



ТЕХНИЧЕСКИ УНИВЕРСИТЕТ-ГАБРОВО

Факултет „Електротехника и електроника”

маг. инж. Христина Светославова Стойчева

СИНТЕЗ И АНАЛИЗ НА ХАОТИЧНИ СИНХРОНИЗАЦИОННИ СИСТЕМИ

А В Т О Р Е Ф Е Р А Т

на дисертация

за придобиване на образователна и научна степен „доктор”

Област на висше образование: 5. Технически науки

Професионално направление: 5.2. Електротехника,
електроника и автоматика

Докторска програма: Автоматизирани системи за обработка
на информация и управление

Научен ръководител: доц. д-р инж. Драгомир Пенков Чантов

Рецензенти: проф. д-р инж. Чавдар Иванов Дамянов
проф. д-р инж. Коста Петров Бошнаков

Габрово, 2021 г.

Дисертационният труд е обсъден и насочен за официална защита на заседание на Разширен катедрен съвет на катедра „АИУТ” към факултет „ЕЕ” на Технически университет – Габрово, проведен на 29 Април 2021 г.

Дисертационният труд съдържа 209 страници. Научното съдържание е представено в въведение, 5 глави, заключение и 1 приложение, включва 153 фигури, 239 формули и 13 таблици. Цитирани са 401 литературни източника. Фигурите, таблиците и формулите в автореферата са в съответствие с тези в дисертацията.

Разработката и изследванията по дисертационния труд са извършени в катедра „АИУТ” към факултет „ЕЕ” на Технически университет – Габрово.

Официалната защита на дисертационния труд ще се състои на г. от ч. в зала на Технически университет – Габрово.

Автор: Христина Светославова Стойчева
Заглавие: Синтез и анализ на хаотични синхронизационни системи

Тираж: 20 бр.
Място на отпечатване: Печатна база при ТУ-Габрово

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Настоящата дисертация е посветена на анализа и синтеза на хаотични синхронизационни схеми. Синхронизацията на хаотични системи се прилага при задачи, за които сложното динамично поведение на една система е предимство и целта е две или повече хаотични системи да настроят динамиката си една към друга посредством подходящо синтезирано управление между тях. Въпреки значителният брой публикации и бързото развитие на областта на хаотичната синхронизация, остават много неизследвани закономерности и проблеми, като основният от тях е липсата на универсален подход за постигане на синхронизация, което предоставя възможности за нови научни изследвания. Това предоставя благодатна възможност за научна и приложна работа, и е причината авторът да избере именно тази тематика.

Хаотичната синхронизация представлява възпроизвеждане от подчинената система на състоянието на управляващата на базата на информацията, получена чрез свързващия (управляващия, синхронизиращия) сигнал. Основна задача при проектирането на хаотични синхронизационни системи е синтезирането на подходящ свързващ сигнал, който ще гарантира възможността за такова възпроизвеждане. Комбинацията от синхронизация и непредсказуемост води до интересни приложения в областта на защита на информацията. Разработването и реализирането на схеми за криптиране на конфиденциална информация, чрез използване на хаотичен сигнал и последващото му декодиране, след осъществяване на процес на синхронизация, повишава степента на защита неимоверно, като на практика прави невъзможно извличането на информацията от предавания сигнал.

Цел и задачи на дисертационния труд

Основната цел на настоящия дисертационен труд е разработване и изследване на нови методики, които да превъзможнат недостатъците на съществуващите такива, доразвиване и комбиниране на съществуващи методи с цел постигане на специфични видове синхронизация, чрез синтез на по-сложни синхронизационни схеми, както и да се изследват възможностите за тяхното приложение (в защитено предаване на информация). За постигане на така поставената цел, освен класификации на известните хаотични системи, видовете и методите за тяхната синхронизация е необходимо решаването на следните основни задачи:

1. Разработка на нова методика за постигане на синхронизация между хаотични системи, която да предоставя високо ниво на защита на информацията. Следователно, разработената методика ще трябва:
 - да синтезира сложно управление, водещо до устойчива хаотична синхронизация;
 - да се базира на вторият метод за устойчивост на Ляпунов, за да има необходимо и достатъчно условие за устойчивост;
 - да се изследва, чрез реализиране на синхронизационни схеми с различни хаотични и хиперхатични системи;
 - да осигурява достатъчно кратки преходни процеси, с цел по-широко приложение в областта на защитените комуникации.
2. Разработка на нов метод за постигане на специфични видове неидентична синхронизация между хаотични системи, който да преодолява някои от недостатъците на известните синхронизационни методи. В тази връзка е необходимо да се формулира такъв подход за синхронизация, който:

- предлага лесна и точна форма за изследване на устойчивостта на синхронизацията;
 - дава възможност за постигане на сложни типове синхронизация;
 - има по-голямо бързодействие в сравнение със съществуващите;
 - е приложим за широк набор от хаотични и хиперхаотични системи.
3. Анализ за приложимостта на предложените подходи за реализиране на защитени комуникации системи за предаване на аналогови и цифрови сигнали и за реализиране на алгоритми за криптиране на изображения.

Методи на изследване

При решаването на поставените задачи са използвани основно методи от теория на нелинейните системи, теория на хаоса, теория на управлението. Използвани са методи, похвати и алгоритми за обработка на сигнали и изображения (методи за филтриране, модулиране, аритметични и логически операции, хистограми, фазови портрети, криви на предпочитанията и др.). Разработката се базира на множество математически и теоретични анализи, симулационни и експериментални изследвания които са направени в среда на MATLAB/Simulink.

Научна новост

Във връзка с разработването на поставените задачи, новите резултати, получени в дисертацията се обобщават както следва:

1. Разработена е методика за постигане на специфичен комбиниран вид синхронизация, базирана на вторият метод за устойчивост на Ляпунов, съчетаваща три базови типа синхронизация, а именно мащабирана, хибридна и изместена, което води до синтезиране на значително по-сложно управление към подчинената система;
2. Предложен е метод за хаотична синхронизация осигуряващ специфични видове неидентично синхронно поведение, базирайки се на модификация на метода на линейно-нелинейната декомпозиция, като посредством прилагането на допълнителното управление към подчинената система, се гарантира постигането на повече от един вид хаотична синхронизация при един и същи синтез на връзка между подлежащите на синхронизация системи;
3. Направена е класификация на известните хаотични системи, която може да служи като база при конкретни задачи, най-вече в областта на синхронизацията на хаотични системи;
4. Разработена е комуникационна схема за защитено предаване на цифров сигнал, посредством хаотично превключване, използваща синхронизационна схема базирана на методиката за получаване на комбиниран вид синхронизация;
5. Предложена е нова архитектура на хаотично маскиране в комуникационна схема за защитено предаване на аналогов сигнал, посредством синхронизационна схема базирана на методиката за получаване на комбиниран вид синхронизация;
6. Разработена е комуникационна схема за защитено предаване на цифров сигнал, посредством хаотично модулиране, използваща синхронизационна схема базирана на методиката за получаване на комбиниран вид синхронизация;
7. Модифициран е алгоритъм за кодиране на изображения базиран на фрактални функции, чрез използване на сигнал от хаотична система във фракталния модул на алгоритъма в предавателя;
8. Модифициран е алгоритъм за кодиране на изображения базиран на генериране на дифузионна матрица, чрез използване на хаотичен сигнал за генериране на изображение и в последващите операции по реализиране на кодирането;

9. Предложена е нова архитектура на стандартен ОТР алгоритъм за кодиране на изображения, базирана на модификация на алгоритъма, чрез генериране на допълнителен хаотичен (динамичен) ключ.

Приложимост

Практическият ефект от направените изследвания се състои във възможността получените резултати да се използват в реализацията на различни комуникационни системи с цел защита на информацията. Предлаганите методи и методики за постигане на хаотична синхронизация предоставят по-голям набор от възможности за реализиране на връзката между приемника и предавателя, за разлика от известните вече такива. Постиганото качество на синхронизация дава възможност за използване на много повече алгоритми и схемни реализации за кодиране на информация.

Разработените комуникационни схеми за кодиране на аналогови и цифрови сигнали се характеризират с много по-голяма степен на защита, благодарение на предложения в Глава 3 комбиниран вид синхронизация.

Модифицираните алгоритми за кодиране на изображения, предоставят много по-голяма гъвкавост в избора на синхронизационна схема, повишават степента на защита и запазват качеството на декодираното изображение. Това са дължи на предложения в Глава 4 метод, осигуряващ специфични видове неидентично синхронно поведение на хаотични и хиперхаотични системи.

Апробация на дисертационния труд

Дисертационната работа е докладвана и обсъждана на разширен катедрен съвет на катедра „Автоматика информационна и управляваща техника” при Технически университет - Габрово. Основните резултати от дисертацията са докладвани на следните научни форуми:

- International Conference on Engineering, Technologies and Systems TECHSYS 2015, Plovdiv;
- Международна научна конференция UNITECH 2016, 2017, 2019, Габрово;
- Международна конференция Автоматика и информатика, 2019, София ;
- International conference Automatics and informatics, 2020, Varna;
- International Scientific conference “Artificial intelligence and E-leadership”, 2019, Plovdiv;
- Международна конференция Автоматика’ 2017, Созопол;
- Известие на Технически университет – Габрово, 2018;
- Годишник на Технически университет – София, 2017.

Структура и обем на дисертационния труд

Дисертационният труд е с обем 219 страници. Структуриран е във въведение, пет глави, заключение и 1 приложение. Включва 153 фигури и графики, 13 таблици и 265 формули. Библиографията съдържа 401 заглавия на публикации, от които 6 на кирилица и 395 на латиница. Номерацията на фигурите, таблиците, формулите и цитираната литература съответства на тази в дисертационния труд.

Глава I: Теоретични основи на хаотичните системи

1.1 Основни понятия от теория на нелинейните системи

В общият смисъл на думата „хаос“ се разбира безпорядък, безредие. В съвременната научна терминология, към понятието „хаос“ се отнася псевдо-случаен феномен, генериран в детерминирана нелинейна система. Не съществува всеобхватно определение за понятието хаос. В теория на хаоса е общоприета следната дефиниция: *Хаосът е продължително аperiодично поведение в една детерминирана система, проявяваща чувствителна зависимост към началните условия.*

При анализа на хаотичните системи, се използват няколко похвати, които дефинират нови понятия в теория на нелинейните системи като:

- Атрактор - траектории, възникващи с ненулева вероятност при случайно избрани начални условия, които с нарастване на времето не се установяват в точка, граничен цикъл или квазипериодично движение.
- Равновесни точки - точките, в които системата се намира в покой.
- Бифуркация - Бифуркация настъпва тогава, когато при промяна на един или няколко системни параметъра, се измени характера на движение на самата система.
- Фрактал - геометрична структура и модел на детерминистичния хаос, която определя количествените и качествени показатели на хаотичния атрактор.

1.2 Методи за доказване хаотичността на една нелинейна система

Присъствието на хаотични колебания в една нелинейна система може да се определи еднозначно, като за целта е необходимо първо да се докаже, че в системата има хаос. Тъй като при много системи е трудно да се разграничи хаотично поведение от квазипериодично от по-висок период е препоръчително, при изследване на една хаотична система, да бъдат приложени на поне два различни метода за доказване на нейната хаотичност. За целта се прилагат някои класически или специфични за теорията на хаоса методи за количествена или качествена оценка на поведението на системата [399,37].

Основните количествени оценки на хаотичните системи са *дисипативност*, *показател на Ляпунов* и *фрактална размерност*.

Качествените методи за оценка на хаоса носят в най-общ вид информация за съществени свойства на динамиката на нелинейните системи. Основните качествени методи са: *времева еволюция на системата*, *чувствителност към начални условия*, *еволюция на системата в пространство на състоянието*, *метод на псевдофазовото пространство*, *честотен спектър*, *сечение на Поанкаре* и др.

1.3 Видове и класификация на хаотичните системи

Известни са стотици непрекъснати хаотични системи. Някои от тях са математични модели на реални обекти от практиката, докато други са само абстрактни математически модели и нямат пряк физически смисъл. Част от тези системи, като системите на Lorenz, Rossler и Chua, са основополагащи и се цитират в хиляди научни публикации, като върху тях се прилагат редица методи за управление и синхронизация на хаотични системи. През последните 10 години броят новооткрити хаотични и хиперхаотични системи расте лавинообразно.

В дисертацията е направен опит да се направи класификация и систематизиране на голяма част от известните непрекъснати хаотични системи. Такава класификация няма как да бъде пълна тъй като непрекъснато се откриват нови хаотични системи. Класификацията обхваща голям брой известни непрекъснати хаотични системи, като по-голямата част от тях са открити след 2010 г. Представените системи се явяват фундаментални модели на

хаотични системи, като те и техните разновидности са широко използвани в редица задачи свързани с теория на хаоса. Системите са разделени според:

- Редът на системата – системи от трети, четвърти и по-висок ред;
- Физическа природа на системата – абстрактни модели или модели на реални обекти и процеси;
- Характера на системата – хаотична или хиперхаотична.

От направената класификация се вижда, че най-голям е броят на системите от трети ред, като от тях преобладават абстрактните математични модели. От реалните системи на първо място преобладават модели на електронни системи, механични системи и системи описващи динамиката на флуиди. Тъй като хаос възниква при относително по-прости системи от нисък ред, логично броя на системите от четвърти и по-висок ред е малък. За сметка на това хиперхаос възниква именно при тези системи, което ги прави по-търсени при реализирането на модули за защита на информацията с висока степен на защита.

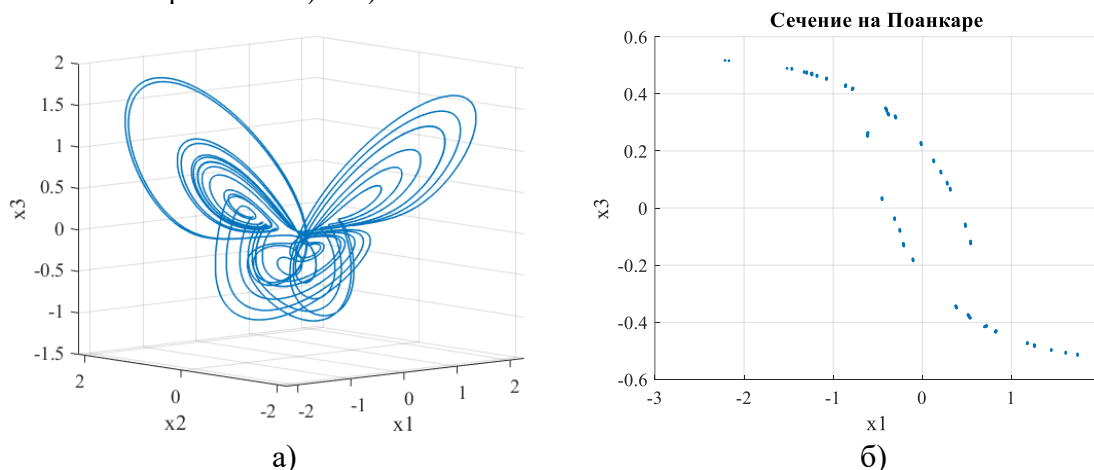
Представените хаотични системи са представени с набора си от диференциални уравнения, графики на атрактора или проекции на атрактора и фигура за сечение на Поанкаре, при зададени определени начални условия. Дадени са и стойности на параметрите, при които системата проявява хаотично поведение.

1.4 Пример за хаотична система - Система на Wang

Моделът на Wang [337] е хаотичната система от трети ред, която се представя чрез следните уравнения:

$$\begin{aligned} \dot{x}_1 &= ax_1 + x_2x_3 \\ \dot{x}_2 &= -bx_1 - cx_2 - x_1x_3 \\ \dot{x}_3 &= -dx_3 - x_1x_2 \end{aligned} \quad (1.5.5)$$

Изменяйки стойностите на параметрите, динамичното поведение на системата се изменя между състояние на хаос и периодичност. За стойности на параметрите $a = 0.2$, $b = 0.01$, $c = 0.4$ и $d = 1$ системата на Wang има хаотичен характер. Полученият, при произволно избрани начални условия $x_0 = [1 \ 0 \ 0]^T$, хаотичен атрактор и неговото сечение на Поанкаре, успоредно на равнината (x_1, x_3) за $x_2 = 0.6$, са показани в пространството на състоянието на фиг. 1.18 а) и б).



Фиг. 1.18 Хаотичен атрактор и сечение на Поанкаре на системата на Wang

Анализи и изводи към Глава I

В настоящата глава са представени общите характеристики на нелинейните динамични системи и е описана появата на хаос. Представени са основните понятия в теория на хаоса, както и методите за неговата количествена и качествена оценка. Представена е класификация на фундаменталните хаотични системи и на по-известните

нови модели според размерността на техния математичен модел, като системите от трети ред са разделени на реални и абстрактни математични модели. Тази класификация може да служи като база при конкретни практически задачи, особено в областта на синхронизацията на хаотичните системи.

Глава II: Синхронизация на хаотични системи

В глава 2 се разглежда по-подробно задачата за синхронизация на хаотични системи. Тъй като една от основните цели на дисертацията е синтезиране и анализиране на хаотични синхронизационни схеми, е необходимо да се класифицират известните до момента видове и методи за синхронизация, за да се направи анализ и обосновка на необходимостта от търсене на нови възможности за постигане на хаотична синхронизация.

2.1 Общи определения и термини за хаотична синхронизация

Под понятието синхронизация на хаотични системи се разбират процеси, при които две или повече хаотични системи приспособяват динамиката си една към друга.

За да се постигне хаотична синхронизация между две или повече хаотични системи, еквивалентни или не по структура и/или параметри, е необходимо между тях да има връзка. Връзката може да бъде взаимна (двупосочна) или както в преобладаващата част от задачите за хаотична синхронизация – еднопосочна. Прието е при конфигурация с еднопосочна връзка системата, която осигурява свързващия сигнал, да се нарича управляваща (Master) система, а системата, към която се подава този сигнал – управлявана или подчинена (Slave) система. Хаотичната синхронизация представлява възпроизвеждане от подчинената система на състоянието на управляващата на базата на информацията, получена чрез свързващия (управляващия, синхронизиращия) сигнал. Основна задача при проектирането на хаотични синхронизационни системи е синтезирането на подходящ свързващ сигнал, който ще гарантира възможността за такова възпроизвеждане.

Тъй като настоящата работа се фокусира върху синхронизацията между *непрекъснати* хаотични системи, са представени основните дефиниции за непрекъснати системи.

Разглеждат се две еднопосочно свързани хаотични системи:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, t), \quad (2.1.1)$$

$$\dot{\tilde{\mathbf{x}}} = \tilde{\mathbf{f}}(\tilde{\mathbf{x}}, \mathbf{x}, t), \quad (2.1.2)$$

със съответните решения: $\mathbf{x}(t, t_0, \mathbf{x}(t_0))$ и $\tilde{\mathbf{x}}(t, t_0, \tilde{\mathbf{x}}(t_0))$, където $\mathbf{x} \in \mathcal{R}^{n_1}$, $\tilde{\mathbf{x}} \in \mathcal{R}^{n_2}$, а началните условия на двете системи са: $\mathbf{x}(t_0)$ и $\tilde{\mathbf{x}}(t_0)$. За $n_1 = n_2$ и $\tilde{\mathbf{f}}(\tilde{\mathbf{x}}) = \mathbf{f}(\mathbf{x})$ системите (2.1.1) и (2.1.2) са *идентични*. Решенията $\mathbf{x}(t, t_0, \mathbf{x}(t_0))$ и $\tilde{\mathbf{x}}(t, t_0, \tilde{\mathbf{x}}(t_0))$ на двете системи с начални условия:

$$\mathbf{x}(t_0) \neq \tilde{\mathbf{x}}(t_0) \quad (2.1.3)$$

са *синхронизирани* по отношение на даден функционал най-общо от вида:

$$Q_t = Q_t[\mathbf{x}(t), \tilde{\mathbf{x}}(t)], \quad (2.1.4)$$

ако функционалът:

$$Q_t \equiv 0, \quad \forall t > 0. \quad (2.1.5)$$

Решенията $\mathbf{x}(t, t_0, \mathbf{x}(t_0))$ и $\tilde{\mathbf{x}}(t, t_0, \tilde{\mathbf{x}}(t_0))$ на двете системи са *асимптотически синхронизирани* по отношение на функционала (2.1.4), ако:

$$\lim_{t \rightarrow \infty} Q_t = 0. \quad (2.1.6)$$

Ако системите (2.1.1) и (2.1.2) са идентични по структура, те могат да се запишат във вида:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{p}_1, t), \quad (2.1.7)$$

$$\dot{\tilde{\mathbf{x}}} = \mathbf{f}(\tilde{\mathbf{x}}, \mathbf{x}, \mathbf{p}_2, t), \quad (2.1.8)$$

където \mathbf{p}_1 и \mathbf{p}_2 са векторите от параметрите на двете системи. При задачите за *идентична синхронизация* се предполага, че параметрите на двете системи са еднакви:

$$\mathbf{p}_1 \cong \mathbf{p}_2 = \mathbf{p}. \quad (2.1.9)$$

При идентичните по структура и параметри системи (2.1.1) и (2.1.2) функционалът (2.1.4) най-често се избира от вида:

$$Q_t = \|\mathbf{e}(t)\|, \quad (2.1.10)$$

където $\mathbf{e}(t)$ е разсъгласуването или “грешката” между двете системи:

$$\mathbf{e}(t) = \mathbf{x}(t, t_0, \mathbf{x}(t_0), \mathbf{p}) - \tilde{\mathbf{x}}(t, t_0, \tilde{\mathbf{x}}(t_0), \mathbf{p}). \quad (2.1.11)$$

В този случай се казва, че системите (2.1.7) и (2.1.8), при спазване на (2.1.9), са *идентично синхронизирани*, ако за подобластта на началните условия $\Omega \in \mathfrak{R}^n$, за която $\mathbf{x}(t_0) \in \Omega$ и $\tilde{\mathbf{x}}(t_0) \in \Omega$, се изпълнява:

$$\lim_{t \rightarrow \infty} \mathbf{e}(t) = 0. \quad (2.1.12)$$

2.2 Доказване на синхронизацията

Разглеждайки стандартния процес на синхронизация, движението на двете свързани системи се наблюдава в обобщено пространство на състоянието с размерност $2n$ или $2n-1$ в зависимост от избрания метод за синхронизация, където n е редът на Master системата. Ако целта е да се постигне идентична синхронизация, траекторията на системата ще остане в равнините $x_i = \tilde{x}_i, i = 1, \dots, n$. Тези равенства определят съществуването на т.н. *хиперравнина на синхронизация (synchronization manifold)* в пространството на състоянието [251]. Между Master и Slave системите е постигната идентична синхронизация ако движението на обобщената система с размерност $2n$ или $2n-1$ се ограничава в такава хиперравнина.

За запазването на синхронизираното поведение на двете системи е от съществено значение устойчивостта на хиперравнината на синхронизация. При практически задачи за синхронизация свързващият сигнал между двете системи винаги е подложен на смущаващи въздействия, освен това параметрите на двете системи никога не могат да бъдат абсолютно еднакви, така че винаги ще възникват колебания около хиперравнината на синхронизация [358]. Именно поради тази причина, от гледна точка на приложението на явлението хаотична синхронизация, в реални системи е задължително хиперравнината на синхронизация да бъде устойчива.

Тъй като хаотичните системи са клас нелинейни системи, то няма общ подход за оценка на устойчивостта на хиперравнината на синхронизация. Съществуват два основни подхода за оценка на устойчивостта на процеса на хаотична синхронизация – метод с показатели на Ляпунов и метод с функции на Ляпунов.

Изчисляването на показателите на Ляпунов е свързано със значителни трудности, именно затова се търсят методи за тяхната приблизителна оценка. Такъв метод е предложен в [106]. Системата от разсъгласуването може да се запише като:

$$\dot{\mathbf{e}}(t) = \mathbf{f}(\mathbf{x}, t) - \mathbf{f}(\tilde{\mathbf{x}}, \mathbf{x}, t) = \mathbf{f}(\mathbf{e}, \mathbf{x}, t). \quad (2.2.2)$$

Ако за всички траектории в околността на точката $\mathbf{e}(t) = 0$ се изпълнява условието (2.1.12), то синхронизацията е устойчива. В този случай хаотичният атрактор A е *асимптотически устойчив*.

Целта на синхронизацията най-често е $\mathbf{e}(t) \rightarrow 0$, следователно ако линеаризираната в точката $\mathbf{0}$ система (2.2.2) е устойчива, ще бъде устойчива и хиперравнината на синхронизация и двете системи ще се синхронизират напълно. Така наречената напречна линеаризация в околността на атрактора може да се запише в следния вид:

$$\dot{\mathbf{e}}(t) = \mathbf{D}_{\mathbf{x}}(\mathbf{x}(t))|_{\mathbf{e}=0} \mathbf{e}(t), \quad (2.2.5)$$

където $\mathbf{D}_{\mathbf{x}}$ е матрицата на Якоби на \mathbf{f} около траекторията на $\mathbf{x}(t)$. Линеаризацията позволява анализът за устойчивостта на атрактора A да се сведе до задача за изследване на устойчивостта на равновесната точка $\mathbf{e}(t) = 0$ на системата (2.2.5).

Необходимото условие точката $\mathbf{e}(t) = 0$ да е асимптотически устойчива равновесна точка на системата (2.2.5) е всички собствени стойности на якубиана $\mathbf{D}_{\mathbf{x}}$ да са отрицателни, ако са реални, или с отрицателна реална част, ако са комплексни.

Така нареченият втори или директен метод на Ляпунов [7,26] е една от повратните точки в теорията на нелинейните системи, доказала се като неимоверно ползотворен инструмент за анализ на устойчивост на системи. Чрез функциите на Ляпунов може да се изследва и устойчивостта на хиперравнината на синхронизация M . За разлика от първия метод на Ляпунов, този метод дава не само необходимо, но и достатъчно условие за устойчивост. По отношение на изследването на времевата еволюция на грешката от синхронизация $\mathbf{e}(t)$ (2.2.2), може да се дефинира функция на Ляпунов със следните свойства:

$$(1) - V(\mathbf{e}) > 0 \text{ за всяко } \mathbf{e} \neq 0; \quad (2.2.6)$$

$$(2) - V(\mathbf{e}) = 0 \text{ за } \mathbf{e} = 0; \quad (2.2.7)$$

$$(3) - \frac{dV(\mathbf{e})}{dt} < 0 \text{ за всяко } \mathbf{e} \neq 0. \quad (2.2.8)$$

Ако за дадена синхронизационна схема може да се намери такава функция за системата от разсъгласуването $V(\mathbf{e})$, която да отговаря на горните условия, то хиперравнината на синхронизация на тази синхронизационна схема ще бъде устойчива.

2.3 Методи за синхронизация на хаотични системи

През последните три десетилетия са предложени редица методи за синхронизация, като най-общо те могат да бъдат класифицирани по следните признаци:

- Според посоката на свързването - Методи с еднопосочна връзка и методи с двупосочна връзка
- Според линейността на връзката - Методи с линейна връзка и методи с нелинейна връзка
- Според типа на свързващия сигнал - Декомпозиционни методи и методи с обратна връзка

2.3.1 Декомпозиционни методи

2.3.1.1 Метод на Pecora-Carroll

Първият предложен метод за синхронизация на хаотични системи, поставящ началото на този клас задачи за управление на хаотични системи, е методът на Pecora-Carroll (PC или Complete Replacement, CR) [11,251,252]. Изходната хаотична система условно се декомпозира на две части, след което се изгражда идентично копие на едната част, управлявано от променливите от другата част. При този метод изходната хаотична система от вида (2.1.1), която ще играе ролята на Master система, условно се разделя (декомпозира) на две части:

$$\text{Master: } \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \Rightarrow \begin{cases} \dot{\mathbf{x}}_1 = \mathbf{f}_1(\mathbf{x}_1, \mathbf{x}_2), \\ \dot{\mathbf{x}}_2 = \mathbf{f}_2(\mathbf{x}_1, \mathbf{x}_2), \end{cases} \quad (2.3.1)$$

където $\mathbf{x}_1 \in \mathcal{R}^l, \mathbf{x}_2 \in \mathcal{R}^m, m + l = n$. След това се изгражда идентично копие на подсистемата $\dot{\mathbf{x}}_2$, играещо ролята на Slave система, което ще бъде управлявано от променливите на подсистемата $\dot{\mathbf{x}}_1$ от (2.3.1):

$$\text{Slave: } \dot{\mathbf{x}}_2 = \mathbf{f}_2(\mathbf{x}_1, \tilde{\mathbf{x}}_2). \quad (2.3.2)$$

Най-често управляващата променлива е една, тогава изразът (2.3.2) се тълкува по следния начин: управляващата променлива от Master системата замества променливата със същия индекс в Slave системата на всички позиции, където тя се среща.

Останалите декомпозиционни методи които са разгледани са: метод на Pecora-Carroll с тройна декомпозиция, метод на частично заместване, метод на активно-пасивната декомпозиция и метод на произволна декомпозиция.

2.3.2 Методи с обратна връзка

2.3.2.1 Метод с едностранно свързване

При метода на едностранното свързване (One-wayCoupling, OW) [239,251], Master и Slave системите са идентични, като те се свързват посредством допълнителна, в частност линейна връзка:

$$\text{Master: } \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (2.3.15)$$

$$\text{Slave: } \dot{\tilde{\mathbf{x}}} = \mathbf{f}(\tilde{\mathbf{x}}) + \alpha \mathbf{E}(\mathbf{x} - \tilde{\mathbf{x}}), \quad (2.3.16)$$

където α е коефициент на връзката, а \mathbf{E} е квадратна матрица с размерност n (матрица на връзката), която определя линейната комбинация от компонентите на вектора $\mathbf{e}(t)$, които ще бъдат използвани за свързването.

Методът на едностранното свързване може да се раздели на няколко подварианта в зависимост от избора на матрицата \mathbf{E} и коефициента (коефициентите) на връзката:

- 1) Метод на стандартно едностранно свързване.
- 2) Метод на пълна връзка.
- 3) Метод на разменено свързване.
- 4) Метод с двойна връзка.

В т. 2.3 са разгледани и други методи с обратна връзка, които са: метод с двупосочно свързване, обобщен метод с едностранно (двупосочно) свързване, метод с последователно свързване, метод с промяна на параметър, разгледани са и методи на каскадната синхронизация и синхронизация чрез непостоянна връзка.

2.4 Видове хаотична синхронизация

Независимо от избрания метод за синхронизация, между две синхронизирани хаотични системи може да се постигне много по-сложно поведение, различно от идентичната синхронизация.

При демонстриране на различните видове хаотична синхронизация в т.2.4 Master и Slave системите се представят посредством следният обобщен запис:

$$\text{Master: } \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (2.4.1)$$

$$\text{Slave: } \dot{\tilde{\mathbf{x}}} = \mathbf{f}(\tilde{\mathbf{x}}) + \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}), \quad (2.4.2)$$

където $\dot{\mathbf{x}}, \dot{\tilde{\mathbf{x}}} \in \mathcal{R}^n$ са векторите на състоянието на системата, $\mathbf{f}(\mathbf{x})$ и $\mathbf{f}(\tilde{\mathbf{x}})$ са нелинейни функции, а $\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}})$ е управляващ сигнал към системата (2.4.2). Началните условия на системата са различни, т.е. $\mathbf{x}(0) \neq \tilde{\mathbf{x}}(0)$.

В т.2.4 са представени някои от видовете синхронизация:

- Монотонна идентична – функциите на разсъгласуване между управляващата и подчинената системи представляват разлики от съответните променливи на

състоянието и клонят към 0, а подчинената система повтаря динамиката на управляващата;

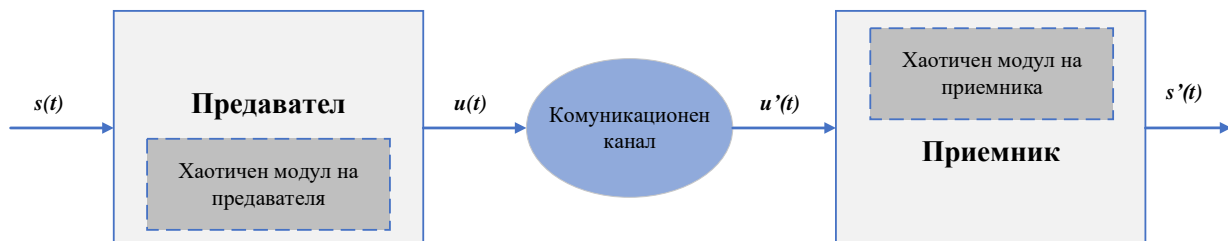
- Антисинхронизация – функциите на разсъгласуване между управляващата и подчинената системи представляват сума от съответните променливи на състоянието и клонят към 0. Динамиката на подчинената система представлява „огледален образ” на динамиката на управляващата;
- Мащабирана синхронизация – разсъгласуването между двете системи клони към 0, но векторите на Master и Slave системите се синхронизират до постоянен мащабиращ фактор α ;
- Хибридна синхронизация – разсъгласуването между двете системи е 0, но изборът кои функции $e_i(t)$ да са суми и кои разлики от съответните променливи на състоянието е произволен;
- Изместена синхронизация – разсъгласуването между двете системи не е нула, а константа;
- Осцилираща синхронизация – разсъгласуването между двете системи е периодична функция;
- Адаптивна синхронизация – не само грешките от разсъгласуването трябва да клонят към нула, а също така и грешките от прогнозираните стойности на параметрите.

Други особени видове хаотична синхронизация са частичната синхронизация, Фазова синхронизация, Обобщена синхронизация, Синхронизация с размита логика, Синхронизация с времезакъснение, Синхронизация на хаотични невронни мрежи и др. [255, 121, 32, 303, 302, 140].

2.5 Приложение на хаотичната синхронизация в защитени комуникации

Приложението на две свързани хаотични системи в схема за защитена комуникация е представено за първи път от Куомо и Опенхайм [64, 65], които изграждат електрическа схема, базирана на уравненията на Лоренц и показват нейните възможности за предаване на малък речеви сигнал.

В най-общ вид една хаотична система за предаване на информация може да бъде представена посредством следната блокова схема.



Фиг. 2.9 Хаотична система за предаване на информация

Информационният сигнал $s(t)$ преминава през предавателната система, включваща в себе си хаотичен модул. Изходният сигнал на предавателя $u(t)$ се предава в средата на комуникационния канал, което го изкривява и на входа на приемника постъпва сигналът $u'(t)$. Приемникът, използвайки специална процедура, извлича информация от сигнала $u'(t)$, и на неговия изход възниква сигналът $s'(t)$, който се явява оценка на изходния информационен сигнал.

Тази обобщена схема включва следните видове комуникационни системи, използващи хаос: схема с хаотично маскиране на информационен сигнал; схема с хаотично превключване; схема с нелинейно смесване на информационния сигнал; схема с двойно нелинейно преобразуване на информационно-хаотичния сигнал; схема, основана на използването на символна динамика в хаотичните системи.

Анализи и изводи към Глава II

В настоящата глава са представени основните методи за синхронизация на хаотични системи. Описани са основните видове хаотична синхронизация, като за повечето от тях са представени графични резултати от синхронизационни схеми, реализирани в среда на Matlab\Simulink.

На база така направеният обзор, могат да се направят следните заключения:

- Най-общо методите за синхронизация се делят на декомпозиционни и такива с обратна връзка;
- Не съществува универсален метод, който да гарантира устойчива синхронизация между хаотични системи;
- Ясно разграничени са основните недостатъци на методите за анализ на устойчивостта на синхронизацията:
 - Методът с показателите на Ляпунов дава само необходимо условие за устойчивост;
 - Методът с линейно-нелинейна декомпозиция дава само достатъчно условие за устойчивост;
 - Методът с функциите на Ляпунов дава необходимо и достатъчно условие за устойчивост, но липсва общ подход за намирането на функция на Ляпунов, който да е приложим за всяка хаотична система;
- Основната област на приложение на хаотичната синхронизация е при реализиране на защитени комуникации;

Базовите видове синхронизация не предоставят достатъчно високо ниво на защита на информацията.

Глава III: Методика за постигане на комбиниран вид синхронизация

3.1 Комбиниран вид синхронизация

При задачите за синхронизация на хаотични системи най-често се синтезира синхронизационна схема между две еднотипни, непрекъснати системи с еднопосочна връзка между тях. При такава конфигурация е прието системата, която осигурява свързващия сигнал, да се нарича управляваща система (3.1.1), а системата, която приема този сигнал и настройва динамиката си - подчинена система (3.1.2). Двете могат да бъдат представени посредством следния обобщен запис:

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}), \quad (3.1.1)$$

$$\dot{\tilde{\mathbf{x}}} = \mathbf{f}(\tilde{\mathbf{x}}) + \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}), \quad (3.1.2)$$

където $\mathbf{x}, \tilde{\mathbf{x}} \in \mathcal{R}^n$ са векторите на състоянието на системата, $\mathbf{f}(\mathbf{x})$ и $\mathbf{f}(\tilde{\mathbf{x}})$ са нелинейни функции, а $\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}})$ е управляващ сигнал към системата (3.1.2). Началните условия на системата са различни, т.е. $\mathbf{x}(0) \neq \tilde{\mathbf{x}}(0)$.

За да се осъществи хибридна синхронизация между системите (3.1.1) и (3.1.2) се търси такова управление $\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}})$, че да бъде изпълнено условието:

$$\lim_{t \rightarrow \infty} e_i(t) = 0, \quad (3.1.3)$$

където за идентична синхронизация, функцията на разсъгласуване между системите $e_i(t)$ има следния вид $e_i(t) = x_i(t) - \tilde{x}_i(t)$, като в резултат подчинената система ще има идентично на управляващата система поведение. При антисинхронизация, подчинената система има поведение - обратно на управляващата система и съответно функцията на разсъгласуване между системите е $e_i(t) = x_i(t) + \tilde{x}_i(t)$.

Функцията на разсъгласуване при хибридна синхронизация, представляваща комбинация от двата метода, има следния вид:

$$e_i(t) = x_i(t) \pm \tilde{x}_i(t). \quad (3.1.4)$$

Съответно вземайки в предвид обобщения запис (3.1.1) и (3.1.2), функцията на разсъгласуване придобива следния вид:

$$\dot{e}_i(t) = \mathbf{f}(\mathbf{x}) \pm \mathbf{f}(\tilde{\mathbf{x}}) \pm \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}) = \mathbf{h}(\mathbf{x}, \tilde{\mathbf{x}}) \pm \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}), \quad (3.1.5)$$

където $\mathbf{h}(\mathbf{x}, \tilde{\mathbf{x}}) = \mathbf{f}(\mathbf{x}) \pm \mathbf{f}(\tilde{\mathbf{x}})$.

При синтезиране на управление на основата на втория метод за устойчивост на Ляпунов, се търси функция $V(\mathbf{e})$, отговаряща на условията:

$$V(\mathbf{e}) > 0 \text{ за всяко } \mathbf{e} \neq 0, \quad (3.1.6)$$

$$V(\mathbf{e}) = 0 \text{ за } \mathbf{e} = 0, \quad (3.1.7)$$

$$\frac{dV(\mathbf{e})}{dt} < 0 \text{ за всяко } \mathbf{e} \neq 0. \quad (3.1.8)$$

Най-често с цел да се изпълнят трите условия избраната функция на Ляпунов е квадратична функция от отделните съставлящи на вектора \mathbf{e} , като изпълнението на третото условие се търси чрез подходящ синтез на управляващите функции към подчинената система $\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}})$.

Нека се избере управляваща функция $\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}})$ от типа:

$$\mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}) = \mathbf{h}(\mathbf{x}, \tilde{\mathbf{x}}) \mp k(e_i), \quad (3.1.9)$$

където първата част $\mathbf{h}(\mathbf{x}, \tilde{\mathbf{x}})$ има за цел да елиминира първата съставляща на системата от разсъгласуването (3.1.5), а втората част да осигури изпълнението на условието (3.1.8).

При така синтезирано двукомпонентно управление (3.1.9), системата от разсъгласуването (3.1.5) ще се стабилизира в точката $e_i = 0$, която съответства на избраната хибридна форма на синхронизация.

Между управляващата (3.1.1) и подчинената 3.1.(2) системи съществува изместена синхронизация тогава, когато се спазва условието:

$$\lim_{t \rightarrow \infty} e_i(t) \rightarrow const \neq 0. \quad (3.1.10)$$

Това условие може да се постигне чрез т.нар. коефициенти на изместване c_i .

При мащабираната синхронизация подчинената система (3.1.2) ще има същото качествено поведение като управляващата система (3.1.1), но атракторите на двете системи ще са с различен мащаб, а понякога и с различна симетрия. За постигане на такъв вид синхронизация е необходимо системата от разсъгласуването да придобие следния вид:

$$\dot{e}_i(t) = \mathbf{f}(\mathbf{x}) \pm \alpha_i \mathbf{f}(\tilde{\mathbf{x}}) \pm \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}), \quad (3.1.11)$$

където α_i са коефициенти на мащабиране. Случаите на идентична, анти- и хибридна синхронизация могат да се разгледат като частен случай на мащабирана синхронизация с коефициент на мащабиране $\alpha_i = 1$.

За постигане на комбинирания метод за синхронизация е необходимо към подчинената система да се прибави не само управляваща функция, а и съответните коефициенти на мащабиране α_i , както и коефициентите на изместване c_i . В този случай системата от разсъгласуването между двете системи придобива следния обобщен вид:

$$\dot{e}_i(t) = \mathbf{f}(\mathbf{x}) \pm \alpha_i \mathbf{f}(\tilde{\mathbf{x}}) \pm \mathbf{u}(\mathbf{x}, \tilde{\mathbf{x}}) + c_i. \quad (3.1.12)$$

Синтезирайки подходящо управление функциите на разсъгласуване ще се установят не в нула, а в константи, които се определят свободно чрез избора на c_i .

3.2 Изследване на представения комбиниран вид синхронизация

Комбинираният вид синхронизация на хаотични системи е тестван върху голяма част от представените в Глава 1 хаотични системи от трети и хиперхаотични системи от четвърти ред. В главата са представени подробно получените резултати за 2 системи от трети ред (Lorenz и Zhou - Li) и една система от четвърти ред (Singh - Roy).

3.2.1 Хаотична система на Lorenz

Синтезирана е хаотична синхронизационна схема с комбиниран вид синхронизация, между две идентични хаотични системи на Lorenz. Подробно са представени резултати за една конкретна комбинация, а резултатите от останалите комбинации са представени в т. 3.2.1.2.

Системата на Лоренц, избрана за основа на метода, е известен математичен модел от трети ред, описван със следните уравнения:

$$\begin{aligned}\dot{x}_1 &= -\sigma x_1 + \sigma x_2, \\ \dot{x}_2 &= -x_1 x_3 + r x_1 - x_2, \\ \dot{x}_3 &= x_1 x_2 - b x_3.\end{aligned}\quad (3.2.1)$$

Оптималните стойности на параметрите, за които в системата възникват хаотични колебания са $\sigma = 10$, $b = \frac{8}{3}$ и $r > 25$.

Нека се синтезира синхронизационна схема от типа (3.1.1), (3.1.2) с управляваща система (3.2.1) и подчинена система:

$$\begin{aligned}\dot{\tilde{x}}_1 &= -\sigma \tilde{x}_1 + \sigma \tilde{x}_2 + u_1, \\ \dot{\tilde{x}}_2 &= -\tilde{x}_1 \tilde{x}_3 + r \tilde{x}_1 - \tilde{x}_2 + u_2, \\ \dot{\tilde{x}}_3 &= \tilde{x}_1 \tilde{x}_2 - b \tilde{x}_3 + u_3.\end{aligned}\quad (3.2.2)$$

3.2.1.1 Изследване на конкретна комбинация

Избират се функции на разсъгласуване, при които първата и третата двойки променливи да бъдат в режим на мащабирана антисинхронизация, а втората – в режим на мащабирана синхронизация. Тогава системата от разсъгласуването \dot{e}_i има следния вид:

$$\begin{aligned}\dot{e}_1 &= \dot{x}_1 + \alpha_1 \dot{\tilde{x}}_1 + c_1, \\ \dot{e}_2 &= \dot{x}_2 - \alpha_2 \dot{\tilde{x}}_2 + c_2, \\ \dot{e}_3 &= \dot{x}_3 + \alpha_3 \dot{\tilde{x}}_3 + c_3.\end{aligned}\quad (3.2.3)$$

При заместване на (3.2.1) и (3.2.2) в (3.2.3) и след няколко прости математически преобразувания се получават следните зависимости:

$$\begin{aligned}\dot{e}_1 &= -10e_1 + 10x_2 + 10\alpha_1 \tilde{x}_2 + \alpha_1 u_1, \\ \dot{e}_2 &= -e_2 - x_1 x_3 + 25x_1 + \alpha_2 \tilde{x}_1 \tilde{x}_3 - 25\alpha_2 \tilde{x}_1 - \alpha_2 u_2, \\ \dot{e}_3 &= x_1 x_2 - \frac{8}{3}e_3 + \alpha_3 \tilde{x}_1 \tilde{x}_2 + \alpha_3 u_3.\end{aligned}\quad (3.2.4)$$

Вземайки в предвид (3.1.12) и (3.2.4) за управляващите функции се получава:

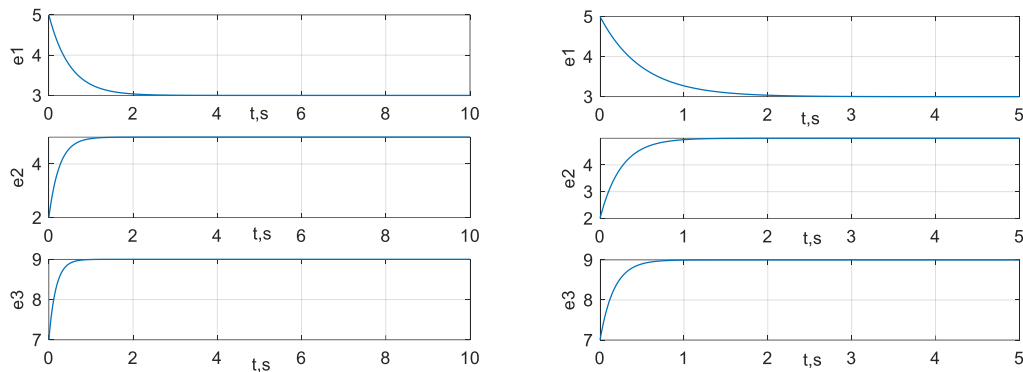
$$\begin{aligned}u_1 &= \frac{10e_1 - 10x_2 - 10\alpha_1 \tilde{x}_2}{\alpha_1} + c_1 - k_1 e_1, \\ u_2 &= \frac{-e_2 - x_1 x_3 + 25x_1 + \alpha_2 \tilde{x}_1 \tilde{x}_3 - 25\alpha_2 \tilde{x}_1}{\alpha_2} - c_2 + k_2 e_2, \\ u_3 &= \frac{-x_1 x_2 + \frac{8}{3}e_3 - \alpha_3 \tilde{x}_1 \tilde{x}_2}{\alpha_3} + c_3 - k_3 e_3.\end{aligned}\quad (3.2.5)$$

При заместване на управляващите функции (3.2.5) в системата от разсъгласуване (3.2.4) се получава запис от вида:

$$\begin{aligned}\dot{e}_1 &= -k_1 e_1, \\ \dot{e}_2 &= -k_2 e_2, \\ \dot{e}_3 &= -k_3 e_3.\end{aligned}\quad (3.2.6)$$

за които, както беше изложено по-горе, при положителни константи k_i се изпълнява условието (3.1.8).

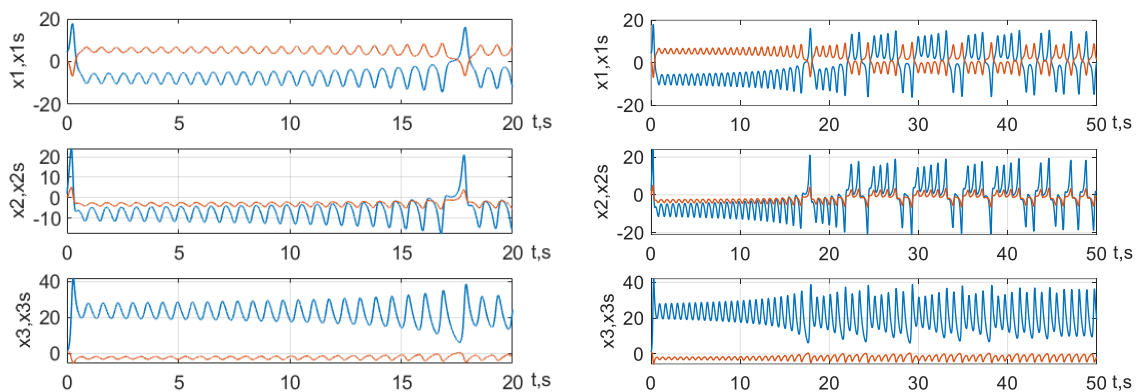
Синхронизационната схема между управляващата система (3.2.1) и подчинената система (3.2.2) с управляващи функции (3.2.5) с коефициенти $k_i = 1, i = 1 \div 3$ е симулирана в среда на Simulink. Графичните интерпретации на синхронизационните процеси са получени в среда на Matlab. Началните условия на управляващата система са $\mathbf{x} = [5 \ 2 \ 1]^T$, а на подчинената система – $\tilde{\mathbf{x}} = [0 \ 0 \ 1]^T$, като и двата набора са избрани произволно. Коефициентите на изместване и мащабиране също са избрани произволно както следва: $\alpha_1 = 2, \alpha_2 = 4, \alpha_3 = 6, c_1 = 3, c_2 = 5$ и $c_3 = 9$.



Фиг. 3.1 Функции на разсъгласуване

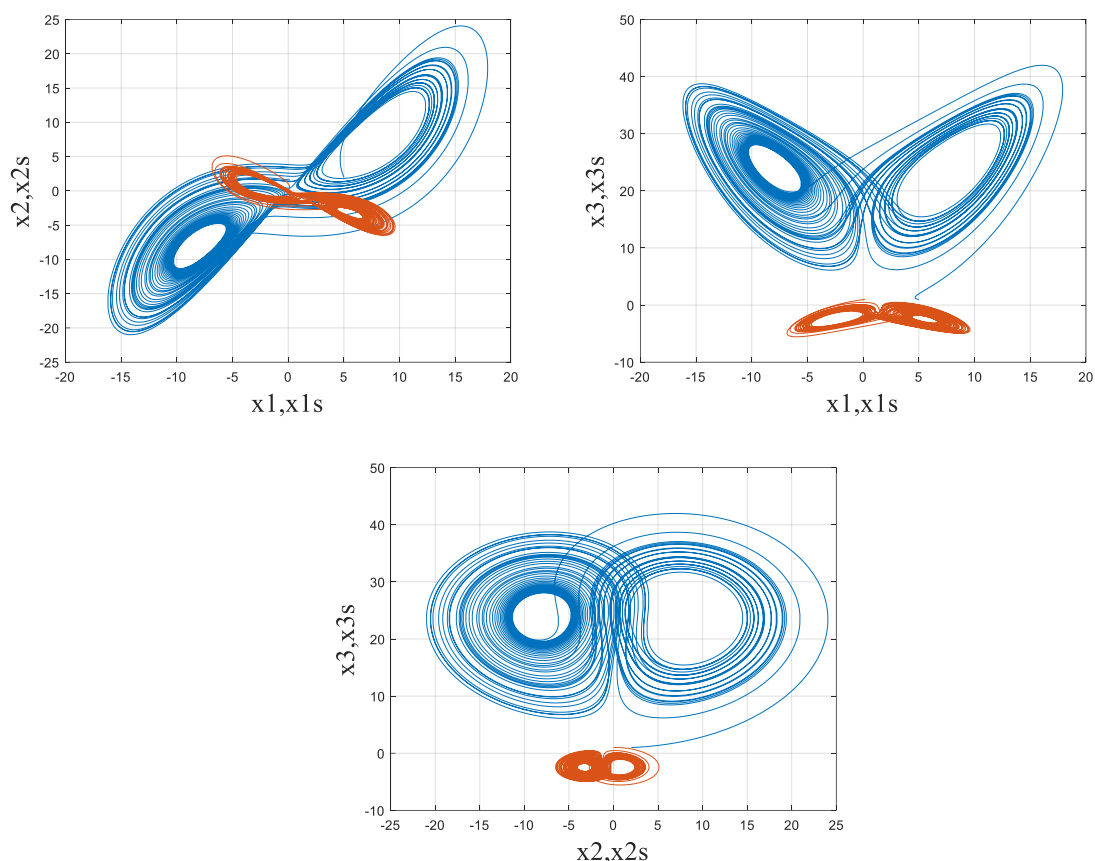
На фиг. 3.1 са представени получените функции на разсъгласуване, които не се установяват в нула, а в съответните коефициенти на изместване, което графично потвърждава настъпването на режим на изместена хаотична синхронизация около втората секунда от преходния процес.

Съвместната динамика на променливите на управляващата и подчинената системи $x_i(t), \tilde{x}_i(t), i = 1 \div 3$ е представена на фигура 3.2. Графичните резултати за управляващата система са представени в син цвят, а за подчинената система, в червен. Тази цветова комбинация се отнася за всички изображения представени в Глава 3.



Фиг. 3.2 Времеви характеристики

От графиката на фиг. 3.2 се вижда, че след края на преходния процес, двойките променливи x_1, \tilde{x}_1 и x_3, \tilde{x}_3 са в режим на антисинхронизация и динамиката на едната система е огледален образ спрямо абсцисата на динамиката на другата, т.е. подчинената система има един вид „обърнато” хаотично движение. Освен това амплитудата на \tilde{x}_1 и \tilde{x}_3 е съответно с α_1 и α_3 пъти по-ниска, т.е. динамиката на подчинената система е мащабирана със съответния коефициент, спрямо поведението на управляващата система. При двойката променливи x_2, \tilde{x}_2 се наблюдава режим на идентична синхронизация, като и тук се наблюдава мащабиране на амплитудата на сигнала на подчинената система с α_2 пъти спрямо управляващата. Фигура 3.2 графично потвърждава настъпването на режим на хибридна мащабирана синхронизация след края на преходния процес.



Фиг 3.3 Двумерни проекции на атракторите на Управляващата и Подчинената системи

На фигура 3.3 са представени трите двумерни проекции на хаотичните атрактори на управляващата и подчинената системи. Ясно се виждат разликите в двата атрактора, а именно не само по-малкия, но и изместен атрактор на подчинената система спрямо управляващата.

3.2.1.2 Таблично представяне на резултатите

Комбинираната синхронизация между две системи от трети ред предлага шест варианта на системата от разсъгласуване между управляващата и подчинената системи (таблица 3.1), за които се постига едновременно мащабирана, изместена и хибридна синхронизация.

За всеки от изброените варианти са направени подробни изследвания на преходните процеси на функциите на разсъгласуване, както и измененията в поведението на системите при различни коефициенти на мащабиране и изместване.

Таблица 3.1 Варианти на системата от разсъгласуване

Вариант 1	Вариант 2	Вариант 3
$\dot{e}_1 = \dot{x}_1 + \alpha_1 \tilde{x}_1 + c_1$ $\dot{e}_2 = \dot{x}_2 + \alpha_2 \tilde{x}_2 + c_2$ $\dot{e}_3 = \dot{x}_3 - \alpha_3 \tilde{x}_3 + c_3$	$\dot{e}_1 = \dot{x}_1 + \alpha_1 \tilde{x}_1 + c_1$ $\dot{e}_2 = \dot{x}_2 - \alpha_2 \tilde{x}_2 + c_2$ $\dot{e}_3 = \dot{x}_3 + \alpha_3 \tilde{x}_3 + c_3$	$\dot{e}_1 = \dot{x}_1 + \alpha_1 \tilde{x}_1 + c_1$ $\dot{e}_2 = \dot{x}_2 - \alpha_2 \tilde{x}_2 + c_2$ $\dot{e}_3 = \dot{x}_3 - \alpha_3 \tilde{x}_3 + c_3$
Вариант 4	Вариант 5	Вариант 6
$\dot{e}_1 = \dot{x}_1 - \alpha_1 \tilde{x}_1 + c_1$ $\dot{e}_2 = \dot{x}_2 + \alpha_2 \tilde{x}_2 + c_2$ $\dot{e}_3 = \dot{x}_3 + \alpha_3 \tilde{x}_3 + c_3$	$\dot{e}_1 = \dot{x}_1 - \alpha_1 \tilde{x}_1 + c_1$ $\dot{e}_2 = \dot{x}_2 + \alpha_2 \tilde{x}_2 + c_2$ $\dot{e}_3 = \dot{x}_3 - \alpha_3 \tilde{x}_3 + c_3$	$\dot{e}_1 = \dot{x}_1 - \alpha_1 \tilde{x}_1 + c_1$ $\dot{e}_2 = \dot{x}_2 - \alpha_2 \tilde{x}_2 + c_2$ $\dot{e}_3 = \dot{x}_3 + \alpha_3 \tilde{x}_3 + c_3$

В таблица 3.2 са представени стойностите на преходните процеси при всички комбинации на функциите на разсъгласуване между системите (3.2.1) и (3.2.2). Изследването е направено при константни стойности на мащабиращите и изместващите коефициенти, а именно $\alpha_1 = 2$, $\alpha_2 = 4$, $\alpha_3 = 6$, $c_1 = 3$, $c_2 = 5$ и $c_3 = 9$. Началните условия също не се изменят, като за Master системата $\mathbf{x} = [5 \ 2 \ 1]^T$, а за Slave системата - $\tilde{\mathbf{x}} = [0 \ 0 \ 1]^T$.

Таблица 3.2 Резултати за времетраенето на преходните процеси за система на Lorenz

Вариант	Времетраене на преходните процеси		
	T_{e1}	T_{e2}	T_{e3}
+ + -	2,08	1,50	1,26
+ - +	2,80	1,50	0,95
+ - -	2,80	1,50	1,20
- + +	3,06	1,50	0,94
- + -	2,84	1,50	1,07
- - +	2,86	1,50	0,93

За всички изброени комбинации са изследвани и влиянията на стойностите на коефициентите на мащабиране и изместване върху продължителността на преходните процеси. Подробно са представени резултатите за следния вариант на системата на разсъгласуване:

$$\begin{aligned} \dot{e}_1 &= \dot{x}_1 + \alpha_1 \tilde{x}_1 + c_1, \\ \dot{e}_2 &= \dot{x}_2 - \alpha_2 \tilde{x}_2 + c_2, \\ \dot{e}_3 &= \dot{x}_3 + \alpha_3 \tilde{x}_3 + c_3. \end{aligned} \quad (3.2.7)$$

Изследването на различни коефициенти на мащабиране е проведено при константни стойности на коефициентите на изместване - $c_1 = 3$, $c_2 = 5$ и $c_3 = 9$. Също така при изследване на коефициента α_1 , стойностите на α_2 и α_3 остават константни и равни на номиналните, аналогично са изследвани и измененията респективно за α_2 и α_3 .

Таблица 3.3 Резултати за времетраенето на преходните процеси при различни мащабиращи коефициенти

	Изменени мащабиращи коефициенти	Времетраене на преходните процеси		
		T_{e1}	T_{e2}	T_{e3}
$\alpha_2 = 4$ $\alpha_3 = 6$	$\alpha_1 = 1$	5.59	1,50	0,95
	$\alpha_1 = 2$	2,80	1,50	0,95
	$\alpha_1 = 3$	1.86	1.50	0.95
	$\alpha_1 = 4$	1.40	1.50	0.95
	$\alpha_1 = 5$	1.12	1.50	0.95
$\alpha_1 = 2$ $\alpha_3 = 6$	$\alpha_2 = 2$	2,80	3.05	0,95
	$\alpha_2 = 3$	2,80	2.04	0,95
	$\alpha_2 = 4$	2,80	1.50	0,95
	$\alpha_2 = 5$	2,80	1.22	0,95
	$\alpha_2 = 6$	2,80	1.02	0,95
$\alpha_1 = 2$ $\alpha_2 = 4$	$\alpha_3 = 4$	2,80	1,50	1.57
	$\alpha_3 = 5$	2,80	1,50	1.20
	$\alpha_3 = 6$	2,80	1,50	0.95
	$\alpha_3 = 7$	2,80	1,50	0.70
	$\alpha_3 = 8$	2,80	1,50	0.70

Таблица 3.4 Резултати за времетраенето на преходните процеси при различни коефициенти на изместване

	Изменени коефициенти на изместване	Времетраене на преходните процеси		
		T_{e1}	T_{e2}	T_{e3}
$c_2 = 5$ $c_3 = 9$	$c_1 = 1$	3,00	1,50	0,95
	$c_1 = 2$	3,00	1,50	0,95
	$c_1 = 3$	2,80	1,50	0,95
	$c_1 = 4$	2,70	1,50	0,95
	$c_1 = 5$	2,65	1,50	0,95
$c_1 = 3$ $c_3 = 9$	$c_2 = 3$	2,80	1,36	0,95
	$c_2 = 4$	2,80	1,40	0,95
	$c_2 = 5$	2,80	1,50	0,95
	$c_2 = 6$	2,80	1,57	0,95
	$c_2 = 7$	2,80	1,63	0,95
$c_1 = 3$ $c_2 = 5$	$c_3 = 7$	2,80	1,50	0,84
	$c_3 = 8$	2,80	1,50	0,84
	$c_3 = 9$	2,80	1,50	0,95
	$c_3 = 10$	2,80	1,50	1,00
	$c_3 = 11$	2,80	1,50	1,07

Анализ и изводи към Глава III

Разработената в настоящата глава методика за постигане на специфичен комбиниран вид синхронизация е базирана на втория метод за устойчивост на Ляпунов. Съчетани са три базови типа синхронизация, а именно мащабирана, хибридна и изместена, което води до синтезиране на значително по-сложно управление към подчинената система. Тъй като методиката използва хибридна синхронизация, са възможни множество вариации на комбинациите между променливите на вектора на състоянието в системата от разсъгласуване, като броят им зависи пряко от реда на използваната система. Възможността за постигане на толкова голям брой комбинации сама по себе си обуславя високо ниво на защита при имплементиране в системи за защитени комуникации. Добавяйки и произволният избор на коефициентите на мащабиране и изместване, се постига значително по-сложна динамика между системите, следователно се повишава и степента на защита.

Методиката е тествана върху всички класифицирани в Глава 1 хаотични и хиперхаотични системи, като всяка синтезирана синхронизационна схема постига устойчива синхронизация след приключване на преходните процеси. За целите на дисертацията са представени две синхронизационни схеми, реализирани със системи от трети ред (Lorenz и Zhou - Li) и една с хиперхаотична система от четвърти ред (Singh - Roy). За всяка от описаните синхронизационни схеми са изследвани всички варианти на комбинации на променливите на вектора на състоянието в системата от разсъгласуването, като различните варианти са сравнени посредством таблично представяне на продължителността на преходните процеси. За всяка представена синхронизационна схема е произволно избрана конкретна комбинация, която е подробно описана и изследвана при изменение на всеки от коефициентите на мащабиране и изместване, като и тук анализът на получените резултати е на база продължителностите на преходните процеси.

В настоящата глава се представя успешно реализиране на предложената методика, базирана на втори метод за устойчивост на Ляпунов, за постигане на по-сложно като вид

синхронно поведение между две хаотични или хиперхаотични системи. Като основно предимство на разработената методика може да се приеме постигането на сложна синхронна динамика между двете системи за достатъчно кратки преходни процеси. Методиката може да се приложи аналогично и в синхронизационни схеми, реализиращи синхронизация между три и повече хаотични или хиперхаотични системи.

Разработената нова методика за постигане на комбиниран вид синхронизация между хаотични системи осигурява достатъчно кратки преходни процеси, което обуславя по-широко приложение в областта на защитените комуникации в сравнение с базовите видове хаотична синхронизация. Представените в настоящата глава синхронизационни схеми са успешно имплементирани в трите фундаментални комуникационни системи за защитено предаване на аналогови и цифрови сигнали, а именно хаотично превключване, маскиране и модулиране, като резултатите са представени в глава 5.

Глава IV: Метод за постигане на специфични видове неидентична синхронизация на база линейно – нелинейна декомпозиция

В настоящата глава е представен метод за синхронизация на хаотични системи, базиран на линейно-нелинейна декомпозиция [84], като се предлага модификация на този метод, която гарантира постигането на повече от един вид хаотична синхронизация при един и същи синтез на връзка между подлежащите на синхронизация системи.

4.1 Формулировка на метода

При методът на линейно-нелинейна декомпозиция [84] изходната Master система условно се декомпозира на:

$$\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t), t) = \mathbf{A}\mathbf{x}(t) + \mathbf{h}(\mathbf{x}(t), t), \quad (4.1.1)$$

където $\mathbf{A}\mathbf{x}(t)$ е линейната част, а $\mathbf{h}(\mathbf{x}(t), t)$ е нелинейната част на $\mathbf{f}(\mathbf{x}(t), t)$. Функцията $\mathbf{h}(\mathbf{x}(t), t)$ се използва като свързващ сигнал между двете системи, които ще се синхронизират. Slave системата се конструира във вида:

$$\dot{\tilde{\mathbf{x}}}(t) = \mathbf{g}(\tilde{\mathbf{x}}(t)) + \mathbf{h}(\mathbf{x}(t), t) = \mathbf{A}\tilde{\mathbf{x}}(t) + \mathbf{h}(\mathbf{x}(t), t). \quad (4.1.2)$$

Системата от разсъгласуването ще бъде:

$$\dot{\mathbf{e}}(t) = \dot{\mathbf{x}}(t) - \dot{\tilde{\mathbf{x}}}(t) = \mathbf{A}(\mathbf{x}(t) - \tilde{\mathbf{x}}(t)) = \mathbf{A}\mathbf{e}(t). \quad (4.1.3)$$

В този случай, условието за устойчивостта на синхронизационната хиперравнина се свежда до анализ на устойчивостта на линейната система (4.1.3). Ако всички собствени стойности на матрицата \mathbf{A} (условните показатели на Ляпунов) са с отрицателни реални части, началото на координатната система за системата (4.1.3) ще бъде устойчиво.

Тъй като връзката между системите (4.1.1) и (4.1.2) е такава, че системата от разсъгласуването (4.1.3) е линейна система - $\dot{\mathbf{e}} = \mathbf{A}\mathbf{e}$, то типът на евентуалната синхронизация между системите може лесно да се определи по собствените стойности на матрицата \mathbf{A} .

- Ако всички собствени стойности на \mathbf{A} са с отрицателна реална част или реални отрицателни, между двете хаотични системи ще има идентична синхронизация.
- Ако поне една от собствените стойности на \mathbf{A} е равна на нула, а останалите са в лявата полуравнина на комплексната равнина, между (4.1.1) и (4.1.2) ще възникне изместена синхронизация.
- Ако измежду собствените стойности на \mathbf{A} има двойка комплексно-спрегнати такива с нулева реална част, а останалите са в лявата полуравнина на комплексната равнина, между двете хаотични системи ще възникне осцилираща синхронизация.

- Ако поне една от собствените стойности на A е в дясната полуравнина на комплексната равнина, между (1) и (2) не може да има синхронизирано движение, тъй като системата от разсъгласуването става неустойчива.

Основното предимство на метода на линейно-нелинейна декомпозиция е, че анализът за устойчивостта се прави върху линейната система (4.1.3), което позволява точното изчисляване на условните показатели на Ляпунов. От друга страна ограничението на метода на линейно-нелинейна декомпозиция е, че за конкретна хаотична система той позволява само един вариант на декомпозиция (4.1.1) и е голяма вероятността той да не води до устойчиво решение.

Методът за хаотична синхронизация с линейно-нелинейна декомпозиция само осигурява линейността на системата от разсъгласуването, без да може да повлияе върху знака на собствените стойности на матрицата A . Така за даден модел на хаотична система при прилагането на този метод матрицата A може да има положителна собствена стойност и между системите да не може да възникне синхронизация, а при прилагането на метода за друг модел на хаотична система матрицата A може да има собствени стойности, които да отговарят на условието за един от трите типа синхронизация, описани по-горе.

Предлага се методът за хаотична синхронизация с линейно-нелинейна декомпозиция да се съчетае с допълнителен управляващ сигнал към подчинената система (4.1.2) от типа:

$$\dot{\tilde{x}} = f(\tilde{x}, x) = A\tilde{x} + h(x) + B(x - \tilde{x}), \quad (4.1.4)$$

където $B_{n \times n}$ е матрица с константи, при което системата от разсъгласуването ще се получи във вида:

$$\dot{e} = Ax - A\tilde{x} - B(x - \tilde{x}) = (A - B)e. \quad (4.1.5)$$

От (4.1.5) се вижда, че при прилагането на допълнителното управление към подчинената система се запазва линейността на системата от разсъгласуването. В същото време чрез подходящ избор на ненулевите елементи на допълнителната матрица B може да се манипулират собствените стойности на матрицата A , така че според избраните и получени чрез матрицата B собствени стойности на системата от разсъгласуването да се получи желан тип синхронизация между хаотичните системи.

4.2 Изследване на метода

Модифицираният метод за постигане на специфични видове неидентична синхронизация на хаотични системи, базиран на линейно-нелинейна декомпозиция, е тестван върху три хаотични системи от трети ред (Rössler, Lorenz и Zhang-Li-Chang) и две хиперхаотични системи от четвърти ред (Singh Roy и Vaidiyanathan). Хаотичните системи, са подбрани така, че модифицираният метод на линейно-нелинейна декомпозиция да бъде тестван при различен брой нелинейни елементи.

4.2.1 Изследване на различни видове синхронизация между две системи на Rössler по модифицирания метод на линейно-нелинейна декомпозиция

Един от класическите модели на хаотични системи е този на Rössler, описващ се със следните уравнения:

$$\begin{aligned} \dot{x}_1 &= -x_2 - x_3, \\ \dot{x}_2 &= x_1 + \alpha x_2, \\ \dot{x}_3 &= \alpha + x_1 x_3 - \mu x_3, \end{aligned} \quad (4.2.1)$$

където $\alpha = 0.2$, а за да бъде хаотична системата бифуркационният параметър $\mu > 4.2$.

Ако (4.2.1) се приеме за Master система, тя може да се декомпозира на линейна и нелинейна част:

$$Master: \dot{x}(t) = Ax(t) + h(x(t), t), \quad (4.2.2)$$

където

$$A = \begin{bmatrix} 0 & -1 & -1 \\ 1 & \alpha & 0 \\ 0 & 0 & -\mu \end{bmatrix}, \quad \mathbf{h}(\mathbf{x}(t), t) = \begin{bmatrix} 0 \\ 0 \\ x_1 x_3 \end{bmatrix}. \quad (4.2.3)$$

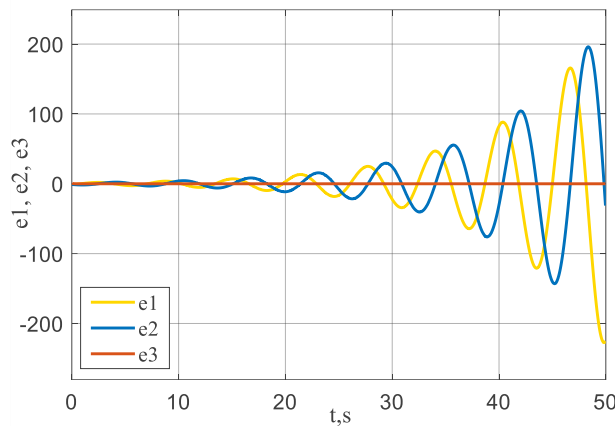
При базовия метод на линейно-нелинейна декомпозиция единственият вариант за Slave система според (4.1.2) е:

$$\begin{aligned} \dot{\tilde{x}}_1 &= -\tilde{x}_2 - \tilde{x}_3, \\ \dot{\tilde{x}}_2 &= \tilde{x}_1 + \alpha \tilde{x}_2, \\ \dot{\tilde{x}}_3 &= \alpha + x_1 x_3 - \mu \tilde{x}_3. \end{aligned} \quad (4.2.4)$$

При номиналните стойности на параметрите на системата $\alpha = 0.2$ и $\mu = 9$, собствените стойности на матрицата \mathbf{A} , от която се определя устойчивостта на синхронизацията, са:

$$\lambda_{1,2} = 0.10 \pm 0.9950j, \lambda_3 = -9, \quad (4.2.5)$$

т.е. базовият метод на линейно-нелинейна декомпозиция не води до устойчива синхронизация поради наличието на собствени стойности с положителна реална част.



Фиг. 4.1 Функции на разсъгласуване

На фиг. 4.1 са показани грешките $e_i(t) = x_i - \tilde{x}_i$ за $i = 1 \div 3$ при стартиране на системите от начални условия $\mathbf{x}_0 = [0 \ 0 \ 1]^T$ и $\tilde{\mathbf{x}}_0 = [1 \ 1 \ 0]^T$. Вижда се, че две от траекториите на системите рязко се раздалечават, т.е. $e_{1,2}(t) \rightarrow \infty$, докато $e_3(t) \rightarrow 0$. Колемателният характер на характеристиките се определя от наличието на комплексно-спрегнати собствени стойности.

4.2.1.1 Идентична синхронизация

За да се получи идентична синхронизация между двете системи на Rössler, трябва да се синтезира такова допълнително управление към подчинената система от вида $\mathbf{B}(\mathbf{x} - \tilde{\mathbf{x}})$, че всички собствени стойности на матрицата на състоянието на системата от разсъгласуването да станат с отрицателни реални части.

Вариант 1

Матрицата \mathbf{B} се избира във вида:

$$\mathbf{B} = \begin{bmatrix} b_{11} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad (4.2.6)$$

която съответства на следната подчинена система с допълнително управление:

$$\begin{aligned} \dot{\tilde{x}}_1 &= -\tilde{x}_2 - \tilde{x}_3 + b_{11}(x_1 - \tilde{x}_1), \\ \dot{\tilde{x}}_2 &= \tilde{x}_1 + \alpha \tilde{x}_2, \\ \dot{\tilde{x}}_3 &= \alpha + x_1 x_3 - \mu \tilde{x}_3. \end{aligned} \quad (4.2.7)$$

Системата от разсъгласуването ще има вида:

$$\begin{aligned} \dot{e}_1 &= -e_2 - e_3 - b_{11}e_1, \\ \dot{e}_2 &= e_1 + \alpha e_2, \\ \dot{e}_3 &= -\mu e_3, \end{aligned} \quad (4.2.8)$$

а матрицата на състоянието - съответно:

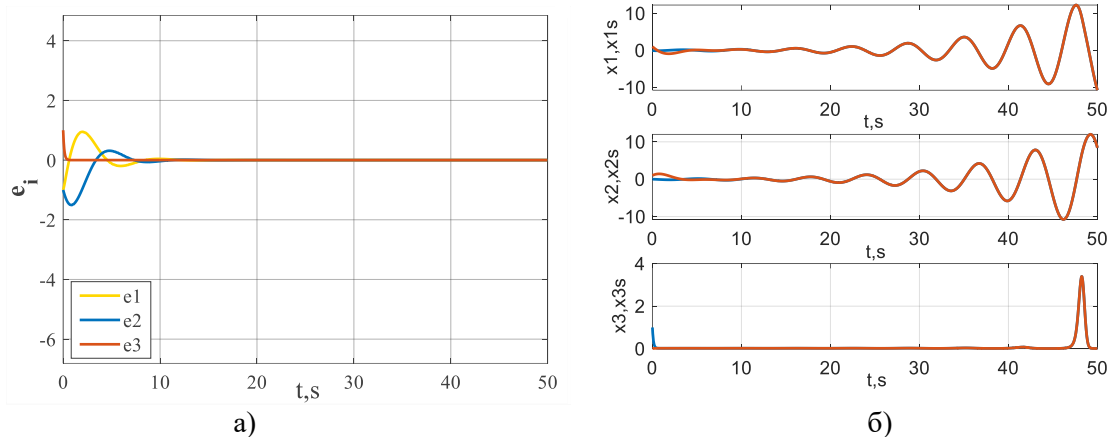
$$\mathbf{A} - \mathbf{B} = \begin{bmatrix} -b_{11} & -1 & -1 \\ 1 & \alpha & 0 \\ 0 & 0 & -\mu \end{bmatrix}. \quad (4.2.9)$$

Собствените стойности на матрицата (4.2.9) за номиналните стойности на параметрите и за $b_{11} = 1$, са:

$$\lambda_{1,2} = -0.4 \pm 0.8j, \lambda_3 = -9. \quad (4.2.10)$$

Така с помощта на допълнителния управляващ сигнал към първото уравнение на подчинената система се осигурява изпълнението на условието за получаване на идентична синхронизация между хаотичните системи.

Синхронизационната схема между управляващата система (4.2.1) и подчинената система (4.2.7) с допълнително управление (4.2.6) е симулирана в среда на Simulink. Началните условия на управляващата система са $\mathbf{x} = [0 \ 0 \ 1]^T$, а на подчинената система – $\tilde{\mathbf{x}} = [1 \ 1 \ 0]^T$, като и двата набора са избрани произволно.



Фиг. 4.2 Функции на разсъгласуване и времеви характеристики при идентична синхронизация между две системи на Rössler

Функциите $e_i = x_i - \tilde{x}_i$, получени при симулация на хаотичната синхронизационна система (4.2.1), (4.2.7), са показани на Фиг. 4.2 а), като и трите се установяват в нула, което съответства на желаната форма на синхронизация. Графично потвърждение за настъпване на идентична синхронизация между двете хаотични системи на Rössler са времевите характеристики показани на фиг. 4.2 б).

4.2.1.2 Изместена синхронизация

За постигането на изместена синхронизация между две идентични хаотични системи на Rössler, е необходимо синтезирането на такова допълнително управление към подчинената система - $\mathbf{B}(\mathbf{x} - \tilde{\mathbf{x}})$, че една от собствените стойности на матрицата на състоянието на системата от разсъгласуването да бъде нулева, а останалите да са с отрицателни реални части. В представения вариант е постигната изместена хаотична синхронизация с матрица $\mathbf{B}_{n \times n}$ съдържаща три ненулеви елемента.

Матрицата $\mathbf{B}_{n \times n}$ се избира във вида:

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 0 \\ b_{21} & b_{22} & 0 \\ b_{31} & 0 & 0 \end{bmatrix}, \quad (4.2.16)$$

което съответства на следната подчинена система с допълнително управление:

$$\begin{aligned} \dot{\tilde{x}}_1 &= -\tilde{x}_2 - \tilde{x}_3, \\ \dot{\tilde{x}}_2 &= \tilde{x}_1 + \alpha \tilde{x}_2 + b_{21}(x_1 - \tilde{x}_1) + b_{22}(x_2 - \tilde{x}_2), \\ \dot{\tilde{x}}_3 &= \alpha + x_1 x_3 - \mu \tilde{x}_3 + b_{31}(x_1 - \tilde{x}_1) \end{aligned} \quad (4.2.17)$$

Системата от разсъгласуването ще има вида:

$$\begin{aligned} \dot{e}_1 &= -e_2 - e_3, \\ \dot{e}_2 &= e_1 + \alpha e_2 - b_{21}e_1 - b_{22}e_2, \\ \dot{e}_3 &= -\mu e_3 - b_{31}e_1, \end{aligned} \quad (4.2.18)$$

а матрицата на състоянието при номиналните стойности на параметрите и за $b_{21} = 1$, $b_{22} = 0,2$ и $b_{31} = -9$, ще има следния вид:

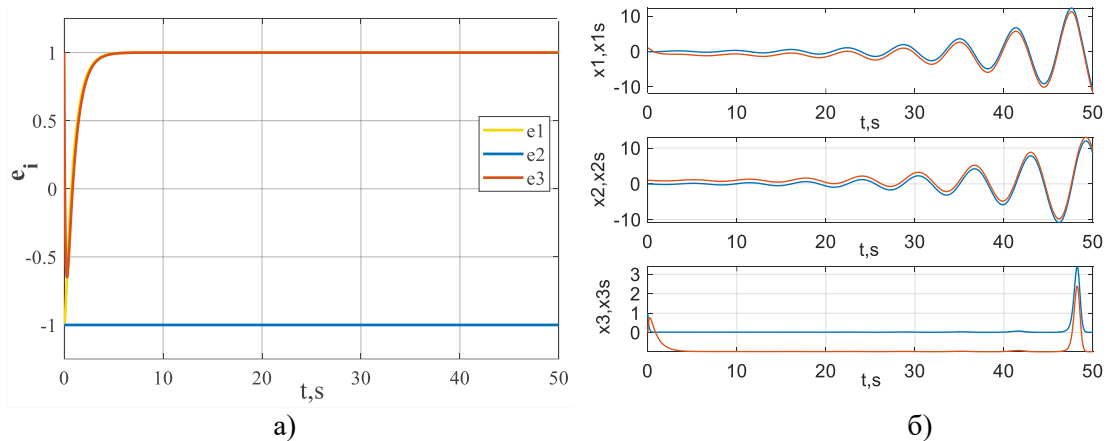
$$\mathbf{A} - \mathbf{B} = \begin{bmatrix} 0 & -1 & -1 \\ 1 - b_{21} & \alpha - b_{22} & 0 \\ -b_{31} & 0 & -\mu \end{bmatrix}. \quad (4.2.19)$$

Собствените стойности на матрицата (4.2.19) са:

$$\lambda_1 = -1.1459, \lambda_2 = -7.8541, \lambda_3 = 0. \quad (4.2.20)$$

Изпълнението на условието за получаване на изместена синхронизация между двете идентични хаотични системи, се постига с помощта на допълнителните управляващи сигнали към второто и третото уравнения на подчинената система.

Синхронизационната схема между управляващата система (4.2.1) и подчинената система (4.2.17) с допълнително управление (4.2.16) е симулирана в среда на Simulink. Графичните интерпретации на синхронизационните процеси са получени в среда на Matlab, при следните начални условия $\mathbf{x} = [0 \ 0 \ 1]^T$ и $\tilde{\mathbf{x}} = [1 \ 1 \ 0]^T$.



Фиг. 4.4 Функции на разсъгласуване $e_i(t)$, $i = 1 \div 3$ и времеви характеристики при изместена синхронизация между две системи на Rössler

След края на преходния процес, функциите на разсъгласуване, показани на Фиг. 4.4 а) се установяват в стойност различна от нула, което съответства на желаната форма на синхронизация. Показаните на фиг. 4.4 б) времеви характеристики, графично потвърждават настъпването на изместена синхронизация след края на преходния процес.

4.2.1.3 Осцилираща синхронизация

Модифицираният метод на линейно-нелинейна декомпозиция постига осцилираща синхронизация между две идентични хаотични системи на Rössler, посредством синтезирането на такова допълнително управление към подчинената система - $\mathbf{B}(\mathbf{x} - \tilde{\mathbf{x}})$,

че една от собствените стойности на матрицата на състоянието на системата от разсъгласуването да бъде отрицателна, а останалите да са с нулеви реални части. В представения вариант е постигната осцилираща хаотична синхронизация с матрица $\mathbf{V}_{n \times n}$ съдържаща четири ненулеви елемента.

Избраната матрица $\mathbf{V}_{n \times n}$ има вида:

$$\mathbf{V} = \begin{bmatrix} b_{11} & 0 & b_{13} \\ 0 & b_{22} & 0 \\ b_{31} & 0 & 0 \end{bmatrix}. \quad (4.2.21)$$

Съответстваща на следната подчинена система с допълнително управление:

$$\begin{aligned} \dot{\tilde{x}}_1 &= -\tilde{x}_2 - \tilde{x}_3 + b_{11}(x_1 - \tilde{x}_1) + b_{13}(x_3 - \tilde{x}_3), \\ \dot{\tilde{x}}_2 &= \tilde{x}_1 + \alpha \tilde{x}_2 + b_{22}(x_2 - \tilde{x}_2), \\ \dot{\tilde{x}}_3 &= \alpha + x_1 x_3 - \mu \tilde{x}_3 + b_{31}(x_1 - \tilde{x}_1). \end{aligned} \quad (4.2.22)$$

Тогава системата от разсъгласуването ще има следния вид:

$$\begin{aligned} \dot{e}_1 &= -e_2 - e_3 - b_{11}e_1 - b_{13}e_3, \\ \dot{e}_2 &= e_1 + \alpha e_2 - b_{22}e_2, \\ \dot{e}_3 &= -\mu e_3 - b_{31}e_1, \end{aligned} \quad (4.2.23)$$

а матрицата на състоянието - съответно:

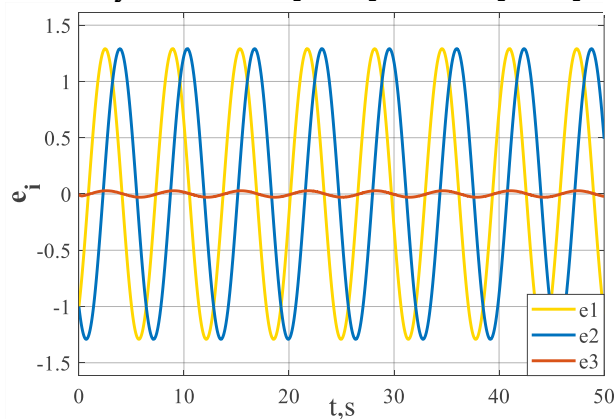
$$\mathbf{A} - \mathbf{V} = \begin{bmatrix} -b_{11} & -1 & -1 - b_{13} \\ 1 & \alpha - b_{22} & 0 \\ -b_{31} & 0 & -\mu \end{bmatrix}. \quad (4.2.24)$$

Собствените стойности на матрицата (4.2.24) за номиналните стойности на параметрите и за $b_{11} = -0.2$, $b_{13} = -1$, $b_{22} = 0.4$ и $b_{31} = -0.2$ са:

$$\lambda_1 = -9, \quad \lambda_{2,3} = 0 \pm 0.9798j. \quad (4.2.25)$$

С помощта на допълнителните управляващи сигнали към уравненията на подчинената система се осигурява изпълнението на условието за получаване на осцилираща синхронизация между двете идентични хаотични системи.

Синхронизационната схема между управляващата система (4.2.1) и подчинената система (4.2.22) с допълнително управление (4.2.21) е симулирана в среда на Simulink като графичните интерпретации на синхронизационните процеси са получени в среда на Matlab, при следните начални условия $\mathbf{x} = [0 \ 0 \ 1]^T$ и $\tilde{\mathbf{x}} = [1 \ 1 \ 0]^T$.



Фиг. 4.5 Функции на разсъгласуване $e_i(t)$, $i = 1 \div 3$

Функциите на разсъгласуване, показани на фиг. 4.5 графично потвърждават настъпването на осцилираща синхронизация.

Анализи и изводи към Глава IV

Предложен е метод за хаотична синхронизация, осигуряващ различни видове неидентично синхронно поведение, в основата на който е методът на линейно – нелинейна декомпозиция. Методът представлява модификация на метода на линейно-нелинейната декомпозиция, като посредством прилагането на допълнителното управление към подчинената система, се гарантира постигането на повече от един вид хаотична синхронизация при един и същи синтез на връзка между подлежащите на синхронизация системи. Реализираният метод запазва основното предимство на метода на линейно-нелинейната декомпозиция – възможен е точен анализ на устойчивостта на конкретната схема, тъй като системата от разсъгласуването остава линейна. Същевременно, посредством прилагането на допълнително управление към подчинената система, предложеният метод преодолява основното ограничение на базовия метод – дава възможност за реализиране на множество варианти на декомпозиция, докато при базовия метод вариантът е само един и за много хаотични системи той не води до устойчива синхронизация.

Модифицираният метод за синхронизация на хаотични системи, осигуряващ различни видове неидентично синхронно поведение, базиран на линейно-нелинейна декомпозиция е тестван върху всички класифицирани в Глава 1 хаотични и хиперхаотични системи, като всяка синтезирана синхронизационна схема постига устойчива синхронизация след приключване на преходните процеси. Подробни резултати са представени за три хаотични системи от трети ред, от които две фундаментални – Rössler и Lorenz и един нов абстрактен математичен модел – Zhang-Li-Chang и две хиперхаотични системи от четвърти ред – системи на Singh Roy и Vaidyanathan. Методът на линейно-нелинейна декомпозиция и предложената по-горе негова модификация са подходящи за прилагане при хаотични системи със сравнително по-малък брой нелинейни елементи. При системи с много нелинейности, методът на линейно-нелинейна декомпозиция предполага реализирането на сложна връзка с използване на пълния вектор на състоянието на Master системата. Затова използваните хаотични системи са подбрани така, че модифицираният метод на линейно-нелинейна декомпозиция да бъде тестван при различен брой нелинейни елементи.

Предложеният метод постига различни специфични неидентични синхронни поведения посредством малки изменения в допълнителното управление към подчинената система, което го прави изключително атрактивен за имплементиране в схеми за защитено предаване на данни. Аналогично на методиката от глава 3, представеният метод може да се разшири, като се приложи в синхронизационни схеми реализиращи синхронизация между три и повече хаотични или хиперхаотични системи.

Разработеният метод осигуряващ различни видове неидентично синхронно поведение между хаотични системи постига достатъчно кратки преходни процеси, които в комбинация със сложното синхронно поведение между системите, обуславят широко приложение в областта на защитените комуникации и в частност криптирането на изображения. Представените в настоящата глава синхронизационни схеми са успешно имплементирани в три различни съвременни и актуални алгоритъма за криптиране на изображения, базирани се на кодиращ ключ, като резултатите от изследването са представени в глава 5.

Глава V: Приложение на хаотични синхронизационни схеми в комуникационни системи за защитено предаване на информация

От началото на 90-те години са разработени изключително много изследвания в две различни, но допълващи се насоки, а именно синхронизирането на хаотични системи и комуникация базирана на хаос. Голяма част от комуникационните системи, базирани на

хаос се основават на синхронизирани хаотични системи. Това означава, че при определени обстоятелства сложната и силно чувствителна нелинейна динамика на свързаните хаотични системи, се синхронизира и полученото синхронно състояние може да се използва в комуникационната схема по няколко различни начина.

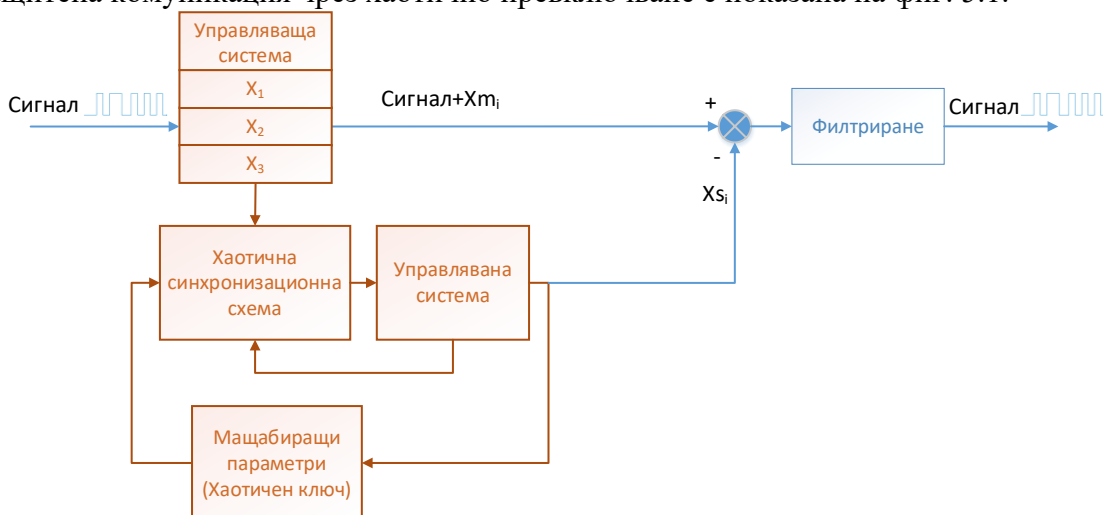
В настоящата глава са представени две основни приложения на синхронизацията на хаотични системи – при защитено предаване на аналогови и цифрови сигнали и при кодиране на изображения.

5.1 Приложение на хаотични синхронизационни схеми в защитено предаване на аналогови и цифрови сигнали

Описани са трите базови приложения на хаотичните синхронизационни схеми за защитено предаване на информационен сигнал (аналогов и цифров), а именно хаотично превключване, хаотично маскиране и хаотично модулиране. Въпреки, че тези приложения имат множество модификации и вариации, се реализират класическите им варианти, като по този начин се акцентира върху синхронизационната схема. На практика комбинацията с дадена хаотична синхронизационна схема се явява нов вариант за защита на сигнала. Така постигнатите ниво на защита и качество на декодирането ще се дължат главно на реализираната синхронизация. И трите приложения са симулирани в среда на Simulink, като избраните хаотични синхронизационни схеми се базират на втория метод за устойчивост на Ляпунов и комбинирания вид синхронизация, подробно описани в глава 3.

5.1.1 Предаване на цифров сигнал чрез хаотично превключване

Прилага се базов вариант на метода за защитена комуникация чрез хаотично превключване. Избрана е синхронизационната схема описана в глава 3, т. 3.2.1.1 при константни стойности на мащабиращите и изместващите коефициенти, а именно $\alpha_1 = 2$, $\alpha_2 = 4$, $\alpha_3 = 6$, $c_1 = 3$, $c_2 = 5$ и $c_3 = 9$. Синтезираната синхронизационна схема между две идентични хаотични системи на Lorenz дава достатъчно кратки продължителности на преходните процеси при избраният конкретен вариант на комбинирана синхронизация, а това е необходимо, тъй като бързодействието е от голямо значение при реализиране на защитена комуникация чрез хаотично превключване. Обобщена блокова схема на метода за защитена комуникация чрез хаотично превключване е показана на фиг. 5.1.

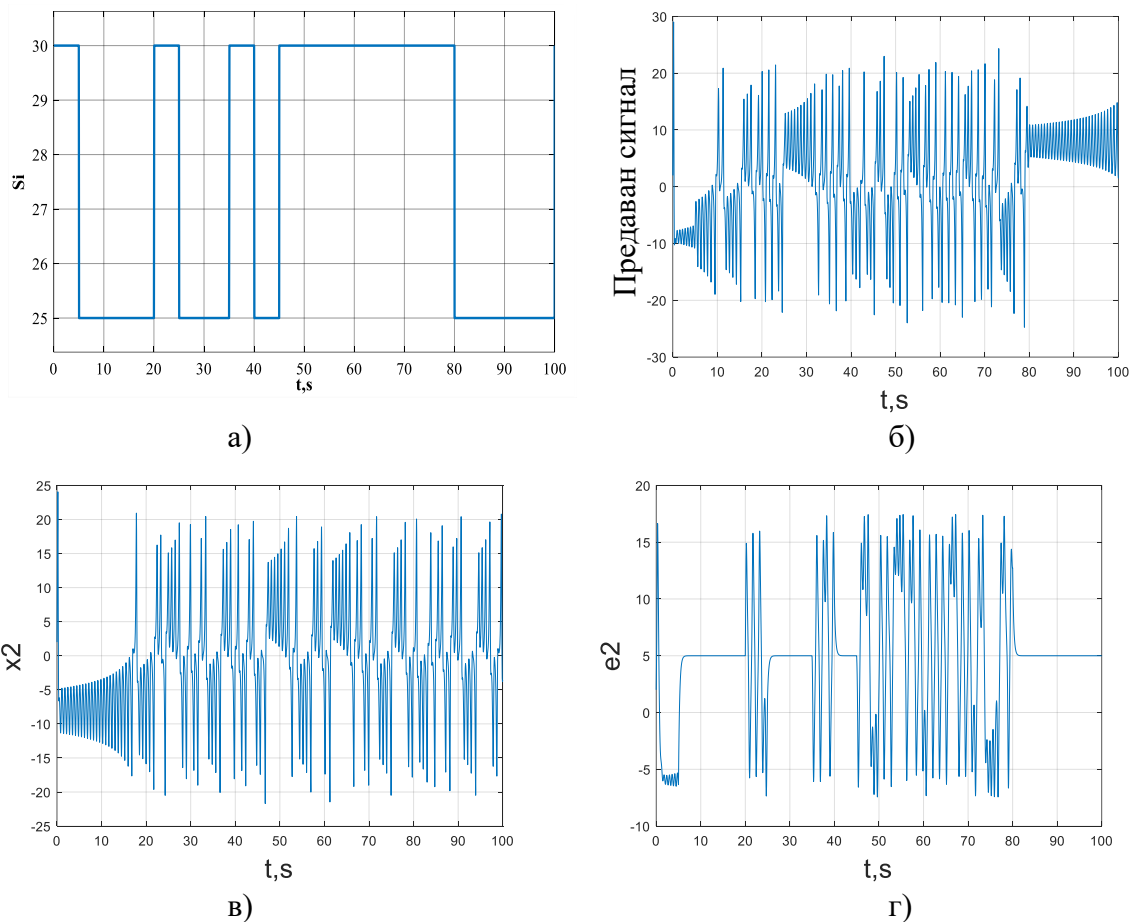


Фиг. 5.1 Обобщена блокова схема за защитена комуникация чрез хаотично превключване

В представената обобщена блокова схема на хаотично превключване, цифровият информационен сигнал заменя бифуркационен параметър в Master системата. По комуникационната линия се предава хаотичният сигнал на тази променлива от вектора на състоянието, към чието уравнение информационният сигнал заменя параметъра. При възстановяване се използва свойството, че при асоциирана единица на информационния сигнал няма синхронизация между двете системи, а при нула – се осъществява

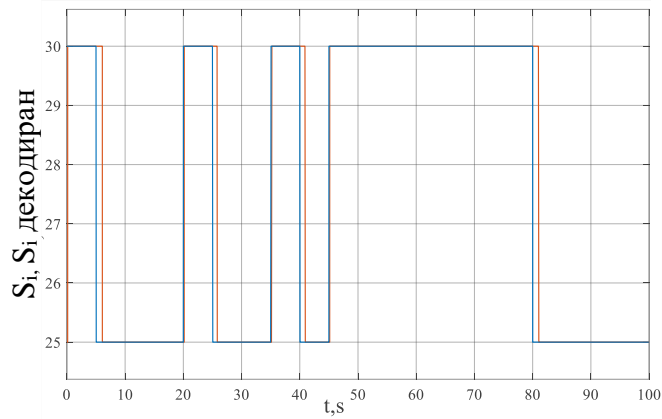
синхронизация. Последващият сигнал преминава през процес на филтриране, който се реализира чрез набор от нискочестотни, медианни и функционални филтри и прагови обработки.

Нека е необходимо защитеното предаване на двоичната последователност показана на фиг. 5.3 а). Избира се атракторът за $r = 25$ да съответства на "0", а този за $r = 30$ - на "1". Предварително е необходимо да се избере продължителността на предаване на всеки бит, съобразена с времето за постигане на синхронизация. За по-нагледна илюстрация на комуникационния метод е избрана по-голяма продължителност – $2.5s/\text{бит}$. Реално синхронизационната схема реализирана на база комбиниран вид синхронизация между две идентични системи на Lorenz, допуска неколкостранно по-малка продължителност. Чрез съответен модулатор в предавателя (Master системата) параметърът r се изменя алтернативно между 25 и 30, съгласно конкретната двоична последователност и избраната продължителност на бит. В моментите, когато трябва да се предаде "1" системите се разсинхронизират, а при "0" се синхронизират отново. На фиг.5.3 а) е показана двоичната последователност чрез стойностите на параметъра r ; на 5.3 б) - свързващият сигнал x_2 при модулацията на параметъра, означен като Transmitted signal; на 5.3 в) - свързващият сигнал x_2 при стандартна синхронизация; на фиг. 5.3 г) – грешката $e_2(t)$.



Фиг. 5.3 Комуникация чрез хаотично превключване

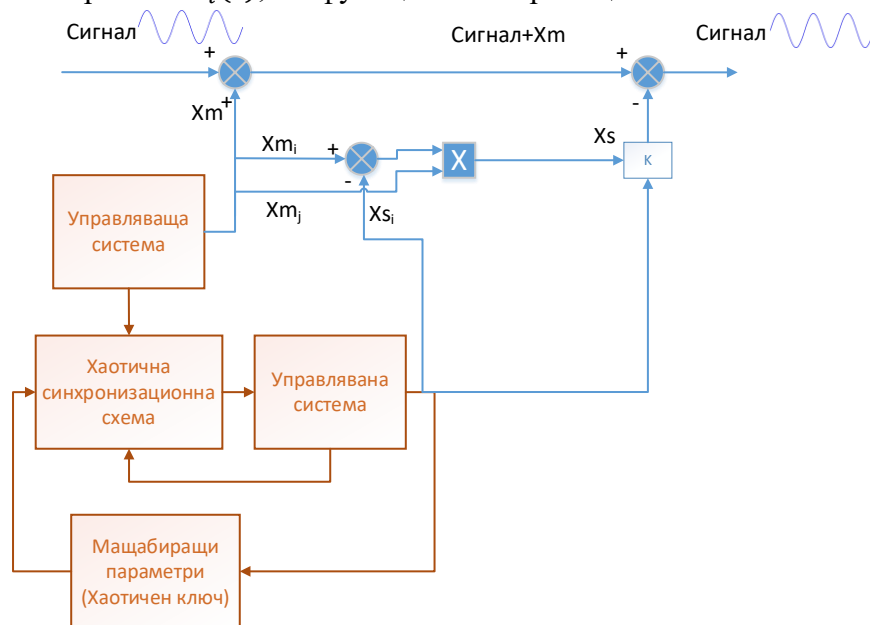
На фигура 5.4 са представени предаваната и възстановената в приемника информационна поредица. Наблюдава се несъответствие в продължителността на импулсите, дължащо се на продължителността на преходния процес при синхронизация. Имайки в предвид продължителността на предаване на даден бит и това, че импулсите могат да се възстановят по преден фронт, то това несъответствие е несъществено.



Фиг. 5.4 Генерирана и декодирана информационна поредица

5.1.2 Предаване на цифров сигнал чрез хаотично маскиране

Само по себе си, хаотичното маскиране е елементарен начин за защита на предаваната информация, който предполага просто сумиране на информационния сигнал S_i със свързващия хаотичен сигнал. Ако информационният сигнал е с много по-малка амплитуда от хаотичния, то сигналят $x_i(t) + S_i(t)$ няма да се различава видимо от $x_i(t)$ и така информацията ще остане скрита по трасето. Има различни вариации на хаотичното маскиране, които водят до по-високо ниво на защита. В някои от тях информационният сигнал се сумира не просто с $x_i(t)$, а с функция на свързващия хаотичен сигнал $f(x_i(t))$.



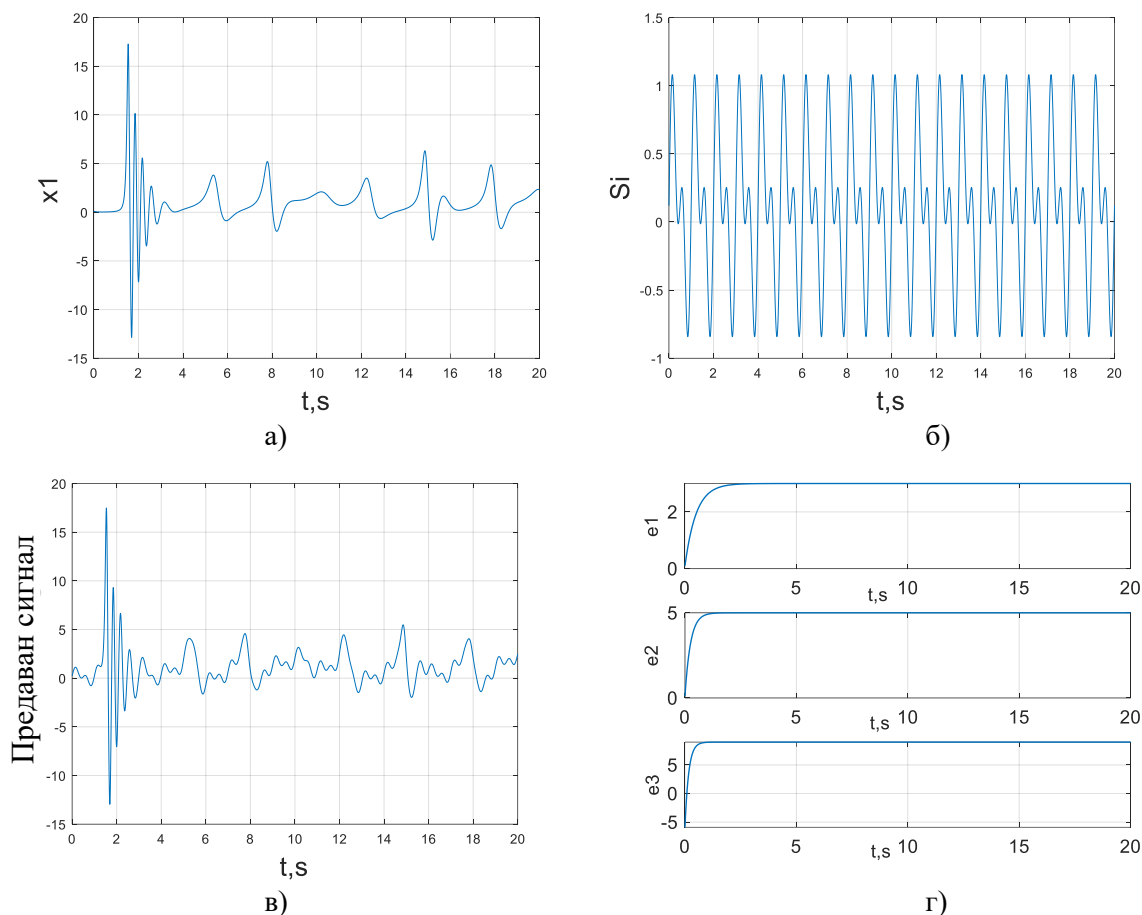
Фиг. 5.6 Обобщена блокова схема за защитена комуникация чрез хаотично маскиране

Добавянето на допълнителен сигнал към свързващия сигнал от гледна точка на синхронизацията е идентично с добавяне на смущаващо въздействие. Тъй като предварително е подбрана устойчива синхронизационна схема, синхронизацията ще бъде стабилна и няма да се повлияе от информационния сигнал. Разбира се това е в сила, ако амплитудата на този сигнал е много по-малка от амплитудата на носещата хаотична компонента.

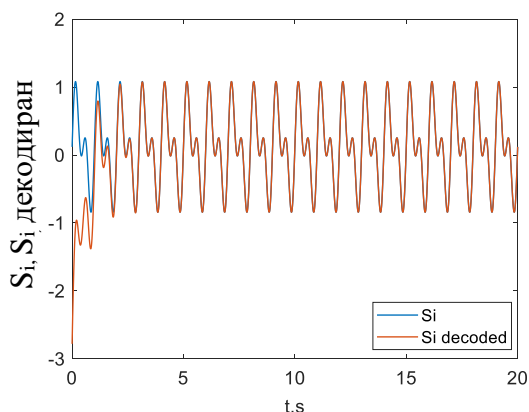
За целите на дисертацията се прилага базов вариант на метода за защитена комуникация чрез хаотично маскиране. Избрана е синхронизационната схема, описана в глава 3, т. 3.2.2.1 при константни стойности на мащабиращите и изместващите коефициенти, а именно $\alpha_1 = 2$, $\alpha_2 = 4$, $\alpha_3 = 6$, $c_1 = 3$, $c_2 = 5$ и $c_3 = 9$. При реализиране на защитена комуникация чрез хаотично превключване, бързодействието е от голямо

значение, а синтезираната синхронизационна схема между две идентични хаотични системи на Zhou – Li, при избраният конкретен вариант на комбинирана синхронизация, дава достатъчно кратки продължителности на преходните процеси.

В реализираната схема за защитено предаване на информация за свързващ сигнал е избран x_1 показан на фигура 5.7 а), като той се сумира с информационният сигнал S_i – показан на фиг. 5.7 б). Предаваният по комуникационния канал сигнал е показан на фиг. 5.7 в), а на фиг. 5.7 г) – грешките от разсъгласуване $e_i(t)$.



Фиг. 5.7. Комуникация чрез хаотично маскиране



Фиг. 5.8 Генериран и възстановен информационен сигнал

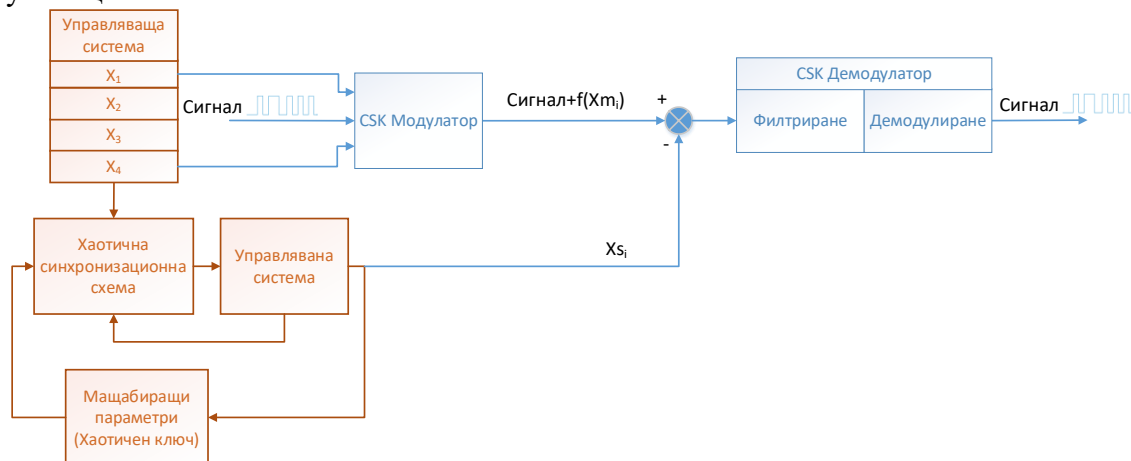
На фигура 5.8 са представени информационният сигнал преди кодиране и възстановеният в приемника информационен сигнал. Наблюдава се разлика между двата сигнала с продължителност равна на времетраенето на преходния процес на синхронизация.

5.1.3 Предаване на цифров сигнал чрез хаотично модулиране

В основата си, хаотичната модулация се състои в примесване на информационния сигнал в уравненията на хаотичната система. Самото примесване функционира като смущение, което променя динамиката на предавателя така, че самият хаотичен сигнал да съдържа информация. Посредством синхронизация, приемникът е способен да регенерира съответния непроменен хаотичен сигнал, а извличането на информационния сигнал се осъществява чрез сравняване на получения и генерирания хаотични сигнали.

Избрана е синхронизационната схема описана в глава 3, т. 3.2.3.1 при константни стойности на мащабиращите и изместващите коефициенти, а именно $\alpha_1 = 2$, $\alpha_2 = 4$, $\alpha_3 = 6$, $\alpha_4 = 8$, $c_1 = 3$, $c_2 = 5$, $c_3 = 7$ и $c_4 = 9$. Синтезираната синхронизационна схема между две идентични хиперхаотични системи на Singh – Roy, дава достатъчно кратки продължителности на преходните процеси при избрания конкретен вариант на комбинирана синхронизация, а това е необходимо, тъй като бързодействието е от голямо значение при реализиране на защитена комуникация чрез хаотично модулиране.

Обобщена блокова схема на метода за защитена комуникация чрез хаотично модулиране е показана на фиг. 5.10. Отново в червено са обозначени блоковете и връзките касаещи хаотичната синхронизация, а в синьо – блоковете и връзките касаещи комуникационната схема.



Фиг. 5.10 Обобщена блокова схема за защитена комуникация чрез хаотично модулиране

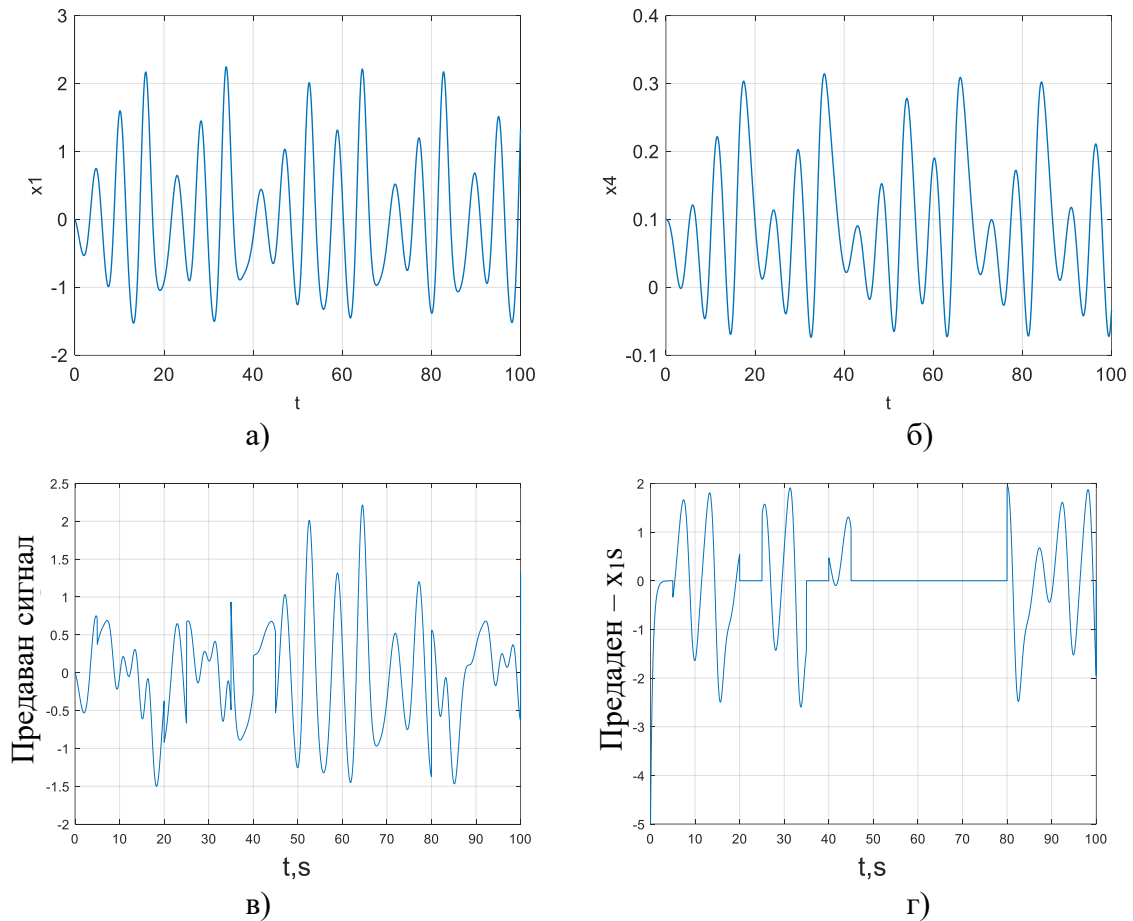
Хаотичното модулиране е най-изтънчения метод за защита на информацията посредством хаос. Често се използват системи от висок ред, като минималният е трети. Самата схема представя цифровия информационен сигнал като функция на два хаотични сигнала от две или повече променливи на състоянието на Master системата, като това се извършва в блока CSK Modulator. В приемника, приетият кодиран сигнал се възстановява при осъществяване на синхронизация, чрез изваждане на хаотичния сигнал на една от променливите от Slave системата. Възстановяването на сигнала се извършва, посредством преминаване през поредица от филтри и демодулиране, като това се реализира в блока CSK Demodulator. Представеният комбиниран вид синхронизация се имплементира лесно и при този тип кодиране, повишавайки драстично степента на защита на информацията, тъй като мащабиращите и изместващи коефициенти образуват хаотични ключове, за повече от една променливи на Slave системата, които могат да се използват за възстановяване на информационния сигнал.

Нека е необходимо защитено предаване на двоичната последователност показана на фиг. 5.11. Съгласно представената схема за защитена комуникация чрез хаотично модулиране, информационната поредица се предава като модулиран сигнал с динамика изменяща се между динамиката на променливите от вектора на състоянието на Master

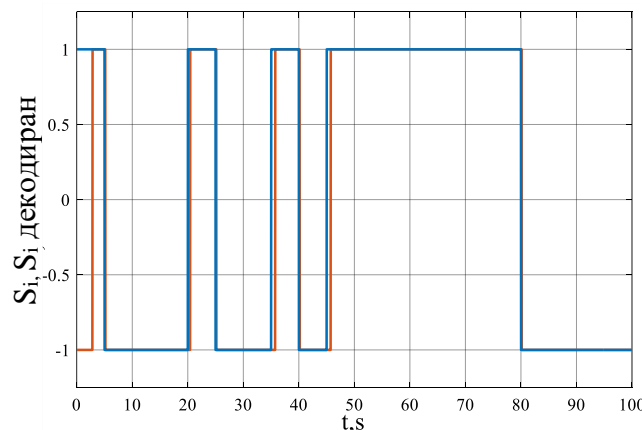
системата - x_1 и x_4 . За конкретната двоична последователност, когато по комуникационната линия трябва да се предаде „1“ се предава x_1 от Master системата, а когато трябва да се предаде „0“ - x_4 .

Процесът по възстановяване на информационния сигнал в приемника е по-сложен от колкото при другите видове кодиращи схеми. След синхронизация, от приетия сигнал се изважда динамиката на променливата от вектора на състоянието на Slave системата - \tilde{x}_1 . Следват функционални и прагови обработки, филтриране и демодулиране.

На фиг. 5.12 а) е показана променливата от вектора на състоянието x_1 ; на 5.12 б) – динамиката на x_4 ; на 5.12 в) – модулираният сигнал, означен като Transmitted signal; на фиг. 5.12 г) – Сигналът в приемника получен след изваждане на \tilde{x}_1 .



Фиг. 5.12 Комуникация чрез хаотично модулиране



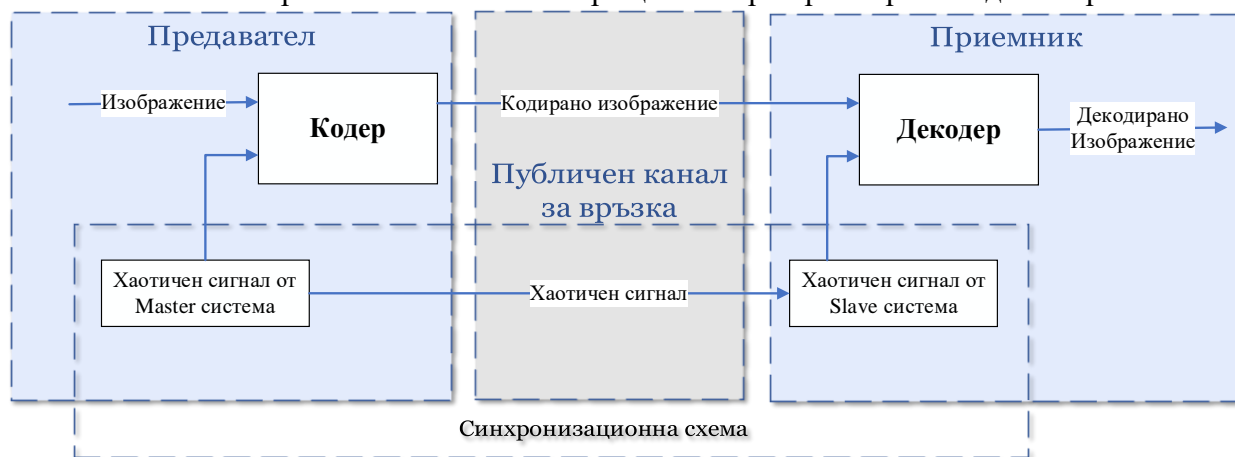
Фиг. 5.13 Генерирана и декодирана информационна поредица

На фигура 5.13 са представени предаваната и възстановената в приемника информационна поредица. Наблюдава се несъответствие в продължителността на импулсите, дължащо се на продължителността на преходния процес при синхронизация. Имайки в предвид продължителността на предаване на даден бит и това, че импулсите могат да се възстановят по заден фронт, то това несъответствие е несъществено.

5.2 Приложение на хаотични синхронизационни схеми в криптиране на изображения.

Поради спецификата на структурата на едно изображение, използването на хаотичен сигнал и хаотични синхронизационни схеми за неговото кодиране, се реализира особен тип модификация на кодиращите алгоритми. Самата комуникационна система се състои от приемник и предавател, като важно условие се явява запазването на изображението в оригиналния му вид (матрица от пиксели със силна корелация между тях). Поради тази причина не е препоръчително преформатирането на файлове, съдържащи изображения, във файлове, съдържащи друг тип информация, или в сигнали. В предавателя се използва хаотичен сигнал от управляващата система, посредством който се формира т.н. кодиращ ключ. В приемника се използва сигнал от подчинената система, която след синхронизация дава необходимия сигнал за формирането на еквивалентен декодиращ ключ. По комуникационния канал се предава кодираното изображение, както и хаотичен сигнал от управляващата система.

На практика хаотичният сигнал може да се въведе на много от етапите на кодиране, но целта е да се запази същността на алгоритъма, т.е. генерирането на определен кодиращ ключ. Този тип алгоритми са и най-често срещаните при криптирането на изображения.



Фиг. 5.17 Обобщена блокова схема на комуникационна система, с имплементирана хаотична синхронизационна схема, за защитено предаване на криптирано изображение в публичен канал за връзка

На фигура 5.17 е представена обобщена блокова схема на комуникационна система, с имплементирана хаотична синхронизационна схема, за защитено предаване на криптирано изображение в публичен канал за връзка. Хаотичната синхронизационна схема е разделена, като в предавателя се намира управляващата система, а в приемника – подчинената система. В общия случай, оригиналното изображение се криптира със сигнал генериран от Master системата. В приемника, подчинената система се синхронизира с управляващата, посредством предадения по комуникационния канал сигнал, а криптираното изображение се декодира посредством сигнал генериран от синхронизираната подчинена система.

В главата са представени три алгоритъма за криптиране на изображения модифицирани посредством използването на хаотичен сигнал имплементиран на различни нива от кодирането и реализирането на последваща хаотична синхронизационна

схема за възстановяване на кодираното изображение. Избраните алгоритми за криптиране на изображения са именно: алгоритъм, базиран на фрактални функции, алгоритъм за криптиране посредством дифузионна матрица и ОТР (One-time path) алгоритъм. Анализът на получените резултати, по отношение на кодираното и декодираното изображение, се осъществява по три основни подхода, използвани в анализа на изображения, а именно чрез сравняване на: хистограми, корелации и криви на предпочитанията. Избраните три алгоритма за криптиране на изображения са реализирани в среда на Matlab, като имплементираните в тях хаотични синхронизационни схеми постигат синхронизация посредством модифицирания метод, базиран на линейно – нелинейна декомпозиция, подробно описан в глава 4. За всеки алгоритъм, в главата са представени реализации за трите вида синхронизация, като подробно са представени резултатите при кодиране и декодиране на различни изображения.

5.2.1 Имплементиране на хаотични синхронизационни схеми в алгоритъм за криптиране на изображения, базиран на фрактални функции

Представената техника за кодиране на изображения се основава на комбинация на известен алгоритъм, базиран на фрактални функции с хаотичен сигнал. За реализиране на декодирането е необходима хаотична синхронизация с цел получаване на използвания за кодирането хаотичен сигнал. Най-общо алгоритъмът се състои от четири модула: генериране на ключ, фрактално кодиране, хаотично кодиране и декодиране. В разглежданата модификация, хаотичният сигнал се използва във всеки един от модулите, започвайки от генерирането на ключа, който за разлика от традиционния алгоритъм тук се изчислява многократно в зависимост от големината на изображението. На практика направената модификация увеличава степента на защита многократно, а използваният хаотичен сигнал, присъства на всички нива от кодирането, включително и в процеса на генериране на фракталното *Tromino*. От друга страна, хаосът се използва и във финалния кодиращ алгоритъм, като DCT (*discrete cosine transform*), след което се получава финалното кодирано изображение. Респективно, кодираното изображение се декодира чрез обратно прилагане на хаотично базирания модул и фрактално базирания декриптиращ алгоритъм. Използваният хаотичен сигнал в процеса на декриптиране, се получава след процес на синхронизация.

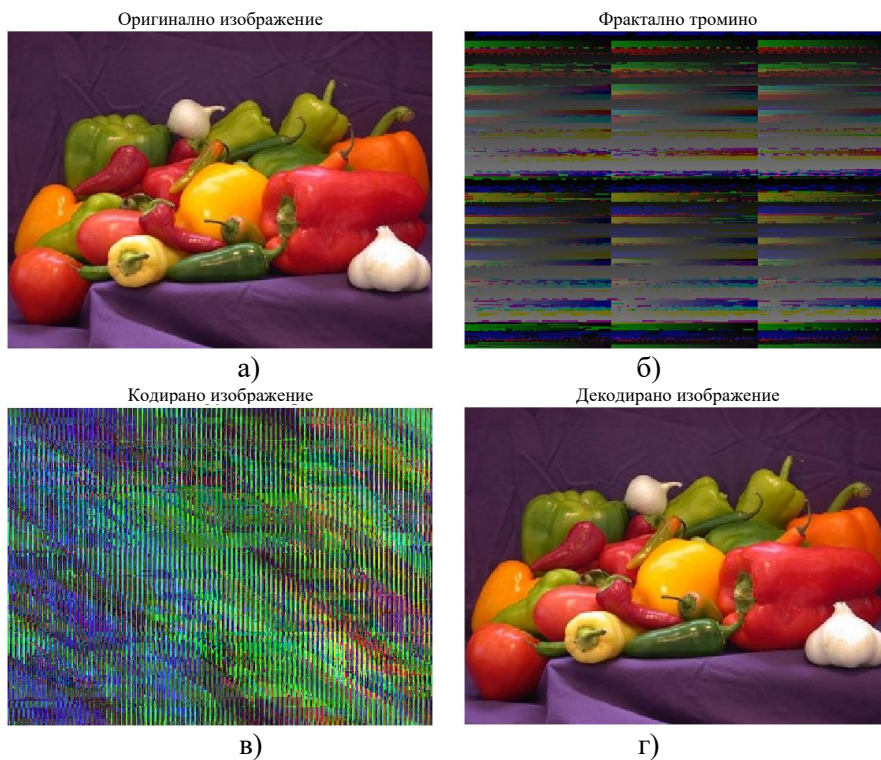
За реализиране на алгоритъма за криптиране на изображения, базиран на фрактални функции се използва хаотична синхронизационна схема между две идентични хаотични системи на Rössler по модифицирания метод базиран на линейно-нелинейна декомпозиция, подробно описан в глава 4, т. 4.2.1.

5.2.1.1 Криптиране на изображения базирано на фрактални функции с идентична синхронизация между две системи на Rössler

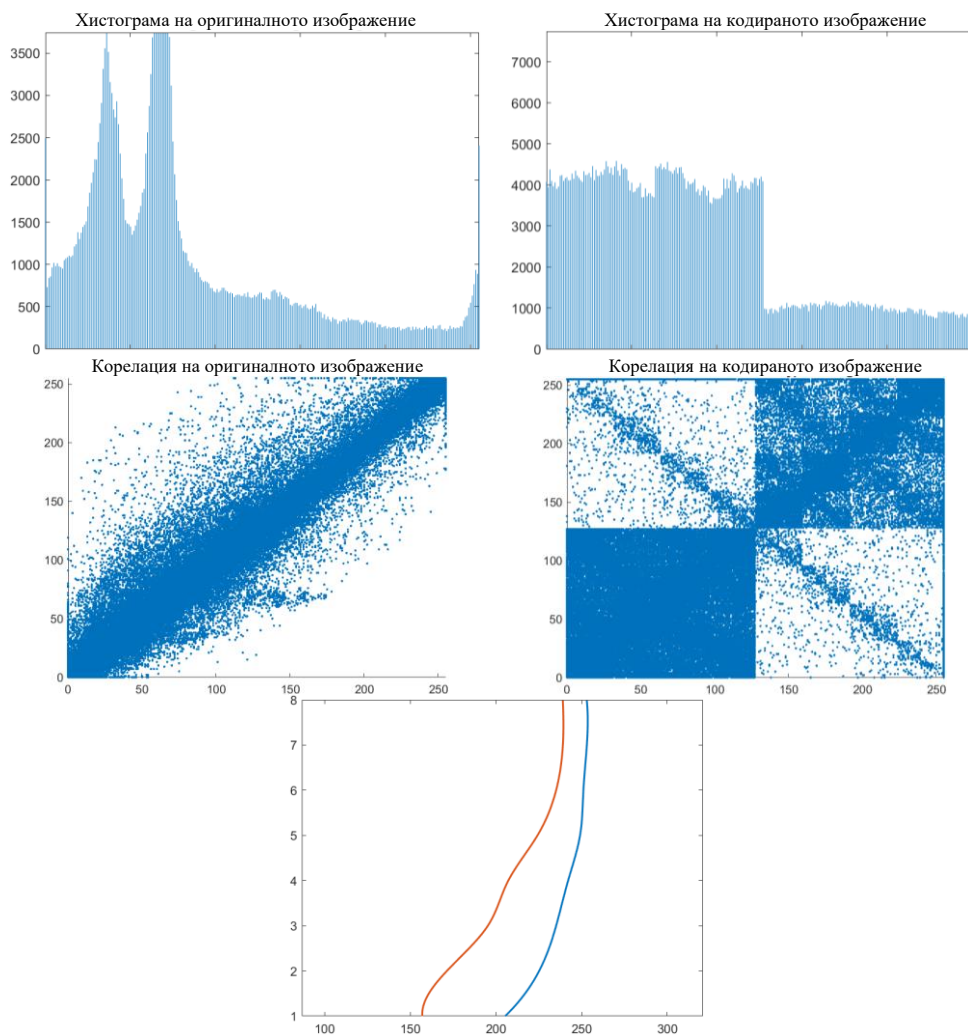
Хаотичната синхронизационна схема осигуряваща идентична синхронизация между две идентични хаотични системи на Rössler е подробно описана в глава 4, т. 4.2.1.1, като за имплементиране в криптирания алгоритъм е избран втория вариант.

Синхронизационната схема е генерирана в среда на Simulink със следните произволно избрани начални условия - за управляващата система $\mathbf{x} = [0 \ 0 \ 1]^T$, а за подчинената система – $\tilde{\mathbf{x}} = [1 \ 1 \ 0]^T$. Алгоритъмът за криптиране на изображения с идентична синхронизация, базиран на фрактални функции е реализиран в среда на Matlab, където са изведени и всички графични резултати.

На фиг. 5.28 са представени: а) Оригинално изображение, б) Фрактално *tormino*, в) Кодирано изображение и г) Декодирано изображение. На фиг. 5.29 са представени хистограмите, корелационните изображения и кривите на предпочитание за оригиналното и кодираното изображения.



Фиг. 5.28 Криптиране на изображения базирано на фрактални функции с идентична синхронизация между две системи на Rössler



Фиг. 5.29 Хистограми, корелационни изображения и криви на предпочитание за оригиналното и кодираното изображения

5.1.1 Имплементиране на хаотични синхронизационни схеми в алгоритъм за криптиране на изображения посредством дифузионна матрица

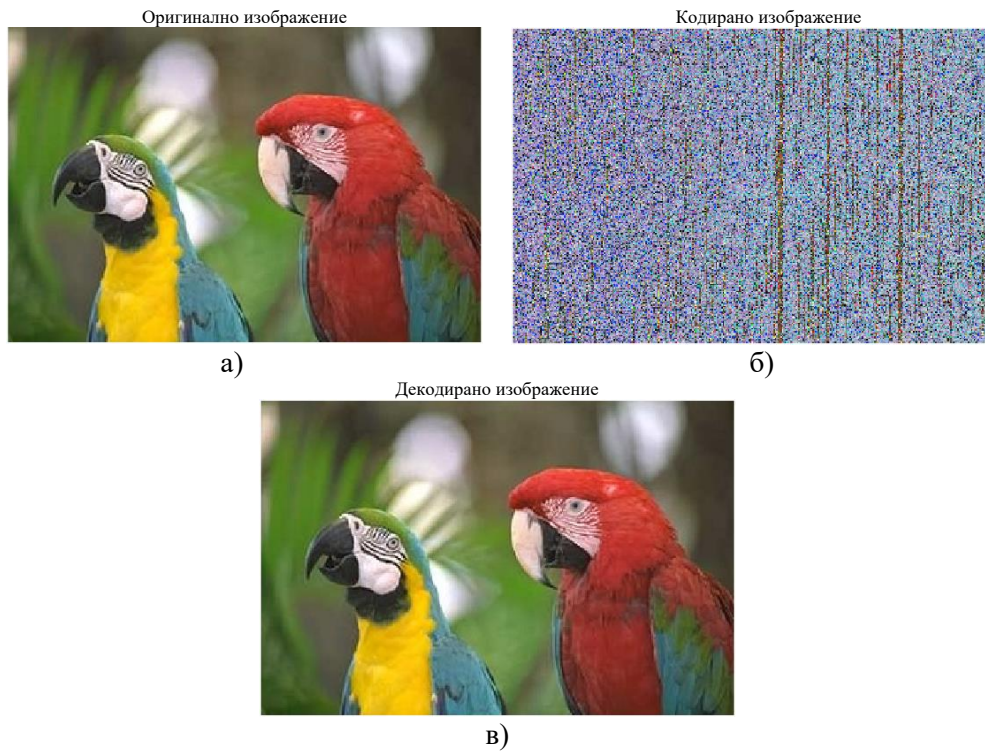
Този тип алгоритми, принадлежат към групата на алгоритми, комбиниращи трансформация на стойностите и пермутация на позицията на пикселите. Традиционната пермутационно - дифузионна архитектура се състои от два итерационни етапа. Първият етап – пермутационният, променя позицията на пикселите на изображението, но не въздейства на техните стойности. Вторият етап – дифузионният, модифицира стойностите на пикселите последователно, така че малки промени на един пиксел разпространяват промяна на стойностите на почти всички пиксели в цялото изображение. Целият пермутационно - дифузионен процес се повтаря n на брой пъти до постигане на задоволително ниво на защита. Резултатът от изпълнението на този процес е получаване на кодираща дифузионна матрица (изображение). Този тип кодиране основно се прилага за монохроматични изображения. Модификацията на тази техника за кодиране посредством хаотична синхронизационна схема се състои в използване на хаотичния сигнал във втория етап на кодирането при създаване на дифузионния ключ, което позволява отделно кодиране на изображението по трите цветови канала. Както при всички методи, генериращи ключ, и тук хаотичният сигнал може да бъде използван на много повече нива, включително за създаване на многосъставно кодиращо изображение. Процесът на декодиране е в обратна последователност на действията от кодирането, след извършване на хаотична синхронизация, без да има риск за загуба на качеството в декриптираното изображение.

За реализиране на алгоритъма за криптиране на изображения, базиран на фрактални функции, се използва хаотична синхронизационна схема между две идентични хаотични системи на Zhang-Li-Chang по модифицирания метод, базиран на линейно-нелинейна декомпозиция, подробно описан в глава 4, т. 4.2.3.

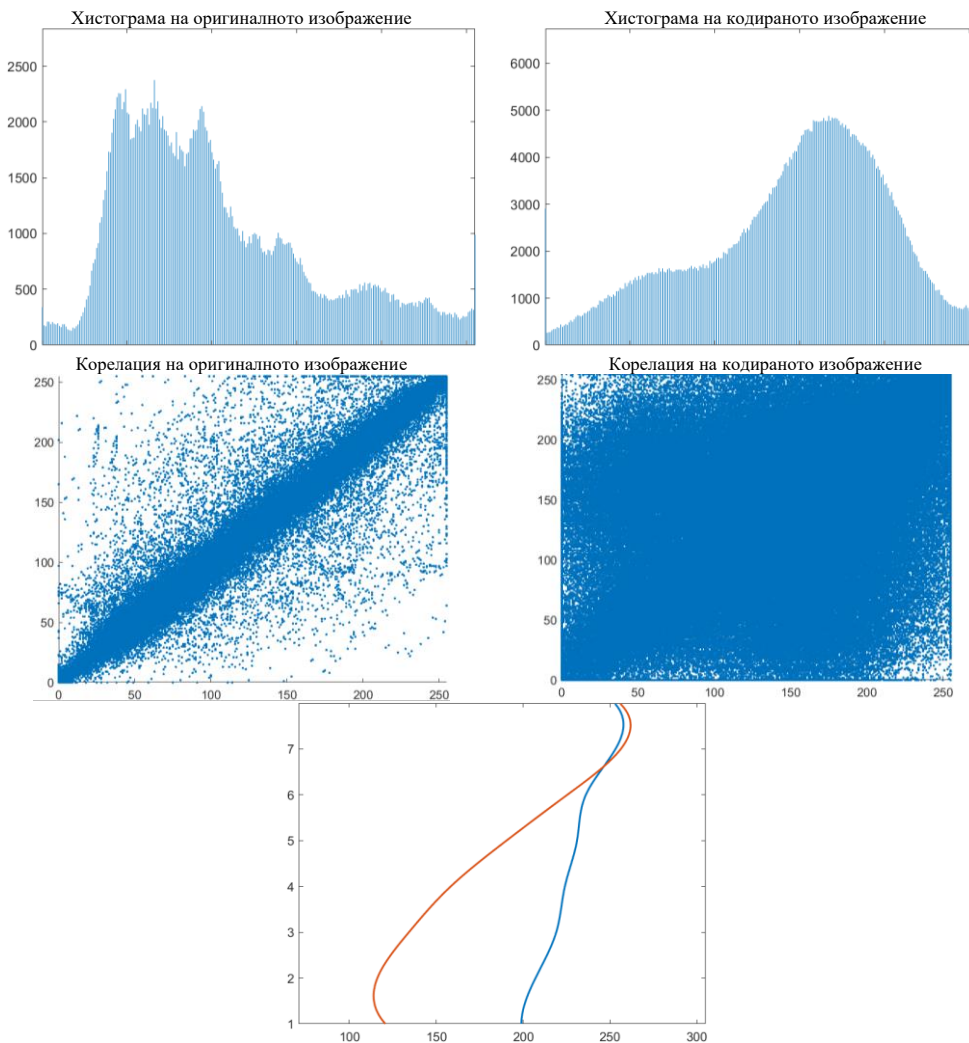
5.1.1.1 Криптиране на изображения посредством дифузионна матрица с изместена синхронизация между две системи на Zhang-Li-Chang

Избраната хаотична синхронизационна схема, осигуряваща изместена синхронизация между две идентични хаотични системи на Zhang-Li-Chang, е подробно описана в глава 4, т. 4.2.3.2. Генерирана е в среда на Simulink с произволно избрани начални условия на управляващата система - $\mathbf{x} = [-1.5 \ -1.8 \ -2.5]^T$, а на подчинената система - $\tilde{\mathbf{x}} = [1 \ 1 \ 1]^T$, като и двата набора са избрани произволно. Алгоритъмът за криптиране на изображения с изместена синхронизация посредством дифузионна матрица е реализиран в среда на Matlab, където са изведени и всички графични резултати.

На фиг. 5.47 са представени: а) Оригинално изображение, б) Кодирано изображение и в) Декодирано изображение. На фиг. 5.48 са представени хистограмите, корелационните изображения и кривите на предпочитание за оригиналното и кодираното изображения.



Фиг. 5.47 Криптиране на изображения посредством дифузионна матрица с изместена синхронизация между две системи на Zhang-Li-Chang



Фиг. 5.48 Хистограми, корелационни изображения и криви на предпочитание за оригиналното и кодираното изображения

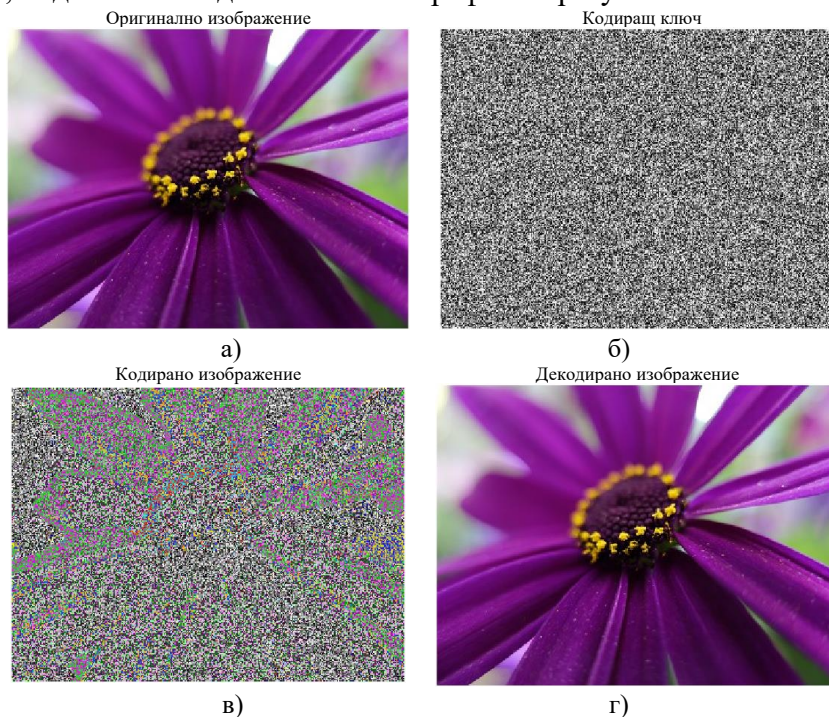
5.2.2 Имплементиране на хаотични синхронизационни схеми в OTP (One-time path) алгоритъм за криптиране на изображения

При кодирането на изображения, OTP алгоритмите представляват кодираща техника, която изисква използването на еднократен предварително споделян ключ с размер равен на този на изображението или по-голям. Тази техника се явява една от най-елементарните и най-общо представлява вдвояване на изображението с генерирания секретен ключ. Алгоритъмът е еквивалентен на метода с маскиране при кодирането на сигнали. При този тип алгоритми за постигане на високо ниво на защита се разчита на сложността на генерирания ключ. Поради тази причина, използването на хаотичен сигнал и имплементирането на хаотични синхронизационни схеми е много подходящо, предвид същността на метода. В текущата реализация хаотичният сигнал от управляващата система се използва в генериране на втори допълнителен ключ, който се комбинира с предварително генериран първичен ключ с псевдослучаен характер. Използването на хаотични сигнали в този тип алгоритми е много ползотворно, тъй като се постига условието за еднократно генериране на ключ, както и постигане на високата му степен на сложност.

За реализиране на OTP (One-time path) алгоритъма за криптиране на изображения, се използва хаотична синхронизационна схема между две идентични хиперхаотични системи на Vaidiyanathan по модифицирания метод, базиран на линейно-нелинейна декомпозиция, подробно описан в глава 4, т. 4.2.5.

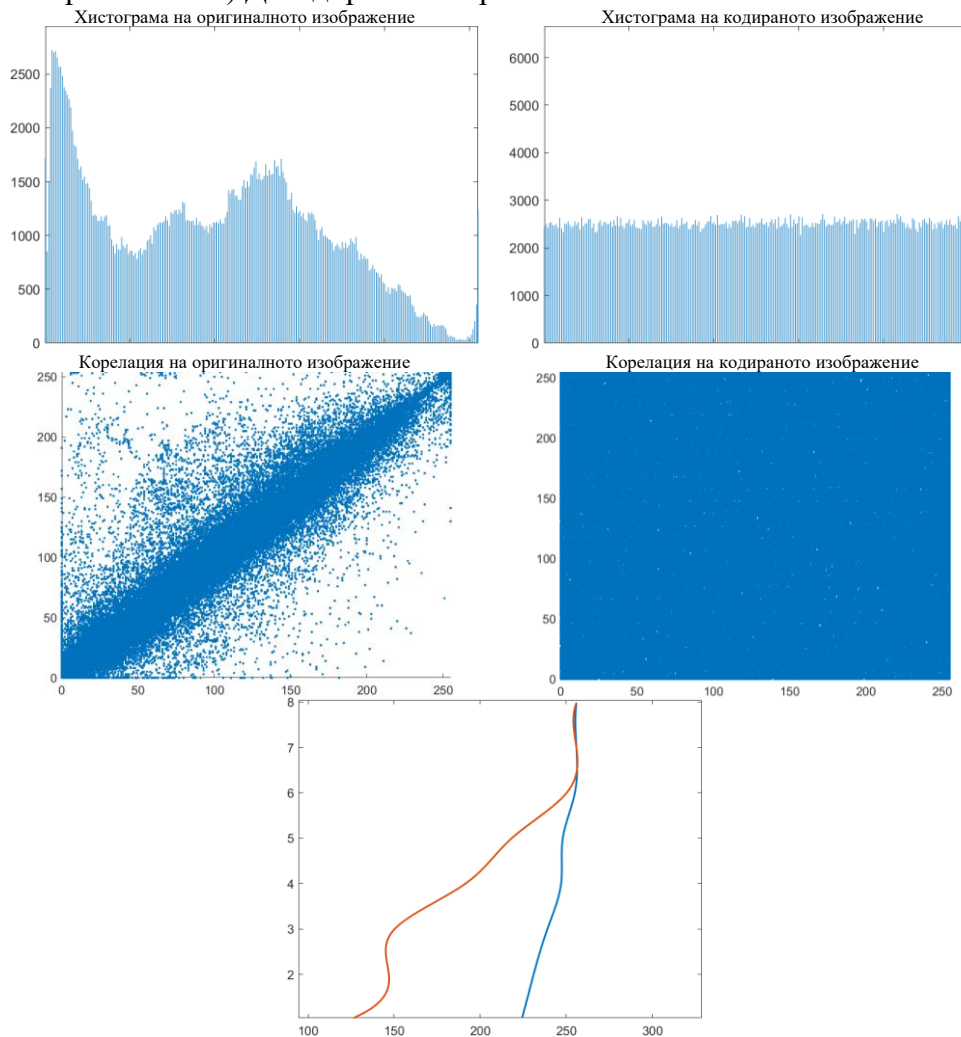
5.2.2.1 OTP (One-time path) алгоритъм за криптиране на изображения посредством идентична синхронизация между две хиперхаотични системи на Vaidiyanathan

За имплементиране в OTP алгоритъма за криптиране на изображения е избрана хаотичната синхронизационна схема, подробно описана в глава 4, т. 4.2.5.1, осигуряваща изместена синхронизация между две идентични хиперхаотични системи на Vaidiyanathan. Генерирана е в среда на Simulink с произволно избрани начални условия на управляващата система - $\mathbf{x} = [0.3 \ 0.3 \ 0.3 \ 0.3]^T$, а на подчинената система - $\tilde{\mathbf{x}} = [0 \ 0 \ 0 \ 0]^T$. OTP алгоритъмът за криптиране на изображения с идентична синхронизация е реализиран в среда на Matlab, където са изведени и всички графични резултати.



Фиг. 5.58 Криптиране на изображения посредством OTP алгоритъм с идентична синхронизация между две хиперхаотични системи на Vaidiyanathan

На фиг. 5.58 са представени: а) Оригинално изображение, б) Кодиращ ключ в) Кодирано изображение и г) Декодирано изображение.



Фиг. 5.59 Хистограми, корелационни изображения и криви на предпочитание за оригиналното и кодираното изображения

На фиг. 5.59 са представени хистограмите, корелационните изображения и кривите на предпочитание за оригиналното и кодираното изображения.

5.2.3 Анализ на получените резултати

В другите подточки на глава 5 са представени графичните интерпретации на хистограмите, корелационните изображения и кривите на предпочитание за изследваните изображения с реализираните кодиращи алгоритми. Тези изображения могат да се използват за визуален анализ и първоначално определяне на степента на защита на информацията. От изведените хистограми и корелационни изображения, могат да се получат числови резултати, които дават конкретен отговор без субективна преценка за постигнатото ниво на защита. Поради тази причина, анализът ще се извърши на базата на изчисление на информационна ентропия от получените хистограми и коефициент на корелация от получените корелационни изображения.

В таблици 5.1 и 5.2 са показани стойностите на информационната ентропия и корелацията на тестовите изображения и съответните криптирани изображения за всеки от разгледаните по-горе алгоритми, а с Δ е оказана разликата в стойностите на информационната ентропия между оригиналното и кодираното изображения.

Таблица 5.1 Числови резултати за информационната ентропия на изследваните изображения за трите реализирани кодиращи алгоритъма

	Изображение	Оригинално	Кодирано	Декодирано	Δ
Алгоритъм с фрактални функции	Lena	7.3283	7.6762	7.3283	0,3479
	Peppers	7.0692	7.7006	7.0692	0,6314
	Pout	6.2156	7.7545	6.2156	1,5389
	Baboon	7.6634	7.8250	7.6634	0,1616
Алгоритъм с дифузионна матрица	Lena	7.3283	7.6007	7.3283	0,2769
	Daffodil	6.7870	7.7662	6.7870	0,9792
	Parrot	7.4122	7.5612	7.4122	0,1490
	Cameraman	7.0706	7.6460	7.0706	0,5754
ОТР алгоритъм	Lena	7.3283	7.8191	7.3283	0,4908
	Flower	7.3961	7.7600	7.3961	0,3639
	Koala	7.8018	7.8696	7.8018	0,0678
	Drawing	2.6664	7.7667	2.6664	5,1003

Таблица 5.2 Числови резултати за корелацията на изследваните изображения за трите реализирани кодиращи алгоритъма

	Изображение	Оригинално	Кодирано	Декодирано	Δ
Алгоритъм с фрактални функции	Lena	0.9811	0.8810	0.9811	0,1001
	Peppers	0.9826	0.8342	0.9826	0,1484
	Pout	0.9796	0.8842	0.9796	0,0954
	Baboon	0.8191	0.7671	0.8191	0,0520
Алгоритъм с дифузионна матрица	Lena	0.9811	0.3907	0.9811	0,5904
	Daffodil	0.9969	0.4721	0.9969	0,5248
	Parrot	0.9735	0.3271	0.9735	0,6464
	Cameraman	0.9791	0.1754	0.9791	0,8037
ОТР алгоритъм	Lena	0.9811	0.2096	0.9811	0,7715
	Flower	0.9798	0.1877	0.9798	0,7921
	Koala	0.9114	0.1950	0.9114	0,7164
	Drawing	0.5161	0.1828	0.5161	0,3333

Анализи и изводи към Глава V

В настоящата глава са представени реализации на защитено предаване на информация по незащитен публичен канал чрез използване на сигнал от хаотични системи. Представени са три схеми на кодиране на аналогови и цифрови сигнали чрез използване на представената в глава 3 методика за постигане на комбиниран вид синхронизация. Реализираните схеми на кодиране на сигналите са базирани на класическите методи за хаотично превключване, хаотично маскиране и хаотично модулиране. Използването на комбинирания вид синхронизация повишава степента на защита на информация, като се позволява да се внедри своеобразен хаотичен ключ. Този ключ се формира както от параметрите и началните условия на хаотичната управляваща система в приемника, така и от стойностите на коефициентите на мащабиране и изместване в получения вид синхронизация. Подробно са представени и описани блок-схемите на получените комуникационни схеми като за реализирането на всяка от тях са използвани различни хаотични системи. Получените резултати за кодирани, предавани, получени и декодирани сигнали са представени графично.

Представеният в глава 4 метод за постигане на различни видове хаотична синхронизация, базиран на линейно-нелинейна декомпозиция е имплементиран в алгоритми за кодиране на изображения. Модифицирани са три актуални и често използвани алгоритъма: алгоритъм, базиран на фрактални функции, алгоритъм за криптиране на изображения посредством дифузионна матрица и ОТР алгоритъм. И трите алгоритъма се основават на използване на кодиращ ключ. Чрез имплементиране на хаотичния сигнал от управляващата система в приемника, което за всеки алгоритъм е индивидуално, се повишава сложността на кодиращия ключ, а от там и степента на защита. Модификациите на алгоритмите са описани подробно, като са показани и блок схемите на реализираните комуникационни системи. Използваният метод за синхронизация на хаотичните системи в предавателя и приемника, позволява възстановяване на предаваното изображение без загуба на качество. В реализациите са използвани различни хаотични системи, като са представени резултати за идентична, изместена и осцилираща синхронизация. Анализът за степента на защита е направен на базата на графично сравнение на хистограми, фазови портрети и криви на предпочитанията и числово, чрез таблично представяне на информационната ентропия и коефициентите на корелация на оригиналните и кодираните изображения.

С оглед решаването на задачите на дисертационния труд, извършената работа по глава 5 може да се обобщи по следния начин:

1. Описани са основните проблеми, възникващи при реализирането на защитата на информацията в комуникационните системи, както и ролята на хаоса за повишаване на степента на защита. Ясно е дефиниран проблемът с възстановяването на информацията след кодиране и предимствата на синхронизацията на хаотичните системи.
2. Реализирано е защитено предаване на цифров сигнал, посредством хаотично превключване с използване на методика за получаване на комбиниран вид синхронизация. Синтезираната синхронизационна схема е между две идентични хаотични системи на Lorenz. Комуникационната схема е реализирана в среда на Matlab/Simulink.
3. Предложена е нова архитектура на хаотично маскиране за защита на аналогов сигнал посредством методика за получаване на комбиниран вид синхронизация. В реализираната комуникационна схема информационният сигнал бива прикрит от хаотичен сигнал на управляващата система в предавателя. Възстановяването на информацията се осъществява чрез синтезираната синхронизационна схема между двете идентични хаотични системи на Zhou – Li в приемника и предавателя. Избраният конкретен вариант на комбинирана синхронизация дава достатъчно кратки продължителности на преходните процеси.
4. На база предложената методика за получаване на комбиниран вид синхронизация е реализирано хаотично кодиране на цифров сигнал в среда на Matlab/Simulink. Използваната схема на кодиране се основава на хаотично модулиране, като кодиращите сигнали се вземат от управляващата хиперхаотична система (система на Singh – Roy) в предавателя. Синтезираната синхронизационна схема позволява качествено възстановяване на предаваната информация при изключително кратки преходни процеси.
5. Реализиран е модифициран алгоритъм за кодиране на изображения, базиран на фрактални функции. Модификацията се състои в използване на сигнал от хаотична система в предавателя във фракталния модул на алгоритъма, който променя механизма за получаване на фракталното троице във фаза 1 и фаза 2 на процеса. Посредством използвания метод, базиран на линейно-нелинейна декомпозиция, се

- осъществява генериране на декодиращ ключ (фрактално троице) от подчинената система в приемника, с който изображението се възстановява. Модифицираният алгоритъм е изследван с трите вида хаотична синхронизация, осигурени от метода.
6. Модифициран е алгоритъм за кодиране на изображения, базиран на генериране на дифузионна матрица. Хаотичният сигнал на управляващата хаотична система в предавателя се използва по-обширно във формирането на кодиращото изображение (дифузионната матрица). Освен като информационен носител за генериране, хаотичният сигнал се използва и в операциите по получаване на кодиращия ключ. След реализиране на един от трите вида синхронизация, получени посредством метод базиран на линейно-нелинейна синхронизация се генерира декодиращ ключ за възстановяване на изображението.
 7. Предложена е нова архитектура на стандартен ОТР алгоритъм за кодиране на изображения. Реализацията се състои в генериране на допълнителен хаотичен (динамичен) ключ, който заедно със стандартния статичен ключ формират общия кодиращ ключ. Кодираното изображение се декодира в приемника отново чрез осъществяване на хаотична синхронизация между двете хаотични системи и последващо генериране на декодиращ ключ.
 8. Представени са резултати за набор от често използвани тестови изображения, използвани за криптиране. Степента на защита се анализира на първо място графично, чрез сравнение на хистограми, фазови портрети и криви на предпочитанията и числово чрез изчисление на информационната ентропия и коефициентите на корелация, за оригиналните и кодираните изображения по трите модифицирани алгоритъма.

Заклучение

Теорията на хаоса и в частност синхронизирането на хаотични системи са обект на засилен научен интерес през последните няколко десетилетия. Въпреки нестихващият интерес към областта, все още съществуват много неизследвани закономерности и явления и липсва универсален подход за синхронизация, които да може без ограничения да се използва за всяка конкретна задача. Именно поради тази причина, в дисертационният труд се разглежда задачата за синхронизация на хаотични системи и прилагането ѝ в комуникационни системи за защитено предаване на информация.

Накратко извършената работа по дисертационният труд може да се обобщи в следното:

- Представен е подробен обзор и класификация на видовете хаотични системи
- Разгледани са основните методи и видове хаотична синхронизация
- Разработена е методика за постигане на специфичен комбиниран вид синхронизация, базирана на втория метод за устойчивост на Ляпунов
- Предложен е метод за хаотична синхронизация, осигуряващ различни видове неидентично синхронно поведение на базата на линейно-нелинейна декомпозиция
- Реализирани са комуникационни схеми за защитено предаване на аналогови и цифрови сигнали, чрез прилагане на комбинираният вид синхронизация
- Модифицирани са три актуални алгоритъма за кодиране на изображения, посредством разработеният метод за хаотична синхронизация

На база проведени изследвания върху приложимостта на синхронизационните схеми, може да се заключи, че подходите предлагат висока степен на защита на информацията поради постигнатото сложно синхронно поведение между управляващата и подчинената хаотични системи.

СПИСЪК НА ОЗНАЧЕНИЯТА И СЪКРАЩЕНИЯТА

CR	Complete Replacement (пълно заместване)
CSK	Chaotic shift key (Модулация с хаотична манипулация)
DCT	Discrete cosine transform (Дискретна косинусова трансформация)
OTP	One-time path алгоритъм
OW	One-way Coupling (еднопосочно свързване)
PC	Метод на Pecora-Carroll

ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

В дисертационния труд са постигнати следните научни, научно-приложни и приложни приноси:

1. Разработена и изследвана е методика за постигане на комбиниран вид синхронизация, базиран на втори метод за устойчивост на Ляпунов, съчетаващ мащабирана, изместена и хибридна синхронизация. Методиката дава възможност за множество комбинации, както и произволен избор на коефициентите на мащабиране и изместване и се прилага успешно при синхронизационни схеми с хаотични и хиперхаотични системи.
2. Разработен и изследван е модифициран метод основан на метода на линейно-нелинейната декомпозиция, при който чрез прилагане на допълнително управление към подчинената система, се гарантира постигането на повече от един вид хаотична синхронизация при един и същи синтез на връзка между подлежащите на синхронизация системи. Метода позволява точен анализ на устойчивостта на конкретната схема и дава възможност за реализиране на множество варианти на декомпозиция водещи до устойчива синхронизация. Методът се прилага успешно при синхронизационни схеми с хаотични и хиперхаотични системи.
3. Предложена е нова класификационна схема на по-известните към момента хаотични системи основана на вида, размерността и физическата реализуемост на математическите модели.
4. Разработена е комуникационна схема за защитено предаване на цифров сигнал, посредством хаотично превключване, използваща синхронизационна схема, базирана на методиката за получаване на комбиниран вид синхронизация. Комуникационна схема е изследвана в среда на Matlab/Simulink.
5. Предложена е нова архитектура на хаотично маскиране в комуникационна схема за защитено предаване на аналогов сигнал, посредством синхронизационна схема, базирана на методиката за получаване на комбиниран вид синхронизация. Комуникационна схема е изследвана в среда на Matlab/Simulink.
6. Реализирано е хаотично модулиране на цифров сигнал, чрез използване на синхронизационна схема, базирана на методиката за получаване на комбиниран вид синхронизация. Така реализираната комуникационна схема постига качествено възстановяване на предаваната информация. Комуникационна схемата е изследвана в среда на Matlab/Simulink.
7. Модифициран е алгоритъм за кодиране на изображения базиран на фрактални функции. Модификацията се състои в използване на сигнал от хаотична система в предавателя във фракталния модул на алгоритъма, който променя механизма за получаване на фракталното тромино. Модифицираният алгоритъм е изследван при синтез на идентична, изместена и осцилираща хаотична синхронизация чрез предложения метод, базиран на линейно-нелинейна декомпозиция.
8. Разработен е модифициран алгоритъм за кодиране на изображения базиран на генериране на дифузионна матрица. Хаотичният сигнал на управляващата хаотична

система в предавателя се използва в ролята на информационен носител за генериране на изображение и в операциите по получаване на основния кодиращ ключ. Алгоритъмът е изследван при синтез на идентична, изместена и осцилираща хаотична синхронизация чрез предложения метод, базиран на линейно-нелинейна декомпозиция.

9. Предложена е нова архитектура на стандартен ОТР алгоритъм за кодиране на изображения, базирана на модификация на алгоритъма, чрез генериране на допълнителен хаотичен (динамичен) ключ, който заедно със стандартния статичен ключ формират общия кодиращ ключ. Алгоритъмът е изследван при синтез на идентична, изместена и осцилираща хаотична синхронизация чрез предложения метод, базиран на линейно-нелинейна декомпозиция.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

- [1] Чантов, Д., **Х. Стойчева**, *Синхронизация и антисинхронизация на нова хаотична система със специфична нелинейност*. Международна конференция Техсис'2016, 26-28.05.2016, Пловдив, България, стр. II-55 - II -60.
- [2] Чантов, Д., **Х. Стойчева**, *Проектиране на хаотични синхронизационни системи с различни видове идентична и неидентична синхронизация на основата на метод с линейно-нелинейна декомпозиция*. Международна конференция Техсис'2016, 26-28.05.2016, Пловдив, България, стр. II-61 - II -66
- [3] **Стойчева, Х.**, Д. Чантов. *Хибридна синхронизация между хиперхаотични системи на Wang от 4-ти ред*. Сборник доклади от Международна научна конференция UNITECH'2016, 18-19.11.2016, Габрово, България, Том I, стр. 315-321.
- [4] **Стойчева, Х.**, Д. Чантов. *Синтез на хаотични синхронизационни схеми с изместена синхронизация*. Сборник доклади от Международна научна конференция UNITECH'2016, 18-19.11.2016, Габрово, България, Том I, стр. 322-327.
- [5] **Стойчева Х.**, Чантов Д., „ *Проектиране на синхронизационни схеми на хаотични системи с изменящи се параметри на основата на втория метод за устойчивост на Ляпунов*“, Годишник на Технически университет – София, том 67, книга 2, ISSN 1311-0829, 2017, pp 297-306.
- [6] Чантов, Д., **Х. Стойчева**. *Проектиране на хаотична синхронизационна система, съчетаваща антисинхронизация и изместена синхронизация*. Сборник доклади от Международна научна конференция UNITECH 2017, ТУ - Габрово, България, стр. 317-323. ISSN 1313-230X
- [7] **Стойчева Х.**, *Глобална синхронизация на три идентични хаотични системи*. Сборник доклади от Международна научна конференция UNITECH 2017, ТУ - Габрово, България, стр. 342-346. ISSN 1313-230X
- [8] Чантов, Д., **Х. Стойчева**, *Получаване на осцилираща синхронизация между две хаотични системи на Van der Pol*, Известия на ТУ-Габрово, Vol. 59, 2019, стр. 92-96.
- [9] **Стойчева Х.**, Д. Чантов, *Проектиране на хаотична синхронизационна система, съчетаваща мащабирана, изместена и хибридна синхронизация*, Сборник доклади от Международна научна конференция "Автоматика и информатика" 2019, София, 2019, стр.39-42, ISSN 1313-1850
- [10] **Стойчева Х.**, Д. Чантов, *Синтез на синхронизационна схема с мащабирана синхронизация между хиперхаотични системи от 4-ти ред*, Сборник. доклади от Международна научна конференция UNITECH '19, Габрово, 2019, стр.258-262, ISSN 1313-230X
- [11] **Stoycheva, H.**, D. Chantov. *Design of chaotic synchronization system combining projective, marginal and hybrid synchronization with application to image encryption*. ICAI2020, IEEE, 2020, pp. 1-6.

SYNTHESIS AND ANALYSIS OF CHAOTIC SYNCHRONIZATION SYSTEMS

Author: Hristina Svetoslavova Stoycheva

Keywords: chaos, chaotic synchronization, secure communications, image encryption.

ABSTRACT

The subject of this dissertation are the chaotic synchronization schemes. Synchronization of chaotic systems is applied to tasks for which the complex dynamic behavior of a system is an advantage and the goal is for two or more chaotic systems to adjust their dynamics to each other by means of appropriately synthesized control between them.

Sensitivity to initial conditions and unpredictability make chaotic systems very suitable for building cryptographic schemes with one-way connection and public key. In chaos-based secure communication schemes, the information signals are masked or modulated by the chaotic signal of the control system in the transmitter and the generated coded signals are sent to the respective receiver via a public (unprotected) channel. To restore the original information signals, perfect and stable chaotic synchronization is needed. Therefore, the recovery of the information signals requires, the chaotic signal generated in the receiver, after the synchronization process, to be an exact copy of the one used in the transmitter. For this reason, the key technique throughout the process is precisely the synchronization of chaotic systems.

The contributions of the dissertation have scientific and practical character and these are as follows:

- A detailed overview and classification of the types of chaotic systems, is presented;
- A methodology for achieving a specific combined type of synchronization based on the second Lyapunov stability law is developed;
- A method for chaotic synchronization is proposed, providing different types of non-identical synchronous behavior based on linear-nonlinear decomposition;
- Communication schemes for secure transmission of analog and digital signals are accomplished, by applying the combined type of synchronization;
- Three 'up to date' image coding algorithms have been modified, using the developed method for chaotic synchronization

Based on research on the applicability of synchronization schemes, it can be concluded that the approaches offer a high degree of information protection due to the achieved complex synchronous behavior between the master and the slave chaotic systems.

Съдържание

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД.....	3
Актуалност на проблема	3
Цел и задачи на дисертационния труд.....	3
Методи на изследване	4
Научна новост	4
Приложимост	5
Апробация на дисертационния труд.....	5
Структура и обем на дисертационния труд	5
Глава I: Теоретични основи на хаотичните системи.....	6
1.1 Основни понятия от теория на нелинейните системи.....	6
1.2 Методи за доказване хаотичността на една нелинейна система.....	6
1.3 Видове и класификация на хаотичните системи	6
1.4 Пример за хаотична система - Система на Wang.....	7
Анализи и изводи към Глава I.....	7
Глава II: Синхронизация на хаотични системи	8
2.1 Общи определения и термини за хаотична синхронизация	8
2.2 Доказване на синхронизацията.....	9
2.3 Методи за синхронизация на хаотични системи	10
2.3.1 Декомпозиционни методи.....	10
2.3.1.1 Метод на Pecora-Carroll.....	10
2.3.2 Методи с обратна връзка.....	11
2.3.2.1 Метод с еднопосочно свързване	11
2.4 Видове хаотична синхронизация.....	11
2.5 Приложение на хаотичната синхронизация в защитени комуникации	12
Анализи и изводи към Глава II.....	13
Глава III: Методика за постигане на комбиниран вид синхронизация	13
3.1 Комбиниран вид синхронизация	13
3.2 Изследване на представения комбиниран вид синхронизация	14
3.2.1 Хаотична система на Lorenz	15
3.2.1.1 Изследване на конкретна комбинация	15
3.2.1.2 Таблично представяне на резултатите.....	17
Анализи и изводи към Глава III	19
Глава IV: Метод за постигане на специфични видове неидентична синхронизация на база линейно – нелинейна декомпозиция	20
4.1 Формулировка на метода.....	20
4.2 Изследване на метода	21
4.2.1 Изследване на различни видове синхронизация между две системи на Rössler по модифицираният метод на линейно-нелинейна декомпозиция	21

4.2.1.1	Идентична синхронизация.....	22
4.2.1.2	Изместена синхронизация	23
4.2.1.3	Осцилираща синхронизация.....	24
	Анализ и изводи към Глава IV	26
	Глава V: Приложение на хаотични синхронизационни схеми в комуникационни системи за защитено предаване на информация.....	26
5.1	Приложение на хаотични синхронизационни схеми в защитено предаване на аналогови и цифрови сигнали.....	27
5.1.1	Предаване на цифров сигнал чрез хаотично превключване.....	27
5.1.2	Предаване на цифров сигнал чрез хаотично маскиране.	29
5.1.3	Предаване на цифров сигнал чрез хаотично модулиране.....	31
5.2	Приложение на хаотични синхронизационни схеми в криптиране на изображения.....	33
5.2.1	Имплементиране на хаотични синхронизационни схеми в алгоритъм за криптиране на изображения, базиран на фрактални функции	34
5.2.1.1	Криптиране на изображения базирано на фрактални функции с идентична синхронизация между две системи на Rössler	34
5.1.1	Имплементиране на хаотични синхронизационни схеми в алгоритъм за криптиране на изображения посредством дифузионна матрица.....	36
5.1.1.1	Криптиране на изображения посредством дифузионна матрица с изместена синхронизация между две системи на Zhang-Li-Chang.....	36
5.2.2	Имплементиране на хаотични синхронизационни схеми в OTP (One-time path) алгоритъм за криптиране на изображения.....	38
5.2.2.1	OTP (One-time path) алгоритъм за криптиране на изображения посредством с идентична синхронизация между две хиперхаотични системи на Vaidyanathan	38
5.2.3	Анализ на получените резултати.....	39
	Анализ и изводи към Глава V	40
	Заключение.....	42
	СПИСЪК НА ОЗНАЧЕНИЯТА И СЪКРАЩЕНИЯТА.....	43
	ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД.....	43
	СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД.....	45
	ABSTRACT	46
	СЪДЪРЖАНИЕ	47