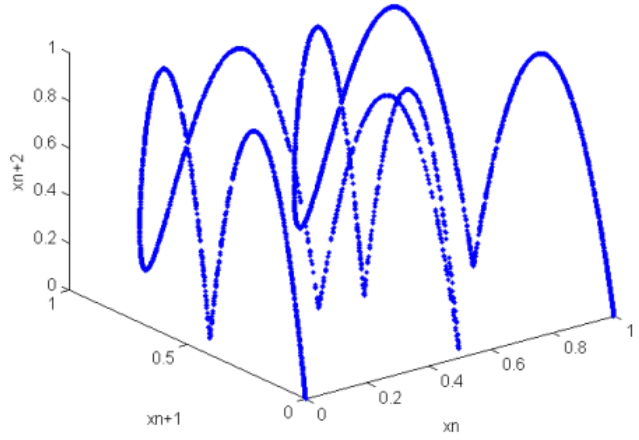
به‌عنوان‌مثال با انتخاب $c_2 = 4 \to k_2 = 2$ و $a_1 = 0.2 \to r_1 = 0$ خانواده نگاشت دو مدال $F$ به‌صورت زیر به دست می‌آید.

$$f_{16}(x) = 16\begin{cases}(1/2 - x)x & for\ x \in [0,0.5); \\ (1-x)(x-1/2) & for\ x \in [0.5,1];\end{cases}$$

شکل (۵-۸) دیاگرام کشیدگی و تاشدگی این خانواده را نشان می‌دهد




(الف)

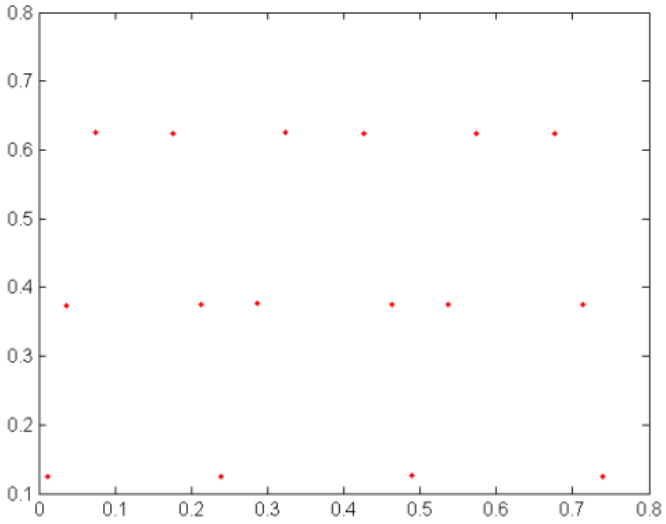



(ب)

شکل ۵-۸. (الف) نگاشت‌های لجستیک خانواده $F$ (ب) دیاگرام فاز کشیدگی و تاشدگی این ساختار

با منطبق کردن محورهای $x_n$ و $x_{n+1}$ نشان داده‌شده در دیاگرام کشیدگی و تاشدگی این ساختار با محورهای $x$ و $y$ تصویر کاور، مقدار ماکزیمم $x_{n+2}$ را به‌عنوان محل مناسب برای جایگذاری اطلاعات انتخاب می‌کنیم. شکل (۵-۹) نقاط انتخاب‌شده برای جای دادن پیام مخفی را نشان می‌دهد. در این

رهیافت تصویر اصلی بلوک‌بندی شده است تا بتوانیم نقاط بیشتری را به دست آورده و حجم اطلاعات بیشتری را در تصویر پنهان کنیم.




شکل ۵-۹. پیکسل‌های انتخاب‌شده برای جایگذاری اطلاعات

در این شبیه سازی به عنوان مثال یک بلوک ۱۶×۱۶ از تصویر کاور را انتخاب می کنیم. پیکسل های هایی که با نگاشت آشوبی چند مدال انتخاب شده اند با عدد ۱ مشخص شده است.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ | ۱ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۱ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ | ۰ |
| ۱ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ | ۰ | ۰ | ۰ | ۱ |

اطلاعاتی که می‌خواهیم در تصویر کاور مخفی کنیم را به‌صورت زیر باینری می‌کنیم. این اطلاعات در شبیه‌سازی ارائه‌شده به‌صورت متن می‌باشد که به‌طور مثال نام و نام خانوادگی و... به‌عنوان اطلاعات مخفی ارسال می‌شود.

1001101110000111100111101111111010111001001…

Masoud khodadad-zadeh
MSc student of control Engineering,
Shahrood University of Technology,
Shahrood,Iran
…

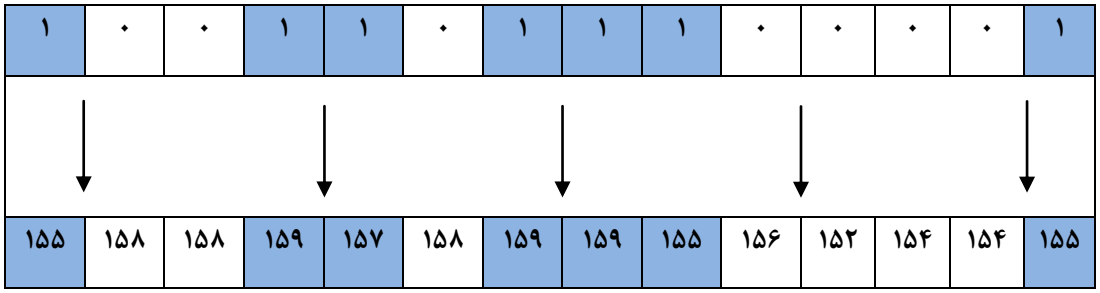
مقادیر شدت روشنایی پیکسل‌های بلوک انتخاب‌شده به‌صورت زیر است.

| ۱۵۶ | ۱۵۹ | ۱۵۸ | ۱۵۵ | ۱۵۸ | ۱۵۶ | ۱۵۹ | ۱۵۸ | ۱۵۷ | ۱۵۸ | ۱۵۸ | ۱۵۹ | ۱۶۰ | ۱۶۰ | ۱۶۰ | ۱۵۸ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ۱۶۰ | ۱۵۴ | ۱۵۷ | ۱۵۸ | ۱۵۷ | ۱۵۹ | ۱۵۸ | ۱۵۸ | ۱۵۸ | ۱۶۰ | ۱۵۵ | ۱۵۶ | ۱۵۹ | ۱۵۸ | ۱۶۰ | ۱۵۷ |
| ۱۵۶ | ۱۵۹ | ۱۵۸ | ۱۵۵ | ۱۵۸ | ۱۵۶ | ۱۵۹ | ۱۵۸ | ۱۵۷ | ۱۵۸ | ۱۵۸ | ۱۵۹ | ۱۶۰ | ۱۶۰ | ۱۶۰ | ۱۵۸ |
| ۱۶۰ | ۱۵۴ | ۱۵۷ | ۱۵۸ | ۱۵۷ | ۱۵۹ | ۱۵۸ | ۱۵۸ | ۱۵۸ | ۱۶۰ | ۱۵۵ | ۱۵۶ | ۱۵۹ | ۱۵۸ | ۱۶۰ | ۱۵۷ |
| ۱۵۶ | ۱۵۳ | ۱۵۵ | ۱۵۹ | ۱۵۹ | ۱۵۵ | ۱۵۶ | ۱۵۵ | ۱۵۵ | ۱۵۷ | ۱۵۵ | ۱۵۴ | ۱۵۴ | ۱۵۸ | ۱۶۲ | ۱۵۷ |
| ۱۵۵ | ۱۵۵ | ۱۵۵ | ۱۵۷ | ۱۵۶ | ۱۵۹ | ۱۵۲ | ۱۵۸ | ۱۵۶ | ۱۵۸ | ۱۵۲ | ۱۵۳ | ۱۵۹ | ۱۵۶ | ۱۵۷ | ۱۶۱ |
| ۱۵۶ | ۱۵۳ | ۱۵۷ | ۱۵۶ | ۱۵۳ | ۱۵۵ | ۱۵۴ | ۱۵۵ | ۱۵۴ | ۱۵۶ | ۱۵۵ | ۱۵۶ | ۱۵۵ | ۱۵۷ | ۱۵۸ | ۱۶۰ |
| ۱۵۹ | ۱۵۹ | ۱۵۶ | ۱۵۸ | ۱۵۶ | ۱۵۹ | ۱۵۷ | ۱۶۱ | ۱۶۲ | ۱۵۷ | ۱۵۷ | ۱۵۹ | ۱۶۱ | ۱۵۶ | ۱۶۳ | ۱۵۸ |
| ۱۵۸ | ۱۵۵ | ۱۵۸ | ۱۵۴ | ۱۵۶ | ۱۶۰ | ۱۶۲ | ۱۵۵ | ۱۵۹ | ۱۶۱ | ۱۵۶ | ۱۶۱ | ۱۶۰ | ۱۵۵ | ۱۵۸ | ۱۶۱ |
| ۱۵۵ | ۱۵۴ | ۱۵۷ | ۱۵۸ | ۱۶۰ | ۱۶۰ | ۱۵۹ | ۱۶۰ | ۱۵۸ | ۱۶۱ | ۱۶۰ | ۱۶۰ | ۱۵۸ | ۱۶۱ | ۱۵۸ | ۱۶۰ |
| ۱۵۴ | ۱۵۷ | ۱۵۷ | ۱۵۷ | ۱۵۶ | ۱۵۵ | ۱۵۹ | ۱۵۴ | ۱۵۹ | ۱۵۸ | ۱۶۱ | ۱۵۸ | ۱۵۸ | ۱۶۰ | ۱۵۹ | ۱۶۰ |
| ۱۵۲ | ۱۵۰ | ۱۵۵ | ۱۵۴ | ۱۵۲ | ۱۵۶ | ۱۵۷ | ۱۵۶ | ۱۵۷ | ۱۵۴ | ۱۵۷ | ۱۵۹ | ۱۵۵ | ۱۵۶ | ۱۵۹ | ۱۶۰ |
| ۱۵۷ | ۱۵۳ | ۱۵۶ | ۱۵۵ | ۱۵۷ | ۱۶۰ | ۱۶۰ | ۱۵۷ | ۱۵۹ | ۱۵۹ | ۱۶۰ | ۱۶۱ | ۱۶۰ | ۱۶۰ | ۱۵۸ | ۱۶۳ |
| ۱۵۱ | ۱۵۴ | ۱۵۷ | ۱۵۶ | ۱۵۶ | ۱۵۸ | ۱۵۸ | ۱۵۶ | ۱۵۷ | ۱۵۹ | ۱۵۸ | ۱۵۶ | ۱۵۹ | ۱۶۱ | ۱۵۹ | ۱۶۰ |
| ۱۵۶ | ۱۵۷ | ۱۵۷ | ۱۶۰ | ۱۵۹ | ۱۵۹ | ۱۵۶ | ۱۵۸ | ۱۵۹ | ۱۶۲ | ۱۶۱ | ۱۶۰ | ۱۶۰ | ۱۶۱ | ۱۶۲ | ۱۶۴ |
| ۱۵۷ | ۱۵۸ | ۱۵۹ | ۱۵۷ | ۱۵۷ | ۱۵۴ | ۱۵۳ | ۱۵۸ | ۱۵۹ | ۱۵۵ | ۱۶۰ | ۱۵۹ | ۱۶۱ | ۱۶۱ | ۱۵۹ | ۱۶۰ |

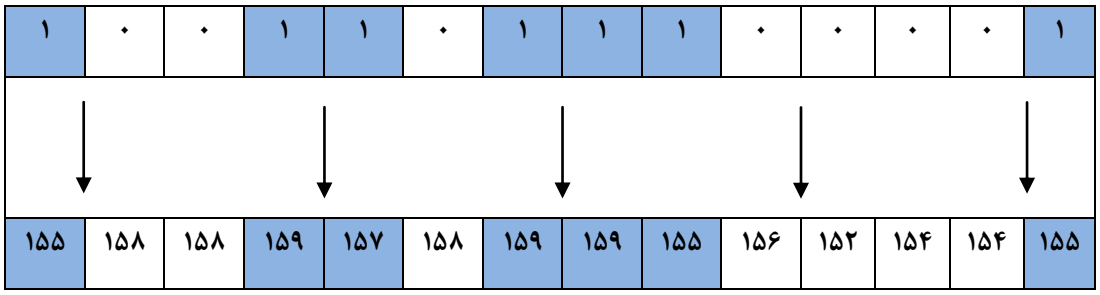
در ابتدا مقادیر شدت روشنایی تمامی پیکسل‌های انتخاب‌شده ازلحاظ زوج یا فرد بودن بررسی می‌شود. در صورت فرد بودن با تغییر یک واحد از آن این مقدار زوج می‌شود و در صورت زوج بودن بدون تغییر باقی می‌ماند. با این روش در هر پیکسل فقط یک بیت از اطلاعات را می‌توان پنهان کرد. این عمل روی تمام پیکسل‌های انتخاب‌شده تکرار می‌شود تا رشته بیت پیام به‌طور کامل نگاشته شود.

به‌عنوان‌مثال یک‌رشته بیت ۱۴ تایی مربوط به ابتدای پیام را انتخاب نموده و مطابق شکل زیر در پیکسل‌های تصویر مخفی می‌کنیم.

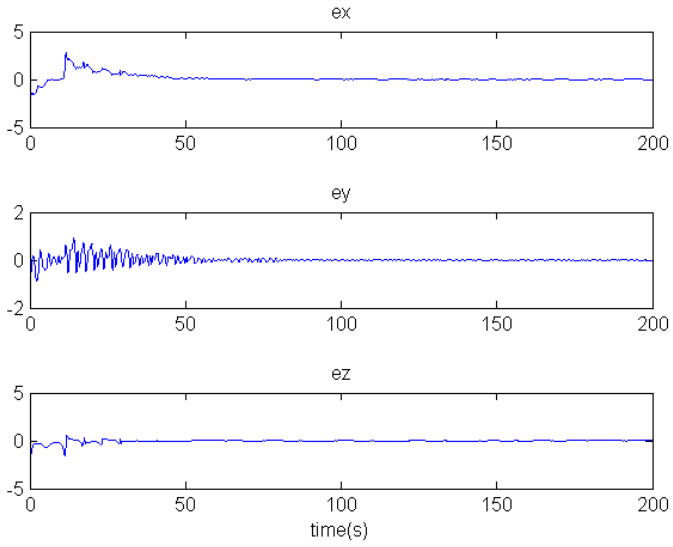
مسیر رفت (رمزنگاری):



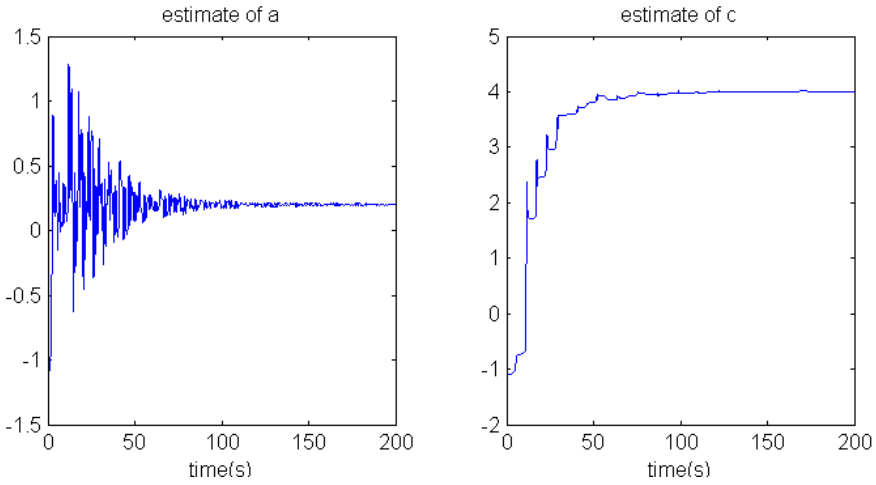

مسیر برگشت (رمزگشایی):




برای نشان دادن کارکرد کنترل‌کننده طراحی‌شده $k_1 = k_2 = 0.7$ و $m = 4$ با شرایط اولیه $x_1(0) = y_1(0) = z_1(0) = 0$ ، $\hat{p}(0) = 0,$ و $\hat{I}_1 = -2$ در نظر می‌گیریم. شکل (۵-۱۰) نشان می‌دهد که خطا در سنکرون سازی صورت گرفته به‌صورت مجانبی به صفر همگرا شده و پارامترهای نامعین سیستم گیرنده به پارامترهای واقعی همگرا می‌شود. مقدار $PSNR = 47dB$ و $r = 0.966$ بدست آمد که نشان دهنده مناسب بودن روش طراحی شده می باشد.



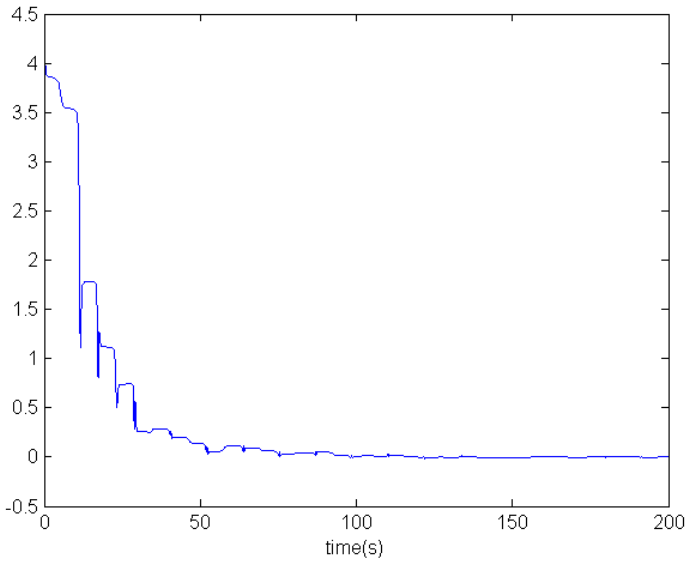

(الف)




(ب)

شکل ۵-۱۰. (الف) خطاهای سنکرون سازی (ب) تخمین پارامترهای سیستم گیرنده زمانی که سیستم در شرایط اولیه $(1,1,1)$ و برای پارامترها با مقدار واقعی $p=(0.2,4)$

همان‌طور که انتظار داریم هرچه زمان افزایش یابد این سنکرون سازی دارای عملکرد بهتر خواهد بود. شکل (۵-۱۱) خطای سیگنال پیام بین گیرنده و فرستنده را در رهیافت مخابرات امن آشوبی ارائه‌شده را نشان می‌دهد که باگذشت زمان به سمت صفر همگرا خواهد شد. بدیهی است به علت تاخیری که در همگرایی سیستم وجود دارد این روش به صورت برخط قابل استفاده نخواهد بود.




شکل ۵-۱۱. نتایج عددی سیگنال پیام $I_1$ و خطای بازیابی اطلاعات ($I_1 - \hat{I}_1$)

در این شبیه‌سازی انجام شده یک متن به‌عنوان سیگنال پیام مورداستفاده قرار گرفت و به‌عنوان اطلاعات مخفی در تصویر استگو جایگذاری شده است. برای افزایش ظرفیت جایگذاری اطلاعات، ابتدا تصویر کاور مورداستفاده به‌صورت $8\times8$ بلوک‌بندی کرده و سپس نقاط موردنظر را با استفاده از نگاشت انتخاب می‌کنیم. این روش بر اساس سنکرون سازی صورت گرفته اطلاعات بطور کامل بازیابی می شود ولی اگر شرایط و نویز کانال را در نظر بگیریم ممکن است باعث از دست دادن نمونه و ایجاد مشکل در بازیابی تصویرشویم.

شکل (۵-۱۲) تصویر استگو پس از جایگذاری متن اطلاعات در تصویر کاور را نشان می‌دهد. همان‌طور مشاهده می‌شود کمترین تأثیر را در خصوصیات و ویژگی‌های تصویر در مقایسه با تصویر اصلی گذاشته است. دراین تصویر اطلاعات متنی به صورت زیر پنهان و بازیابی شده است:

Masoud khodadad-zadeh
MSc student of control Engineering,
Shahrood University of Technology,
Shahrood,Iran
…

شکل ۵-۱۲. شکل تصویر استگو پس از جایگذاری اطلاعات متنی در تصویر

# فصل ششم: نتیجه‌گیری و پیشنهادات

نسل‌های ارائه‌شده دارای درجه امنیت پایین هستند بنابراین می‌بایست رهیافتی جدید و دارای امنیت بیشتر ارائه شود ازاین‌رو روشی جدید برای سیستم‌های مخابرات امن آشوبی با ترکیبی از نسل دوم و سوم، نگاشت‌های آشوبی چند مدال و استگانوگرافی[۶۴] در تصویر ارائه شد.

از وقتی نتایج بررسی‌های انجام‌شده برای به‌کارگیری آشوب در رمزنگاری منجر به سیستم‌های مخابراتی امن آشوبی از مرتبه پایین شد، نگرانی‌هایی در مورد اینکه این شماها که ممکن است به‌اندازه کافی امن نباشد به وجود آمد. به‌منظور رفع این نگرانی یک‌راه استفاده از سیستم‌های مخابرات امن فوق آشوب[۶۵] است اما همزمان سازی این سیستم‌ها دارای مشکلات بسیار بیشتری است. از سویی دیگر می‌توانیم امنیت سیستم‌های مخابرات امن آشوبی مرتبه پایین را با استفاده از ترکیب سیستم‌های رمزنگاری معمول با سیستم‌های آشوبی افزایش دهیم. برای رفع مشکل امنیت پایین سیستم‌های مخابرات امن آشوبی پیوسته مرتبه پایین، می‌توان یکی از دو روش زیر را بکار برد. اولین روش افزایش پیچیدگی سیگنال ارسالی و روش دوم کاهش افزونگی[۶۶] در سیگنال ارسالی است. در این پایان‌نامه از ترکیب روش‌ها و نسل‌های مختلف سیستم‌های مخابرات امن آشوبی برای افزایش پیچیدگی سیگنال ارسالی با بهره‌گیری از نگاشت‌های آشوبی چند مدال و استگانوگرافی در تصویر استفاده‌شده است. همچنین لازم به ذکر است که برای کاهش افزونگی سیگنال ارسالی می‌توان از روش‌های سنکرون سازی غیر پیوسته ضربه‌ای استفاده نمود.

در این شما ابتدا سیگنال پیام را با استفاده از نگاشت آشوبی چند مدال با روش اصلاح مقادیر پیکسل‌ها[۶۷] استگانوگرافی[۶۸] نموده و با مدولاسیون پارامتر آشوبی ارسال می‌کنیم. سپس با سنکرون سازی انجام‌شده در گیرنده و تعیین پارامترهای نامعین سیستم و مشخص نمودن خانواده نگاشت، تصویر بازیابی می‌شود.

---

[۶۴] Steganography
[۶۵] Hyper chaos
[۶۶] Redundancy
[۶۷] Gray level modification
[۶۸] Steganography

از نگاشت‌های آشوبی چند مدال برای بالا بردن امنیت سیستم‌های مخابرات آشوبی استفاده می‌شود. به‌طورکلی یکی از روش‌های بالا بردن امنیت در سیستم‌های مخابرات امن آشوبی ارسال اطلاعات رمز شده به‌وسیله این سیستم‌ها است. سیستم‌های آشوبی به دلیل دارا بودن ماهیت شبه نویز کاربردهای بسیار زیادی در این زمینه دارند. معمولاً نسل‌های مختلف سیستم‌های امن آشوبی به‌تنهایی از امنیت بالایی برخوردار نمی‌باشند. استگانوگرافی برخلاف رمزنگاری که در آن فرد مزاحم از ارسال اطلاعات رمز شده اطلاع داشته ولی قادر به شناسایی رمز آن نیست؛ ارسال اطلاعات مخفی را بدون اطلاع از فرد مزاحم انجام می‌دهد بطوریکه آن فرد از ارسال اطلاعات مخفی مطلع نیست. به دلیل همین خصوصیات استگانوگرافی یکی از مواردی است که می‌توان از آن سود جست.

همچنین می‌توان از پیشنهادها زیر برای ادامه کار و بهبود روش‌های موجود استفاده نمود:

- ✓ به دست آوردن و تحلیل روابط فضای حالت طراحی‌های صورت گرفته در کانال‌های متغیر بازمان و طراحی مناسب رویتگر به‌منظور همزمانی در این شرایط.
- ✓ به دست آوردن و تحلیل روابط فضای حالت طراحی‌های صورت گرفته با تغییر در ساختار فرستنده و نیز نوع مولدهای آشوبی و طراحی رویتگر مناسب به‌منظور همزمانی در این شرایط.
- ✓ مدل‌سازی دقیق‌تر کانال‌های مخابراتی به‌صورت کانال‌های متغیر بازمان و تلاش برای استفاده از تکنیکهای مخابراتی متداول در این کانال‌ها.
- ✓ تحلیل دقیق پارامترهای امنیتی سیستم‌های طراحی‌شده و مقایسه آن با سایر سیستم‌های پهن باند.
- ✓ تلاش برای تحلیل و بررسی انواع حملات امنیتی به سیستم آشوبی و ارائه راهکارهایی به‌منظور افزایش امنیت سیستم

- ✓ پیاده‌سازی سخت‌افزاری طراحی‌های صورت گرفته بر روی تراشه‌های DSP یا FPGA پس از تحلیل کامل مداری آن.

## پیوست الف- اثبات همگرایی خطا در روش شبه مد لغزشی

اگر با $u(t)$ ارائه‌شده در خطا سیستم را کنترل کنیم، مسیر حالت سیستم به مانیفولد شبه لغزشی با $|s(t)| \le \delta_Q = \frac{w\delta}{w-1}$ محدود خواهد شد.

اثبات:

تابع لیاپانوف $V = \frac{1}{2}s^2$ را در نظر می‌گیریم، داریم:

(الف-۱)

$$\begin{aligned}
\dot{V} &= s\dot{s} \\
&= s(\dot{e}_2 + \lambda \dot{e}_1) \\
&= s((28 - \frac{35}{29}k)e_1 + (k-1)e_2 - y_1 y_2 + \\
&\quad x_1 x_2 + d(t) + u + \lambda(10 + \frac{25}{29}k)(e_2 - e_1)) \\
&\le \eta|s| - \frac{w\eta s^2}{|s| + \delta} \\
&= \eta|s| - w\eta(|s| - \frac{|s|\delta}{|s| + \delta})
\end{aligned}$$

تا زمانی که $\frac{|s|\delta}{|s| + \delta} \le \delta$ داریم:

$$\dot{V} \le \eta|s| - \frac{w\eta s^2}{|s| + \delta} = (1-w)\eta\left(|s| - \frac{w\delta}{w-1}\right) \qquad \text{(الف-۲)}$$

هنگامی‌که برای کنترل‌کننده‌های $w > 1$ را انتخاب کنیم تا زمانی که $|s(t)| > \delta_Q = \frac{w\delta}{w-1}$ باشد، $\dot{V} < 0$خواهد بود بدین معنی که $|s|$ به ناحیه $|s(t)| \le \delta_Q = \frac{w\delta}{w-1}$ همگرا خواهد شد بنابراین اثبات کامل می‌شود.

## پیوست ب- اثبات همگرایی مدلغزشی تطبیقی

تابع لیاپانوف زیر را در نظر می‌گیریم

$$V(t)=\frac{1}{2}S^T(y_e)S(y_e)+\frac{1}{2}(\rho-\hat{\rho})^2 \qquad (ب-۱)$$

$$\begin{aligned}
&\dot{V}(t)=S^T(y_e)\dot{S}(y_e)-(\rho-\hat{\rho})\dot{\hat{\rho}}\\
&=S^T(y_e)\left[\sigma\hat{A}e(t)+\sigma\hat{B}(f(T^{-1}\hat{x},t)-f(T^{-1}\hat{x}_0,t))+\sigma\hat{B}\phi(u(t))\right]-k(\rho-\hat{\rho})\|S(y_e)\|\\
&\le\|S(y_e)\|\left[\left\|\sigma\hat{A}\right\|\|e(t)\|+\|\sigma_2B_1\|\left\|f(T^{-1}\hat{x},t)-f(T^{-1}\hat{x}_0,t)\right\|+S^T(y_e)\sigma_2\hat{B}_1\phi(u(t))\right]-k(\rho-\hat{\rho})\|S(y_e)\|\\
&\le k\|S(y_e)\|\left[\|e(t)\|+\left\|f(T^{-1}\hat{x},t)-f(T^{-1}\hat{x}_0,t)\right\|\right]+S^T(y_e)\sigma_2\hat{B}_1\phi(u(t))]-k(\rho-\hat{\rho})\|S(y_e)\|
\end{aligned}$$

(ب-۲)

داریم:

$$u(t)\phi(u(t))=-\gamma k\hat{\rho}(t)\frac{S^T(y_e)\sigma_2B_1}{\left\|B_1{}^T\sigma_2{}^TS(y_e)\right\|}\phi(u(t))\ge\beta_1\gamma^2\hat{\rho}^2(t)\frac{(S^T(y_e)\sigma_2B_1)(B_1{}^T\sigma_2{}^TS(y_e))}{\left\|B_1{}^T\sigma_2{}^TS(y_e)\right\|^2} \qquad (ب-۳)$$

با استفاده از رابطه

$$(S^T(y_e)\sigma_2B_1)(B_1{}^T\sigma_2{}^TS(y_e))=\left\|B_1{}^T\sigma_2{}^TS(y_e)\right\|^2$$

$$\begin{aligned}
&-\frac{S^T(y_e)\sigma_2B_1}{\left\|B_1{}^T\sigma_2{}^TS(y_e)\right\|}\phi(u(t))\ge\beta_1\gamma k\hat{\rho}(t)\\
&\Rightarrow S^T(y_e)\sigma_2B_1\phi(u(t))\\
&\le\beta_1\gamma k\hat{\rho}(t)\left\|B_1{}^T\sigma_2{}^TS(y_e)\right\|
\end{aligned} \qquad (ب-۴)$$

همواره ثابت مثبت و نامشخص $\rho$ وجود دارد که رابطه زیر را برآورده می‌کند:

$$\|e(t)\| + \|(f(T^{-1}\hat{x},t) - f(T^{-1}\hat{x}_0,t))\| \le \rho < \infty \quad \forall t\ ,0 < t < \infty \qquad (ب-۵)$$

$$\begin{aligned}
&\dot{V}(t) \le \beta_1 \gamma k\hat{\rho}(t)\|B_1{}^T \sigma_2{}^T S(y_e)\| + k\hat{\rho}\|S(y_e)\| \\
&= -\beta_1 \gamma k\hat{\rho}(t)\|B_1{}^T \sigma_2{}^T S(y_e)\| + k\|(B_1{}^T \sigma_2{}^T)^{-1}(B_1{}^T \sigma_2{}^T)S(y_e)\|\hat{\rho}(t) \qquad (ب-۶) \\
&= \{\|(B_1{}^T \sigma_2{}^T)^{-1}\| - \gamma\beta_1\} \times k\hat{\rho}(t)\|(B_1{}^T \sigma_2{}^T)S(y_e)\|
\end{aligned}$$

هنگامی که $\gamma > \dfrac{\|(B_1{}^T \sigma_2{}^T)^{-1}\|}{\beta_1}$ و $k > 0$، $\hat{\rho}(t) > 0$

بنابراین $\dot{V}(t) \le 0$ حاصل خواهد شد و این اثبات کامل می‌شود.

# مراجع


[۱] C. Sparrow, *The Lorenz equations: bifurcations, chaos, and strange attractors* vol. 41: Springer-Verlag New York, 1982.

[۲] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Physical review letters,* vol. 64, p. 1196, 1990.

[۳] K. M. Cuomo and A .V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Physical review letters,* vol. 71, pp. 65-68, 1993.

[۴] L. Jui-Sheng, Y. Jun-Juh, H. Meei-Ling, T. Jiong-He, Z.-J. Pei-Zhi, and L. Teh-Lu, "Robust synchronization for a class of chaotic systems via quasi sliding mode control," in *Fluid Power and Mechatronics (FPM), 2011 International Conference on*, 2011, pp. 893-897.

[۵] J. L. Mata-Machuca, R. Martínez-Guerra, R. Aguilar-López, and C. Aguilar-Ibañez, "A chaotic system in synchronization and secure communications," *Communications in Nonlinear Science and Numerical Simulation,* vol. 17, pp. 1706-1713, 2012.

[۶] D. Wei, C. Guangzhao, W. Zhenjun, and F. Jie, "Synchronization of a class of hyper-haotic systems with multivariable Transmission Using Observer," in *Intelligent System and Knowledge Engineering, 2008. ISKE 2008. 3rd International Conference on*, 2008, pp. 215-219.

[۷] J.-S. Lin, J.-J. Yan, and T.-L. Liao, "Chaotic synchronization via adaptive sliding mode observers subject to input nonlinearity," *Chaos, Solitons & Fractals,* vol. 24, pp. 371-381, 2005.

[۸] M. R. Akella and K. Subbarao, "A novel parameter projection mechanism for smooth and stable adaptive control," *Systems & control letters,* vol. 54, pp.۲۰۰۵ ,۵۱-۴۳ .

[۹] A. El-Gohary, "Optimal synchronization of Rössler system with complete uncertain parameters," *Chaos, Solitons & Fractals,* vol. 27, pp. 345-355, 2006.

[۱۰] T. Yang and L. Chua, "Secure communication via chaotic parameter modulation," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on,* vol. 43, pp. 817-819, 1996.

[۱۱] C.-J. Cheng, S.-T. Feng, and C.-K. Wang, "An image encryption algorithm based on adaptive synchronization between two different chaotic systems ",in *2010 International Conference on Electronics and Information Engineering*, 2010.

[۱۲] S. Banerjee, M. Mitra, and L. Rondoni, *Applications of chaos and nonlinear dynamics in engineering* vol. 1: Springer, 2011.

[۱۳] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences,* vol. 20, pp. 130-141, 1963.

[۱۴] G. L. Baker, *Chaotic dynamics: an introduction*: Cambridge University Press, 1996.

[۱۵] E. Campos-Cantón, R. Femat, and A. Pisarchik, "A family of multimodal dynamic maps," *Communications in Nonlinear Science and Numerical Simulation,* vol. 16, pp. 3457-3462, 2011.

[۱۶] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical review letters,* vol. 64, p. 821, 1990.

[۱۷] H. Nijmeijer, I. Blekhman, A. Fradkov ,and A. Y. Pogromsky, "Self-synchronization and controlled synchronization," 1997.

[۱۸] M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," *Chaos, Solitons & Fractals,* vol. 18, pp. 141-148, 2003.

[۱۹] M. Chen, D. Zhou, and Y. Shang, "A new observer-based synchronization scheme for private communication," *Chaos, Solitons & Fractals,* vol. 24, pp. 1025-1030, 2005.

[۲۰] A. Alasty and R. Shabani, "Chaotic motions and fractal basin boundaries in spring-pendulum system," *Nonlinear analysis: real world applications,* vol. 7, pp. 81-95, 2006.

[۲۱] O. Diallo and Y. Koné, "Melnikov analysis of chaos in a general epidemiological model," *Nonlinear Analysis: Real World Applications*, vol. 8, pp. 20-26, 2007.
[۲۲] S. Boccaletti, C. Grebogi, Y.-C. Lai, H. Mancini, and D. Maza, "The control of chaos: theory and applications," *Physics reports*, vol. 329, pp. 103-197, 2000.
[۲۳] J. Lü, G. Chen, D. Cheng, and S. Celikovsky, "Bridge the gap between the Lorenz system and the Chen system," *International Journal of Bifurcation and Chaos*, vol. 12, pp. 2917-2926, 2002.
[۲۴] D. Li, J.-a. Lu, X. Wu, and G. Chen, "Estimating the bounds for the Lorenz family of chaotic systems," *Chaos, Solitons & Fractals*, vol. 23, pp. 529-534, 2005.
[۲۵] O. Rossler, "An equation for hyperchaos," *Physics Letters A*, vol. 71, pp. 155-157, 1979.
[۲۶] K.-C. Hsu, "Sliding mode controllers for uncertain systems with input nonlinearities," *Journal of guidance, control, and dynamics*, vol. 21, pp. 666-669, 1998.
[۲۷] J. J. Yan" ,Sliding mode control design for uncertain time-delay systems subjected to a class of nonlinear inputs," *International Journal of Robust and Nonlinear Control*, vol. 13, pp. 519-532, 2003.
[۲۸] S. H. Zak and S. Hui, "On variable structure output feedback controllers for uncertain dynamic systems," *IEEE Transactions on Automatic Control*, vol. 38, pp. 1509-1512, 1993.
[۲۹] S. Hui and S. H. Żak, "Low-order state estimators and compensators for dynamical systems with unknown inputs," *Systems & control letters* ,vol. 21, pp. 493-502, 1993.
[۳۰] J. Peng, E. Ding, M.-z. Ding, and W. Yang, "Synchronizing hyperchaos with a scalar transmitted signal," *Physical Review Letters*, vol. 76, p. 904, 1996.
[۳۱] P. Ioannou and J. Sun, "Stable and robust adaptive control," *Englewood Cliffs, NJ: Printice Hall*, vol. 2, 1995.
[۳۲] K. S. Narendra and A. M. Annaswamy, *Stable adaptive systems*: Courier Dover Publications, 2012.
[۳۳] R. Bakker and A. Annaswamy, "Stability and robustness properties of a simple adaptive controller," *Automatic Control, IEEE Transactions on*, vol. 41, pp. 1352-1358, 1996.
[۳۴] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *Circuits and systems II: Analog and digital signal processing, IEEE Transactions on*, vol. 40, pp. 634-642, 1993.
[۳۵] L. O. Chua, T. Yang, G.-Q. Zhong, and C. W. Wu, "Adaptive synchronization of Chua's oscillators," *International Journal of Bifurcation and Chaos*, vol. 6, pp. 189-201.۱۹۹۶ ,
[۳۶] K. M. Short, "Unmasking a modulated chaotic communications scheme," *International Journal of Bifurcation and Chaos*, vol. 6, pp. 367-375, 1996.
[۳۷] T. Yang, "Recovery of digital signals from chaotic switching," *International Journal of Circuit Theory and Applications*, vol. 23, pp. 611-615, 1995.
[۳۸] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *International Journal of Bifurcation and Chaos*, vol. 3, pp. 1619-1627, 199.۳
[۳۹] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 44, pp. 469-472, 1997.
[۴۰] X. Yang, Z. Yang, and X. Nie, "Exponential synchronization of discontinuous chaotic systems via delayed impulsive control and its application to secure communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 1529-1543, 2014.
[۴۱] H. Xi, S. Yu, R. Zhang, and L. Xu, "Adaptive impulsive synchronization for a class of fractional-order chaotic and hyperchaotic systems," *Optik-International Journal for Light and Electron Optics*, vol. 125, pp. 2036-2040, 2014.
[۴۲] T. Yang, *Impulsive systems and control: theory and applications*: Nova Science Publishers, Inc., 2001.

[٤٣] A. T. Al-Taani and A. M. Al-Issa, "A Novel Steganographic Method for Gray-Level Images," *International Journal of Computer, Information & Systems Science & Engineering*, vol. 3, 2009.

# Abstract

In this thesis a novel picture steganography method using multimodal chaotic maps for improvement of chaotic secure communication is presented. Stego image is sent by modulating parameters of the transmitter. The presented method includes a receiver system for asymptotic convergence as well as estimating uncertain parameters of rossler system. The gain of the receiver system changes continuously by a high order sliding mode adaptive controller (HOSMAC), so that system output errors converges to zero. Convergence analysis is accomplished using Barbalat's lemma. The converged parameters are used to determine the map set that is considered. After deciding map set, Gray level modification for hiding the message is selected and the stego image is produced. Using the synchronization and chaotic modulation method, the proposed method is studied in the field of secure communications.

***Keywords— secure communication; chaotic synchronization; multimodal chaotic maps; steganography; gray level modification***

Shahrood University of Technology

Faculty of electrical and robotic engeenering

# Improvement of chaotic secure communication systems

**Masoud Khodadadzadeh**

Supervisore:

**Hosein Gholizadeh**

**2014**