CRIPTOGRAFIA BASEADA EM CAOS: APLICAÇÃO USANDO UM SISTEMA HIPERCAÓTICO

DANIEL VASCO ROCHA

TRABALHO DE CONCLUSÃO DE CURSO EM ENGENHARIA ELÉTRICA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

CRIPTOGRAFIA BASEADA EM CAOS: APLICAÇÃO USANDO UM SISTEMA HIPERCAÓTICO

DANIEL VASCO ROCHA

Orientador: PROF. DR. JOSÉ ALFREDO RUIZ VARGAS

TRABALHO DE CONCLUSÃO DE CURSO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO - VR672C/2019
BRASÍLIA-DF, 4 DE DEZEMBRO DE 2019.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

CRIPTOGRAFIA BASEADA EM CAOS: APLICAÇÃO USANDO UM SISTEMA HIPERCAÓTICO

DANIEL VASCO ROCHA

TRABALHO DE CONCLUSÃO DE CURSO ACADÊMICO SUBMETIDO AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ENGENHEIRO ELETRICISTA.

APROVADA POR:

Prof. Dr. José Alfredo Ruiz Vargas
Orientador ENE/UnB

Prof. Dr. Renato Alves Borges
Membro ENE/UnB

Prof. Dr. Guilhermo Alvarez Bestard
Membro - FGA/UnB

BRASÍLIA, 4 DE DEZEMBRO DE 2019.

FICHA CATALOGRÁFICA
DANIEL VASCO ROCHA
Criptografia baseada em caos: aplicação usando um sistema hipercaótico
2019xv, 43p., 201x297 mm
(ENE/FT-UnB/FT/UnB, Engenheiro Eletricista, Engenharia Elétrica, 2019)
Trabalho de Conclusão de Curso - Universidade de Brasília
Faculdade de Tecnologia - Departamento de Engenharia Elétrica

REFERÊNCIA BIBLIOGRÁFICA

ROCHA, D. V. Criptografia baseada em caos: aplicação usando um sistema hipercaótico. Trabalho de Conclusãode Cursoem Engenharia Elétrica, Publicação VR672c/2019, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2019. 43p.

CESSÃO DE DIREITOS

AUTOR: Daniel Vasco Rocha
TÍTULO: Criptografia baseada em caos: aplicação usando um sistema hipercaótico.
GRAU: Engenheiro Eletricista ANO: 2019

É concedida à Universidade de Brasília permissão para reproduzir cópias deste trabalho de conclusão de curso e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor se reserva a outros direitos de publicação e nenhuma parte deste trabalho de conclusão de curso pode ser reproduzida sem a autorização por escrito do autor.

Daniel Vasco Rocha
Cln 411 Bloco C, Asa Norte, Brasília

Agradecimentos

Acima de tudo agradeço a Deus por ter proporcionado tudo na minha vida.

Um grande agradecimento especial aos meus pais Claudionor Vasco Silva e Gislene Gislene Oliveira Rocha pelo infinito amor aos seus filhos e por nunca me deixarem desistir.

Também agradeço as minhas irmãs Ana Claudia Vasco e Marina Vasco pelo icentivo e fraternidae . As minhas sobrinhas Cecília Vasco, Júlia Vasco e Larissa Rocha por me mostrarem o mais intenso sentimento.

A minha namorada Thamires Pereira Pinheiro pelo nosso amor e por me incentivar nos momentos difíceis.

Aos amigos Augusto Cesar Nobre de Castro, João Luiz Santana Nascimento , Lucas Moura gomes e Vanessa Lacerda de Menezes pelo companheirismo e aprendizado juntos.

Agradeço Prof. José Alfredo Ruiz Vargas e ao Doutorando Kevin Herman Muraro Gularte por ter me proporcionado esta oportunidade.

Muito Obrigado!

Resumo

Neste trabalho se propõe um esquema para telecomunicação segura baseado na sincronização de um sistema nonodimensional hipercaotico e analise de Lyapunov. Ao contrário da maioria dos esquemas usualmente encontrados na literatura, o esquema proposto requer apenas que o controle atue em uma das equações de estado do sistema escravo. Foi verificada matematicamente a convergência do erro de sincronização para um conjunto compacto arbitrário, permitindo-se obter um erro convergente a uma vizinhança da origem.

Com um circuito caótico transmissor (ou mestre) codifica-se o sinal (ou mensagem) e com outro circuito caótico receptor (ou escravo) recupera-se a mensagem. O esquema proposto tem como vantagens ser robusto contra perturbações (internas e externas) e ser estruturalmente simples, quando comparado com as propostas existentes na literatura, o que é importante, uma vez que leva a redução de custos quando implementado utilizando eletrônica analógica. Para validar a robustez e simplicidade do esquema proposto, simulações computacionais utilizando software MATLAB/Simulink foram realizadas.

Palavras-chave - controle não linear, hipercaótico, Teoria de Lyapunov, sistemas seguro, telecomunicação.

Keywords - nonlinear, hypercytotic control, Lyapunov theory, secure telecommunication, systems.

Abstract

This work proposes a scheme for secure telecommunication based on the synchronization of a hyperchaotic system and Lyapunov analysis. Unlike most schemes usually found in the literature, the proposed scheme only requires that the control act on one of the slave state equations. The convergence of the synchronization error to an arbitrary compact set was verified mathematically, allowing a convergent error to be arbitrarily small neighborhood of the origin. With a transmitting (or master) chaotic circuit the signal (or message) is encoded and with another receiving (or slave) chaotic circuit the message is retrieved. The proposed scheme has the advantages of being robust against disturbances (internal and external) and being structurally simple when compared to the existing proposals in the literature, which is important as it leads to cost savings when implemented using analog electronics. To validate the robustness and simplicity of the proposed scheme, computer simulations using MATLAB/Simulink software were performed.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

Símbolo	Descrição
$\forall$	Para qualquer que seja
$\| \quad \|$	Norma
$\Rightarrow$	Implica que
$\exists$	Existe
$\in$	É elemento de
$\mathbb{R}$	Conjunto dos números reais
∞	Infinito
$_s$	"Subscrito" Escravo
$_m$	"Subscrito" Mestre
$*$	"Sobrescrito"Ponto de equilíbrio
$-$	"Sobrescrito" Limitante superior

Capítulo 1

Introdução

1.1 Introdução

A comunicação de uma maneira geral sempre foi foco de estudo, e quando se trata de comunicação segura em especial, aumenta-se o cuidado, pois, agora a proteção de dados sigilosos deve ser levada em consideração. A comunicação no campo de sistemas caóticos possui aplicações em diversas áreas da ciência, biologia, geografia e entre outros meios de tecnologia e suas aplicações estão sendo pesquisadas corriqueiramente (AKEMANN; BURDA; KIEBURG, 2019), (CHAI et al., 2019), (GONG et al., 2019), (TLELO-CUAUTLE et al., 2014), (TREJO-GUERRA et al., 2013), (VARAN; AKGUL, 2018).

A dinâmica caótica nos seus primórdios foi considerada prejudicial em grande parte das implementações nas engenharias, ela era mais utilizada para auxiliar algumas teorias da física, química e biologia. A inovação do caos foi estudada por Poincaré no final do século XIX e hoje é usada para descrever sistemas dinâmicos determinísticos extremamente sensíveis a condições iniciais quando esses são aperiódicos (STROGATZ, 2018). Devido ao caos ter uma imprevisibilidade no seu comportamento, a comunidade acadêmica começou a investir nesse tipo de tecnologia para a comunicação segura (PECORA; CARROLL, 1990) e (TANG; MEES; CHUA, 1983). Por exemplo, em (TANG; MEES; CHUA, 1983), foi possível constatar uma intuição entre a sincronização e o caos através de experimentos com aparelhos eletrônicos. Já em (PECORA; CARROLL, 1990), pode-se ver uma metodologia para sincronização do caos. Quando dois ou mais sistemas caóticos se ajustam em uma sintonia em que um sistema caótico convergirá para valores próximos ao do outro sistema caótico fala-se de sincronização, a qual está em vigor desde os anos 90. Existem muitos tipos de sincronização do caos, incluindo a sincronização completa, sincronização por ruído, sincronização projetiva, sincronização por atraso etc.. vide (BOCCALETTI et al., 2002), (FENG et al., 2019), (HASLER, 1998), (JAKIMOSKI; KOCAREV, 2001), (MATOUK; ELSADANY, 2014), (OUANNAS; AZAR; VAIDYANATHAN, 2017), (WANG; ZHANG; FAN, 2017). Com um circuito caótico transmissor (ou mestre) codifica-se o sinal (ou mensagem) e com outro circuito caótico receptor (ou escravo) recupera-se a mensagem. Um diferencial deste trabalho é que outras metodologias de sincronização exemplificadas na literatura anteriormente apresentam limitações visto que para fazer a sincronização eles precisam ter o controle em todas as equações de estado do sistema caótico em questão. Ou seja, adiciona-se uma atuação em cada uma das equações diferenciais. Outro empecilho consiste em que os algoritmos de sincronização raramente consideram a presença de distúrbios. Quando consideram-se distúrbios, como por exemplo, em (YANG; ZHU, 2013), que prevê um distúrbio inerente aos multiplicadores de sinal, a solução se torna complexa, pois requer um observador para fazer o controle corretamente.

Levar em conta distúrbios no sinal codificado que podem surgir devido às interferências de qualquer natureza foi de grande importância para este trabalho. Nele foram implementadas análises que possuem incertezas (por exemplo tolerâncias dos componentes usados na implementação das equações via eletrônica analógica). Futuramente, buscar-se a implementação dos circuitos eletrônicos que contenham tais incertezas. Existem três formas geométricas para a representação da dinâmica dos sistemas hipercaóticos (VARAN; AKGUL, 2018): quando se tem apenas um expoente de Lyapunov positivo a forma geométrica é um segmento de linha, quando tem-se dois expoentes a forma geométrica parece um segmento de área, a última quando se tem três expoentes de Lyapunov a forma geométrica parece um elemento de volume. Os sistemas hipercaóticos, assim como o sistema que é o foco deste trabalho (WANG, P. et al., 2011), apresentam mais complexidade do que um sistema caótico.

O primeiro sistema hipercaótico apresentado na literatura foi o sistema Rossler (ROSSLER, 1979) que consiste em um sistema quadridimensional. Para ser considerado hipercaótico, é preciso ser um sistema maior que um tridimensional, ou seja, no mínimo ter quatro equações de estado e ter pelo menos dois expoentes de Lyapunov positivos (MUKHERJEE; PORIA, 2012). O sistema quadridimensional essencial de Lorenz (JIA, 2007) é contribuinte direto da criação do sistema monodimensional que é utilizado neste trabalho, como pode ser concluído de (WANG, P. et al., 2011). Outros sistemas quadridimensional relevantes são: Chen (WEI et al., 2012), circuito de Chua (BARBOZA, 2008) e (THAMILMARAN; LAKSHMANAN; VENKATESAN, 2004) , Rikitake (QI et al., 2008), Qi (VAIDYANATHAN; VOLOS; PHAM, 2015), Lu (JIA; CHEN; QI, 2011) e financeiro (KAI et al., 2017). Diversos sistemas hipercaóticos foram publicados recentemente na literatura em especial, a partir de 2018, tem-se, quadridimensional (LI; FAN et al., 2019) e (SABAGHIAN; BALOCHIAN, 2019) , pentadimencional (UMOH; TOLA, 2018), (WANG, R. et al., 2018) e (ZHANG, F. et al., 2018) , hexadimencional (MEZATIO et al., 2019), (AL-OBEIDI; AL-AZZAWI, 2018), (SINGH; ROY, 2018),(WANG, J. et al., 2019) e (YI et al., 2018) , heptadimencional (VARAN; AKGUL, 2018) e (YANG; ZHU; YANG, 2018).

Em conjunto com os esquemas de comunicação segura, encontram-se controladores baseados na teoria de estabilidade de Lyapunov para extinguir ou duplicar proporcionalmente o caos. Pode-se citar algumas técnicas como controle ativo, controle de modo deslizante e controle adaptativo (HUA; GUAN, 2004), (VAIDYANATHAN, 2014) e (VAIDYANATHAN; SAMPATH, 2012) são alguns métodos usados para controlar esses sistemas. Esses métodos também são utilizados para a sincronização dos sistemas hipercaóticos.

1.2 Justificativa

Motivado pelos fatos apresentados anteriormente, neste trabalho é proposto um sistema para comunicação segura baseado em um sistema hipercaótico subatuado (WANG, P. et al., 2011) e na teoria de estabilidade de Lyapunov.

Mais precisamente, este trabalho é motivado pela necessidade de implementar um sistema de comunicação seguro no qual o sinal transmitido não poderá ser decodificado por terceiros. Além disso, a da robustez, o baixo custo e a praticidade aprimoradas, em relação ao que existe na literatura, são motivação complementares.

Cabe ressaltar que as principais peculiaridades do sistema proposto consistem em:

- O esquema é robusto uma vez que considera distúrbios limitados em todos os estados para análise de estabilidade ao contrário de (BOWONG, 2004).
- Ao contrário de (AKEMANN; BURDA; KIEBURG, 2019) no sincronizador proposto somente é preciso a atuação em um estado dentre os nove existentes.
- O sincronizador é estruturalmente simples já que não precisa de observadores adaptativos, ao contrário de(MATOUK; ELSADANY, 2014), (WANG; ZHANG; FAN, 2017).

1.3 Objetivo Geral

O principal objetivo desse trabalho é apresentar um sistema de comunicação baseado em um sistema hipercaótico nonodimensional em que é possível criptografar uma mensagem de áudio, de voz ou de dados, codificando e decodificando a mensagem sigilosa que se deseja transmitir, com um transmissor (mestre) e outro receptor (escravo), através através de um método específico de sincronização de sistemas caóticos.

1.4 Objetivos específicos

O trabalho tem como objetivo específico propor um sistema de comunicação segura baseada em caos, um sincronizador (controlador), um transmissor (mestre) e um receptor(escravo).

E também como objetivo específico apresentar a prova matemática do erro de sincronização e mostrar através de simulações que a sincronização de fato funciona para um sistema especifico hipercaótico.

1.5 Organização do trabalho

O trabalho está organizado da seguinte forma

- Capítulo 1: Encontra-se o estado da arte e a motivação.
- Capítulo 2: : Apresentam-se as definições e conceitos fundamentais para compreensão desse trabalho.
- Capítulo 3: Formula-se a dinâmica do erro a partir da teoria de Lyapunov.
- Capítulo 4: Foram validados os resultados satisfatórios da criptografia caótica através de simulações exaustivas usando software Matlab/Simulink.
- Capítulo 5: Encontram-se as principais conclusões desta monografia.

Capítulo 2

Definições e conceitos

Neste capitulo apresentam-se e discutem-se as definições e conceitos fundamentais para a compreensão do trabalho. Um resumo de técnicas e definições essenciais retirados de (BOCCALETTI et al., 2002), (CUOMO; OPPENHEIM, 1993), (CUOMO; OPPENHEIM; STROGATZ, 1993) (IOANNOU; SUN, 2012), (JOVIC, 2011), (KHALIL, 2002), (PECORA; CARROLL, 1990), (STROGATZ, 2018), (VARAN; AKGUL, 2018) e (YANG, 2004) são introduzidos incluindo: sistemas não lineares, sistemas caóticos, teoria da estabilidade de Lyapunov e comunicação segura baseada em caos.

2.1 Sistemas não lineares

Os conceitos apresentados a seguir foram retirados de (KHALIL, 2002). Considere um sistema dinâmico que seja composto e modelado por um número finito de equações diferenciais ordinárias acopladas da seguinte forma:

$$\begin{aligned} \dot{\mathrm{x}}_1 &= f_1\left(t, x_1, \ldots, x_n, u_1, \ldots, u_p\right) \\ \dot{\mathrm{x}}_2 &= f_2\left(t, x_2, \ldots, x_2, u_2, \ldots, u_2\right) \\ \dot{\mathrm{x}}_3 &= f_3\left(t, x_3, \ldots, x_3, u_3, \ldots, u_3\right) \\ \dot{\mathrm{x}}_n &= f_n\left(t, x_1, \ldots, x_n, u_1, \ldots, u_p\right) \end{aligned} \tag{2.1}$$

onde x_i denota a derivada de x_i com respeito a variável temporkal t e $u_1, u_2, \ldots, u_p$ são as variáveis de entrada. Chama-se as variáveis $x_1, x_2, \ldots, x_n$ de variáveis de estado. Eles representam a memória que o sistema dinâmico tem do seu passado. Pode-se usar a notação vetorial para reescrever na seguinte forma compacta.

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_2 \\ \vdots \\ \vdots \\ x_n \end{bmatrix}, \quad u_{\square} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ \vdots \\ u_p \end{bmatrix}, \quad f(t,x,u) = \begin{bmatrix} f_1(t,x,u) \\ f_2(t,x,u) \\ f_3(t,x,u) \\ \vdots \\ \vdots \\ f_n(t,x,u) \end{bmatrix} \tag{2.2}$$

e rescrevendo as n equações diferenciais de primeira ordem como uma equação diferencial vetorial de primeira ordem n-dimensional tem-se

$$\dot{x} = f(t,x,u) \tag{2.3}$$

Chamamos (2.2) de equação do estado, e referimos x como vetor de estado e u como vetor de entrada. Quando não há entrada u presente no sistema, chamamos de equação de estados não forçada e é escrita na seguinte forma

$$\dot{x} = f(t,x) \tag{2.4}$$

Um sistema dinâmico continuo pode ser classificado como invariante no tempo se a parte direita de (2.4) não depende explicitamente do tempo, i.e. se $f(t,x) = f(x)$. Por outro lado, se $f(t,x)$ depende explicitamente do tempo então o sistema dinâmico é chamado de variante no tempo. Deve-se salientar que a entrada u comumente é representada por uma função da seguinte forma

$$u = g(t,x) \tag{2.5}$$

Sendo assim, a equação (2.3) pode ser representada do seguinte modo

$$\dot{x} = f(t,x,g(t,x)) = f(t,x) \tag{2.6}$$

Conforme explicitado na equação (2.4)

Um conceito importante ao lidar com equações de estado é a definição de ponto de equilíbrio. Um ponto $x = x^*$ no espaço de estados è dito ser um ponto de equilíbrio do sistema representado pela equação (2.3) se ele possuir a propriedade de se o sistema começar em x^* ele se manterá em x^* para sempre na ausência de perturbações. Para o sistema autônomo representado pela equação (2.4) , os pontos de equilíbrio são as raízes reais da equação

$$f(x) = 0 \tag{2.7}$$

Pontos de equilíbrio podem ser isolados, ou ser um conjunto de pontos de equilíbrios contínuos, como por exemplo uma reta, esfera, elipse, etc.

Para sistemas lineares o modelo (2.3) assume a forma

$$\begin{aligned} \dot{x} &= A(t)x + B(t)u \\ y &= C(t)x + D(t)u \end{aligned} \tag{2.8}$$

em que A, B, C e D são matrizes variantes no tempo de dimensões apropriadas.

À medida que passamos de sistemas lineares para não-lineares, existe um confronto com uma situação mais difícil. O princípio da superposição não se sustenta mais e as ferramentas de análise envolvem matemática mais avançada. Devido às poderosas ferramentas que se conhecem para sistemas lineares, o primeiro passo na análise de um sistema não linear é geralmente linearizá-lo, se possível, sobre algum ponto operacional nominal e analisar o modelo linear resultante. Essa é uma prática comum em engenharia e útil. Não há dúvida de que, sempre que possível, deve-se usar a linearização para modelar o máximo possível o comportamento de um sistema não-linear. No entanto, a linearização sozinha não é suficiente. Existem duas limitações básicas da linearização. Primeira, como a linearização é uma aproximação na vizinhança de um ponto de operação, ela só pode prever o comportamento local do sistema não linear nas proximidades desse ponto. Ela não pode prever o comportamento global longe do ponto de operação e em todo o espaço de estados. Segunda, a dinâmica de um sistema não-linear é muito mais rica que a dinâmica de um sistema linear. Existem fenômenos essencialmente não lineares que podem ocorrer apenas na presença da não linearidade; portanto, eles não podem ser descritos ou previstos por modelos lineares. Abaixo segue, exemplos de fenômenos essencialmente não lineares:

- Um sistema não forçado pode ter mais de um ciclo limite. Um sistema forçado com excitação periódica pode exibir um comportamento em estado estacionário harmônico, sub-harmônico ou mais complicado, dependendo da amplitude e frequência da entrada. Pode até exibir um salto descontínuo no modo de comportamento, dependendo da amplitude ou a frequência da excitação

- Equilíbrios isolados múltiplos: Um sistema linear pode ter apenas um ponto de equilíbrio isolado; portanto, ele pode ter apenas um ponto de operação em estado estacionário que atrai o estado do sistema, independentemente do estado inicial. Um sistema não linear pode ter mais de um ponto de equilíbrio isolado. O estado pode convergir para um dos vários pontos operacionais em estado estacionário, dependendo do estado inicial do sistema.

- Escape em tempo finito. O estado de um sistema linear instável chega ao infinito à medida que o tempo se aproxima do infinito; o estado de um sistema não linear, no entanto, pode chegar ao infinito em tempo finito.

- Caos: Um sistema não linear pode ter um comportamento em estado estacionário mais complicado em que não há um equilíbrio, uma oscilação periódica ou uma oscilação quase aperiódica. Esse comportamento é geralmente chamado de caos. Alguns desses movimentos caóticos exibem aleatoriedade, apesar da natureza determinística do sistema.

2.2 Teoria de estabilidade de Lyapunov

Nesta sessão apresentam-se definições sobre a teoria da estabilidade de Lyapunov. Esses conceitos são de suma importância para apresentação dos capítulos 3, 4, e 5. Todos os conceitos utilizados nessa seção foram retirados de (IOANNOU; SUN, 2012).

2.2.1 Conceitos sobre estabilidade

Considere os sistemas descritos por equações diferenciais ordinárias na forma

$$\dot{x} = f(t, x), \quad x(t_0) = x_0 \tag{2.9}$$

onde $x \in \Re^n, f : \tau \times B(r) \to \Re, \tau = [t_0, \infty)$ e $B(r) = \{x \in \Re^n \|x\| < r\}$. Assume-se que f é de tal natureza que, para cada $x_0 \in B(r)$ e cada $t_0 \in \Re^+$, (2.9) tem uma, e apenas uma solução $x(t; t_0; x_0)$.

Definição 2.2.1.1: Um estado x_e é dito ser um **estado de equilíbrio** para o sistema descrito por (2.9) se

$f(t, x_s) \equiv 0$ para todo $t \geq t_0$

Definição 2.2.1.2 . Um estado de equilíbrio x_s é **chamado um estado de equilíbrio isolado** se existe uma constante $r > 0$ tal que $B(x_e, r) : = \{x| \, \|x - x_s\| < r\} \subset R^n$

Definição 2.2.1.3: O estado de equilíbrio x_e é dito ser estável (no sentido de Lyapunov) se para um t_o arbitrário e $\varepsilon > 0$ existe um $\delta(\varepsilon, t_0)$ tal que $\|x_0 - x_e\| < \delta$ implica $\|x(t; t_0; x_0) - x_e\| < \varepsilon$ para todo $t \geq t_0$.

Definição 2.2.1.4: O estado de equilíbrio x_e é dito ser **uniformemente estável** se ele for estável e se $\delta(\varepsilon, t_0)$ na definição 2.1.3 não depender de t_o.

Definição 2.2.1.5 :O estado de equilíbrio x_e é dito ser **assintoticamente estável** se (i) ele for estável e (ii) existir um $\delta(t_0)$ tal que $\|x_0 - x_e\| < \delta(t_0)$ implica $\lim_{t\to+\infty} \|x(t, t_0; x_0) - x_s\| = 0$. Se a condição (ii) for satisfeita, então o estado de equilíbrio x_e é dito **atrativo**.

Definicão 2.2.1.6: O conjunto de todos $x_0 \in \Re^n$ tal que $x(t; t_0; x_0) \to x_e$ quando $t \to \infty$ para algum $t_0 \geq 0$ é chamado de **região de atração** do estado de equilíbrio x_e.

Definição 2.2.1.7: O estado de equilíbrio x_e é dito ser **uniformemente assintoticamente estável** se (i) ele for uniformemente estável e (ii) para cada

$\varepsilon > 0$ e qualquer to $\Re^{+}$, existe um $\delta_0 > 0,$ independente de t_0, ε e umT($\varepsilon) > 0$, independente de t_0, tal que $\|x\,(t; t_0; x_0) - x_\varepsilon\| < \varepsilon$ para todo $t \geq t_0 + T(\varepsilon)$ sempre que $\|x_0 - x_\varepsilon\| < \delta_0$.

Definição 2.2.1.8: O estado de equilíbrio x_e é **exponencialmente estável** se para cada $\varepsilon > 0$ existe um $\delta(\varepsilon) > 0$, tal que

$\|x\,(t; t_0; x_0) - x_e\| < \varepsilon e^{-\alpha(t-t_0)}$ para todo $t \geq t_0$

sempre que $\|x_0 - x_\varepsilon\| < \delta(\varepsilon)$, onde $\alpha > 0$

Definição 2.2.1.9: O estado de equilíbrio x_e é dito **instável** se ele não for estável.

Quando a equação (2.9) tem uma solução única para cada $x_0 \in \Re^{n} e t_0 \in \Re^{+}$, precisa-se das seguintes definições para a caracterização global de soluções.

Definição 2.1.10: Uma solução $x\,(t; t_0; x_0)$ de (2.9) é **limitada** se existe um $\beta >$ o tal que $\|x\,(t; t_0; x_0) - x_e\| < \beta$ para todo $t > t_0$, onde β pode depender de cada solução.

Definição 2.2.1.11: As soluções de (2.9) são **uniformemente limitadas** se para quaisquer $\alpha > 0$ e $t_0 \in \Re^{+}$, existe um $\beta = \beta(\alpha)$, independente de t_0, tal que se $\|x_0\| < \alpha$, então $\|x\,(t; t_0; x_0) - x_e\| < \beta$ para todo $t > t_0$.

Definição 2.2.1.12: As soluçares de (2.9) são **uniformemente finalmente limitadas** (com limitante B) se existe um $B > 0$ e se para quaisquer $\alpha \geq 0$ e $t_0 \in \Re^{+}$, então existe um $T = T(\alpha) > 0$ (independente de t_0) tal que $\|x_0\| < \alpha$ implica $\|x\,(t; t_0; x_0)\| < B$ para todo $t > t_0 + T$.

Definição 2.2.1.13: Se $x\,(t; t_0; x_0)$ é uma solução de $\dot{x} = f(t, x)$, então a trajetória $x\,(t; t_0; x_0)$ é dita **estável** se o ponto de equilíbrio $z_e = 0$ da equação diferencial $\dot{z} = f\,(t, z + x\,(t; t_0; x_0)) - f\,(t, x\,(t; t_0, ; x_0))$ é estável.

2.3 Sistemas caóticos

Sistemas dinâmicos caóticos tem sido foco de grande atenção da comunidade acadêmica. Embora não exista nenhuma formalização universal para definir o termo caos, existem três conceitos necessários para que um sistema apresente caoticidade. Por exemplo, Strogatz, em (STROGATZ, 2018), define o caos do seguinte modo:

Definição 2.1: Caos é um comportamento aperiódico de longo prazo em um sistema determinístico que apresenta dependência sensível às condições iniciais, dessa forma tornando impossível a previsão de seu estado futuro.

A seguir, descreve-se, conforme no livro de Strogatz (STROGATZ, 2018), cada umas das características estabelecidas acima.

- **Comportamento aperiódico de longo prazo:** significa a existência de trajetórias que não se acomodam em pontos fixos, órbitas periódicas, ou órbitas quasi-periódicas quando

$t \to \infty$.

- **Sistema determinístico:** implica que o sistema não possui entradas ou parâmetros aleatórios. O comportamento irregular do sistema é devido a sua natureza não-linear, isto é, o sistema é governado por equações determinísticas.

- **Dependência sensível às condições iniciais**: Implica que trajetórias próximas, caracterizadas pelas variáveis de estado, se separam exponencialmente rápido.

Para caracterização da separação das trajetórias infinitesimalmente próximas ao longo do tempo, usa-se o expoente de Lyapunov. Considere $\delta(t)$ como a distância no tempo t de duas trajetórias que iniciaram com uma distância inicial δ_0 no tempo t_0. Se $\delta(t)$ cresce exponencialmente com a evolução do sistema, então este apresenta dependência e sensibilidade as condições iniciais. Assim tém-se

$$\delta(t) = \delta_0 e^{\gamma(t-t_0)} \tag{2.10}$$

Sendo γ o expoente de Lyapunov. Um sistema dinâmico caótico n-dimensional apresenta n expoentes de Lyapunov. No mínimo 1 expoente de Lyapunov deverá ser positivo para o sistema apresente condições caóticas e para ser hipercaótico deverá apresentar 2 expoentes de Lyapunov positivos e ter mais que três dimensões (VARAN; AKGUL, 2018).

2.4 Sincronização de sistemas caóticos

Nesta sessão, os conceitos fundamentais e relevância da sincronização caótica são descritos.
A sincronização caótica tem despertado bastante interesse da comunidade cientifica desde a década de 1990. Vide, por exemplo, (CUOMO; OPPENHEIM, 1993) e (CUOMO; OPPENHEIM; STROGATZ, 1993) . Nestes trabalhos promissores seus fundamentos são avaliados em termos dos expoentes de Lyapunov e do método direto de Lyapunov. Vale ressaltar que a metodologia nestes trabalhos serviu como base para desenvolver uma abordagem básica geral de sincronização caótica.

Também na década de 1990, Pecora e Carroll (PECORA; CARROLL, 1990) comentam que sistemas caóticos por si só desafiam a sincronização. Entretanto, estes sistemas possuem uma propriedade de autosincronização quando interconectados em uma configuração específica. Mais precisamente, o sistema para comunicação segura pode ser decomposto em subsistemas idênticos, sendo o receptor alimentado por um estado do transmissor, o que permite a sincronização, mesmo diferenciando moderadamente as condições iniciais. Ressalta-se que se dois sistemas caóticos idênticos começarem com condições iniciais diferentes, porém próximas, irão se separar exponencialmente no tempo. Logo, percebe-se que sistemas caóticos desafiam a sincronização quando ambos os sistemas começam com as condições iniciais diferentes.

Uma outra definição indica que a sincronização é uma característica em que dois ou mais sistemas caóticos ajustam suas evoluções no tempo para um comportamento comum (BOCCALETTI et al., 2002).

O método de sincronização que foi usado neste trabalho tem como motivação o de (PECORA; CARROLL, 1990) que é conhecido como o de sinal comum. Entretanto, nossa abordagem difere significativamente da precursora, pois realimenta-se o sistema receptor com uma função escalar do erro de sincronização de um dos estados do sistema mestre, a qual é projetada através da teoria de estabilidade de Lyapunov, ao contrário do trabalho precursor de Pecora e Carroll. Assim, os trabalhos precursores da década de 1990 podem ser considerados como casos particulares do proposto nesta monografia. Adicionalmente, convém ressaltar que a possibilidade de escolher uma função escalar arbitrária como realimentação permite um aprimoramento da segurança em relação aos trabalhos precursores.

Na sequência, será mostrado o problema da sincronização para um sistema dinâmico composto por um sistema de equações diferenciais ordinárias, considere o sistema caótico mestre

$$\dot{x}_m = f_m\left(x_m, d_m(t)\right) \tag{2.11}$$

em que x_m é o estado do sistema mestre, $d_m(t)$ é um vetor de distúrbio desconhecido e f_m são um mapeamento conhecido.

Defina agora o sistema escravo

$$\dot{x}_s = f_s\left(x_s, u, d_s(t)\right) \tag{2.12}$$

em que x_s é o estado do sistema escravo, u é a entrada, $d_s(t)$ é um distúrbio desconhecido e $f(s)$ é um mapeamento conhecido. Com base em (2.11) e (2.12), o erro dinâmico de sincronização pode ser escrito como

$$\dot{e} = \dot{x}_m - \dot{x}_s = f_m\left(x_m, d_m(t)\right) - f_s\left(x_s, u, d_s(t)\right) \tag{2.13}$$

em que

$$e = x_m - x_s \tag{2.14}$$

é definido como erro de sincronização. Os sistemas descritos pelas equações (2.11) e (2.12) serão considerados sincronizados, em geral, se $e(t) \to 0$ quando $t \to \infty$ ou seja, as trajetórias do sistema escravo convergem para os mesmos valores do sistema mestre. Em particular, quando a sincronização é em tempo finito, temos a sincronização em tempo finito

2.5 Comunicação segura baseada em caos

A comunicação com segurança baseada em caos neste trabalho é implementada a partir da sincronização de um oscilador hipercaótico que codifica as informações (mestre), e um oscilador hipercaótico que decodifica a informação passada (escravo). Por se tratar de uma dinâmica caótica extremamente complexa, a quebra do sigilo para usuários que não possuam a chave de decodificação, i.e., a lei de controle, os parâmetros, as condições iniciais e o sistema caótico em questão tornam a criptografia inviolável. Desta forma, métodos inovadores de comunicação segura baseado em caos estão ganhando cada vez mais notoriedade.

A primeira geração foi desenvolvida a partir de 1993 (CUOMO; OPPENHEIM; STROGATZ, 1993) conhecida como mascaramento caótico aditivo: considera-se dois sistemas caóticos idênticos. A máscara caótica $xi(t)$ representa um dos estados do sistema caótico transmissor, tendo uma faixa de amplitude entre que 20 dB a 30 dB sendo $m(t)$ adicionada a mascara caótica, fornecendo o sinal $s(t)$. Como o sinal caótico $xi(t)$ é muito complexo e $m(t)$ é muito menor que este sinal, espera-se que a mensagem não possa ser separada de $s(t)$ sem que alguém tenha o conhecimento exato de $xi(t)$, conforme mostrado na figura 2.1. Nesta seção, todos os conceitos foram retirados de (YANG, 2004).

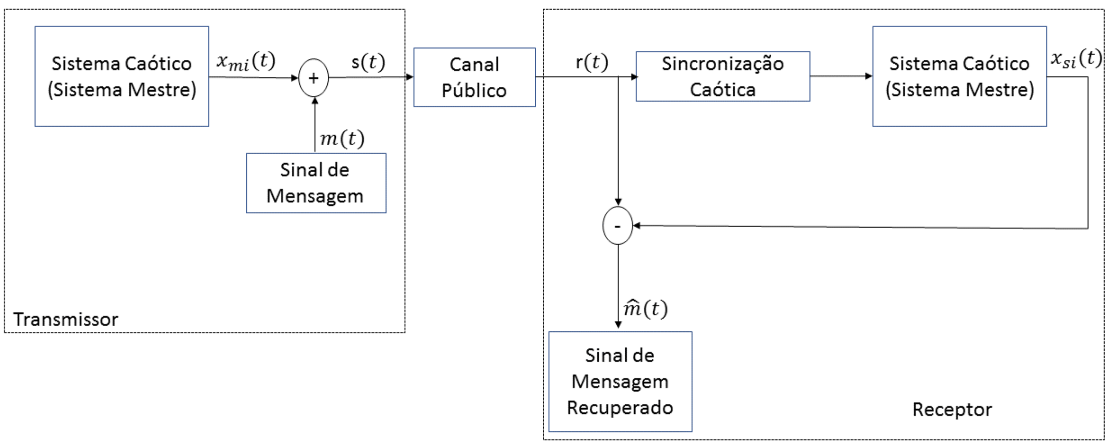

Figura 2.1: Esquema do mascaramento caótico aditivo representada em diagramas de blocos (JOVIC, 2011).

Modulação de parâmetros caótica: A modulação de parâmetros caóticos é basicamente para transmissão de sinais digitais, que é diferente do mascaramento caótico que se utiliza na transmissão de sinais principalmente analógicos. Essa metodologia consiste em usar o sinal da mensagem para modificar os parâmetros do sistema caótico mestre de modo a alterar a dinâmica do sistema. Assim, a mensagem original é recuperada com base em parâmetros estimados, vide figura 2.2. Diferente do mascaramento caótico, no qual as informações são somadas constantemente para algum estado do transmissor, sem alterar a dinâmica deste, na modulação caótica, a dinâmica do transmissor é alterada, mas sem perder a caoticidade, já que a mensagem altera os parâmetros no sistema mestre (YANG; CHUA, 1996).

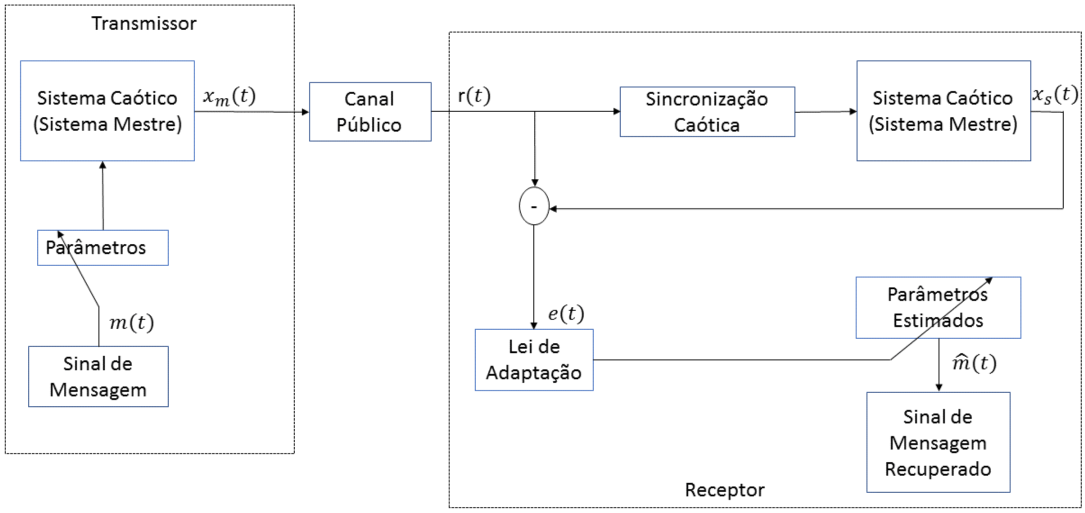

Figura 2.2: Esquema para modulação caótica de parâmetros representada em diagrama de blocos (JOVIC, 2011).

Modulação caótica não autônoma: Esta metodologia usa o sinal de mensagem para alterar diretamente as trajetórias que o sistema mestre segue. Diferente da máscara caótica aditiva a mensagem não deve ser tão menor que o usual. A mensagem é adicionada a todos os estados do sistema, não em apenas um. A recuperação da mensagem é através de uma função de decodificação que o receptor possui, vide figura 2.3

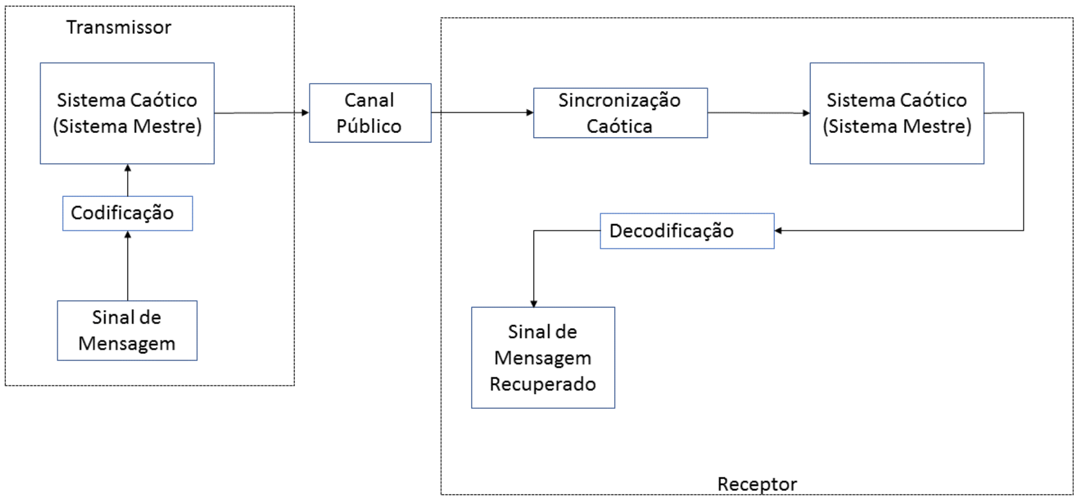

Figura 2.3: Esquema de modulação caótica não autônoma representada em diagramas de blocos (JOVIC, 2011) .

Capítulo 3

Sincronização de um sistema hipercaótico baseada em controle proporcional.

3.1 Introdução

A sincronização do caos ocorre quando dois ou mais sistemas caóticos não idênticos são acoplados de modo que, apesar da divergência exponencial de suas trajetórias próximas, a sincronia pode ser alcançada em tempo finito ou em $t \to \infty$. A sincronização depende de várias condições, como a força do acoplamento, a região dos parâmetros do sistema e o grau de divergência dos dois sistemas caóticos. Uma condição básica frequentemente encontrada na literatura para a sincronização mestre-escravo é que ambos os sistemas devem apresentar as mesmas não linearidades.

Diferentes abordagens para a implementação de controladores e sincronizadores de sistemas caóticos foram propostos na literatura. Por exemplo, em (AL-OBEIDI; AL-AZZAWI, 2018), trata-se de um sistema hexadimensional, mas com um controle em cada equação de estado para tornar a prova de estabilidade exequível. Em (SINGH; ROY, 2018), considera-se a prova de estabilidade da sincronização de um sistema completamente atuado e sem nenhum distúrbio. Da mesma forma, considera-se em (UMOH; TOLA, 2018) a sincronização de um sistema heptadimensional completamente atuado e sem distúrbios. Outros trabalhos mais recentes, contudo com as mesmas limitações, podem ser encontrados em (BOCCALETTI et al., 2002),(CHEN; AIHARA, 1995), (TAVAZOEI; HAERI, 2007), (VAIDYANATHAN; AZAR, 2016) e (VAIDYANATHAN; VOLOS; KYPRIANIDIS et al., 2015). Apesar de alguns desses métodos serem eficazes no controle e sincronização, eles geralmente são computacionalmente complexos. Em (YANG; ZHU, 2013), trata-se de um sistema hipercaótico heptadimensional e a prova matemática da sincronização leva considerações como o agrupamento em uma matriz de termos não lineares.

Uma deficiência comum na literatura consiste em considerar o sistema caótico escravo como completamente atuado. Vide, por exemplo, (OUANNAS; AZAR; VAIDYANATHAN, 2017), (VAIDYANATHAN; AZAR, 2016) e (WANG; ZHANG; FAN, 2017). Adicionalmente, muitas vezes a complexidade do sincronizador é elevada (MATOUK; ELSADANY, 2014), (VAIDYANATHAN; VOLOS; PHAM, 2015) e (VARAN; AKGUL, 2018) com um impacto negativo na implementação. Também, a sincronização hipercaótica com aplicações em comunicação segura é raramente encontrada na literatura. Pode-se citar, por exemplo (LI; LIAO; WONG, 2005), (QI et al., 2008), e (SMAOUI; KAROUMA; ZRIBI, 2011) como exceções. Entretanto, nestas propostas é considerada uma sincronização completamente atuada.

Com base no anteriormente exposto, neste capitulo será proposto um esquema de sincronização para a telecomunicação segura baseado no sistema hipercaótico de Lorenz (WANG, P. et al., 2011) e na teoria de estabilidade de Lyapunov. A contribuição está no fato que foi usado apenas um controle escalar em um estado, dentre os nove estados do sistema mestre. Também foi considerada a presença de distúrbios na análise, ao contrário de (WU; CHEN; CAI, 2007) (ZHANG, J. et al., 2004). Ressalta-se que o sistema hipercaótico aqui usado é robusto, pois foram considerados distúrbios em todos os estados. A prova de convergência do erro de sincronização mostra que o mesmo fica em uma vizinhança da origem, o que é posteriormente validado pela implementação da sincronização usando MATLAB/Simulink. As principais características do esquema proposto são: 1) o sincronizador baseia-se em sistema hipercaótico, ao contrário de (CHEN; LÜ, 2002), (LI, 2007), 2) o sincronizador é estruturalmente simples, ao contrário de (BOCCALETTI et al., 2002), (ZHANG; ZHU, 2008), 3) a análise de estabilidade considera a presença de distúrbios, ao contrário de (MATOUK; ELSADANY, 2014), (WANG; ZHANG; FAN, 2017), 4) o esquema proposto baseia-se em um sistema escravo subatuado, ao contrário de (SINGH; ROY, 2018), (VARAN; AKGUL, 2018) 5) considera-se aplicações do sincronizador para comunicação segura, ao contrario de (HE; VAIDYA, 1998), (KOLUMBÁN; KENNEDY; CHUA, 1998) e (YU; LIU, 2003).

3.2 Formulação do Problema

Considere o seguinte sistema hipercaótico (WANG, P. et al., 2011)

$$
\begin{aligned}
\dot{x}_1 &= -\sigma b_1 x_1 - x_2 x_4 + b_4 x_4^2 + b_3 x_3 x_5 - \sigma b_2 x_7 \\
\dot{x}_2 &= -\sigma x_2 + x_1 x_4 - x_2 x_5 + x_4 x_5 - \frac{\sigma x_9}{2} \\
\dot{x}_3 &= -\sigma b_1 x_3 + x_2 x_4 - b_4 x_2^2 - b_3 x_1 x_5 + \sigma b_2 x_8 \\
\dot{x}_4 &= -\sigma x_4 - x_2 x_3 - x_2 x_5 + x_4 x_5 + \frac{\sigma x_9}{2} \\
\dot{x}_5 &= -\sigma b_5 x_5 + \frac{x_2^2}{2} - \frac{x_4^2}{2} \\
\dot{x}_6 &= -b_6 x_6 + x_2 x_9 - x_4 x_9 \\
\dot{x}_7 &= -b_1 x_7 - r x_1 + 2 x_5 x_8 - x_4 x_9 \\
\dot{x}_8 &= -b_1 x_8 + r x_3 - 2 x_5 x_7 + x_2 x_9 \\
\dot{x}_9 &= -x_9 - r x_2 + r x_4 - 2 x_2 x_6 + 2 x_4 x_6 + x_4 x_7 - x_2 x_8
\end{aligned}
\tag{3.1}
$$

Onde

$$
\begin{aligned}
b_1 &= 4\frac{1+a^2}{1+2a^2}, \qquad b_2 = \frac{1+2a^2}{2\left(1+a^2\right)}, \qquad b_3 = 2\frac{1-a^2}{1+a^2} \\
b_4 &= \frac{a^2}{1+a^2}, \qquad b_5 = \frac{8a^2}{1+2a^2}, \qquad b_6 = \frac{4}{1+2a^2}
\end{aligned}
\tag{3.2}
$$

Sendo; $a = 1/2; \sigma = 1/2; r = 15,1$. Observe que se trata de um sistema hipercaótico de Lorenz, onde $x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ e x_9 são os estados do sistema e b_1, b_2, b_3, b_4, b_5 e b_6 são constantes reais. Com base em (3.1), considere os seguintes sistemas mestre e escravo perturbados.

mestre:

$$
\begin{aligned}
\dot{x}_{1m} &= -\sigma b_1 x_{1m} - x_{2m}x_{4m} + b_4 x_{4m}^2 + b_3 x_{3m}x_{5m} - \sigma b_2 x_{7m} \\
\dot{x}_{2m} &= -\sigma x_{2m} + x_{1m}x_{4m} - x_{2m}x_{5m} + x_{4m}x_{5m} - \frac{\sigma x_{9m}}{2} \\
\dot{x}_{3m} &= -\sigma b_1 x_{3m} + x_{2m}x_{4m} - b_4 x_{2m}^2 - b_3 x_{1m}x_{5m} + \sigma b_2 x_{8m} \\
\dot{x}_{4m} &= -\sigma x_{4m} - x_{2m}x_{3m} - x_{2m}x_{5m} + x_{4m}x_{5m} + \frac{\sigma x_{9m}}{2} \\
\dot{x}_{5m} &= -\sigma b_5 x_{5m} + \frac{x_{2m}^2}{2} - \frac{x_{4m}^2}{2} \\
\dot{x}_{6m} &= -b_6 x_{6m} + x_{2m}x_{9m} - x_{4m}x_{9m} \\
\dot{x}_{7m} &= -b_1 x_{7m} - r x_{1m} + 2x_{5m}x_{8m} - x_{4m}x_{9m} \\
\dot{x}_{8m} &= -b_1 x_{8m} + r x_{3m} - 2x_{5m}x_{7m} + x_{2m}x_{9m} \\
\dot{x}_{9m} &= -x_{9m} - r x_{2m} + r x_{4m} - 2x_{2m}x_{6m} + 2x_{4m}x_{6m} + x_{4m}x_{7m} - x_{2m}x_{8m}
\end{aligned}
\tag{3.3}
$$

Escravo:

$$
\begin{aligned}
\dot{x}_{1s} &= -\sigma b_1 x_{1s} - x_{2s}x_{4s} + b_4 x_{4s}^2 + b_3 x_{3s}x_{5s} - \sigma b_2 x_{7s} + h_1(t) \\
\dot{x}_{2s} &= -\sigma x_{2s} + x_{1s}x_{4s} - x_{2s}x_{5s} + x_{4s}x_{5s} - \frac{\sigma x_{9s}}{2} + h_2(t) \\
\dot{x}_{3s} &= -\sigma b_1 x_{3s} + x_{2s}x_{4s} - b_4 x_{2s}^2 - b_3 x_{1s}x_{5s} + \sigma b_2 x_{8s} + h_3(t) \\
\dot{x}_{4s} &= -\sigma x_{4s} - x_{2s}x_{3s} - x_{2s}x_{5s} + x_{4s}x_{5s} + \frac{\sigma x_{9s}}{2} + u + h_4(t) \\
\dot{x}_{5s} &= -\sigma b_5 x_{5s} + \frac{x_{2s}^2}{2} - \frac{x_{4s}^2}{2} + h_5(t) \\
\dot{x}_{6s} &= -b_6 x_{6s} + x_{2s}x_{9s} - x_{4s}x_{9s} + h_6(t) \\
\dot{x}_{7s} &= -b_1 x_{7s} - r x_{1s} + 2x_{5s}x_{8s} - x_{4s}x_{9s} + h_7(t) \\
\dot{x}_{8s} &= -b_1 x_{8s} + r x_{3s} - 2x_{5s}x_{7s} + x_{2s}x_{9s} + h_8(t) \\
\dot{x}_{9s} &= -x_{9s} - r x_{2s} + r x_{4s} - 2x_{2s}x_{6s} + 2x_{4s}x_{6s} + x_{4s}x_{7s} - x_{2s}x_{8s} + h_9(t)
\end{aligned}
\tag{3.4}
$$

em que x_{im} i=1..,9 são os estados do sistema mestre, x_{is} i=1..,9 são os estados do sistema escravo, $h_1(t), h_2(t), h_3(t), h_4(t), h_5(t), h_7(t), h_8(t)$ e $h_9(t)$ são distúrbios do sistema escravo e u é o sinal de controle.

Comentário 1: O sistema (3.1) é caótico, seu comportamento é não previsível e depende das condições iniciais escolhidas, nesse modelo o sistema é sensível a mudança das condições iniciais.

Hipótese 1: Assume-se que os distúrbios são limitados. Mais especificamente,

$$\begin{aligned}
|h_1(t)| &\leq \bar{h}_1 \\
|h_2(t)| &\leq \bar{h}_2 \\
|h_3(t)| &\leq \bar{h}_3 \\
|h_4(t)| &\leq \bar{h}_4 \\
|h_5(t)| &\leq \bar{h}_5 \\
|h_6(t)| &\leq \bar{h}_6 \\
|h_7(t)| &\leq \bar{h}_7 \\
|h_8(t)| &\leq \bar{h}_8 \\
|h_9(t)| &\leq \bar{h}_9
\end{aligned} \tag{3.5}$$

em que $\bar{h}_1, \bar{h}_2, \bar{h}_3, \bar{h}_4, \bar{h}_5, \bar{h}_6, \bar{h}_7, \bar{h}_8$ e $\bar{h}_9$ são constantes positivas.

3.3 Equação de erro de sincronização e sinal de controle proposto

Define-se a dinâmica dos erros de sincronização como sendo:

$$\begin{aligned}
\dot{e}_1 &= \dot{x}_{1s} - \dot{x}_{1m} \\
\dot{e}_2 &= \dot{x}_{2s} - \dot{x}_{2m} \\
\dot{e}_3 &= \dot{x}_{3s} - \dot{x}_{3m} \\
\dot{e}_4 &= \dot{x}_{4s} - \dot{x}_{4m} \\
\dot{e}_5 &= \dot{x}_{5s} - \dot{x}_{5m} \\
\dot{e}_6 &= \dot{x}_{6s} - \dot{x}_{6m} \\
\dot{e}_7 &= \dot{x}_{7s} - \dot{x}_{7m} \\
\dot{e}_8 &= \dot{x}_{8s} - \dot{x}_{8m} \\
\dot{e}_9 &= \dot{x}_{9s} - \dot{x}_{9m}
\end{aligned} \tag{3.6}$$

Substituindo-se (3.3) e (3.4) em (3.6), obtém-se que:

$$\begin{aligned}
\dot{e}_1 =& -\sigma b_1 e_1 - e_2 e_4 - e_2 x_{4m} - e_4 x_{2m} + 2b_4 x_{4m} e_4 + b_4 e_4^2 + b_3 e_3 e_5 + b_3 e_3 x_{5m} \\
& + b_3 e_5 x_{3m} - \sigma b_2 e_7 + h_1 \\
\dot{e}_2 =& -\sigma e_2 + e_1 e_4 + e_1 x_{4m} + e_4 x_{1m} - e_2 e_5 - e_2 x_{5m} - e_5 x_{2m} + e_4 e_5 + e_4 x_{5m} \\
& + e_5 x_{4m} - 0,5\sigma e_9 + h_2 \\
\dot{e}_3 =& -\sigma b_1 e_3 + e_2 e_4 + e_2 x_{4m} + e_4 e_{2m} - 2b_4 x_{2m} e_2 - b_4 e_2^2 - b_3 e_1 e_5 - b_3 e_1 x_{5m} \\
& - b_3 e_5 x_{1m} + \sigma b_2 e_8 + h_3 \\
\dot{e}_4 =& -\sigma e_4 - e_2 e_3 - e_2 x_{3m} - e_3 x_{2m} - e_2 e_5 - e_2 x_{5m} - e_5 x_{2m} + e_4 e_5 + e_4 x_{5m} \\
& + e_5 x_{4m} + 0,5\sigma e_9 + h_4 + u \\
\dot{e}_5 =& -\sigma b_5 e_5 + e_2 x_{2m} + 0,5 e_2^2 - e_4 x_{4m} - 0,5 e_4^2 + h_5 \\
\dot{e}_6 =& -b_6 e_6 + e_2 e_9 + e_2 x_{9m} + e_9 x_{2m} - e_4 e_9 - e_4 x_{9m} - e_9 x_{4m} + h_6 \\
\dot{e}_7 =& -b_1 e_7 - r e_1 + 2e_5 e_8 + 2e_5 x_{8m} + 2e_8 x_{5m} - e_4 e_9 - e_4 x_{9m} - e_9 x_{4m} + h_7 \\
\dot{e}_8 =& -b_1 e_8 + r e_3 - 2e_5 e_7 - 2e_5 x_{7m} - 2e_7 x_{5m} + e_2 e_9 + e_2 x_{9m} + e_9 x_{2m} + h_8 \\
\dot{e}_9 =& -e_9 - r e_2 + r e_4 - 2e_2 e_6 - 2e_2 x_{6m} - 2e_6 x_{2m} + 2e_4 e_6 + 2e_4 x_{6m} + 2e_6 x_{4m} \\
& + e_4 e_7 + e_4 x_{7m} + e_7 x_{4m} - e_2 e_8 - e_2 x_{8m} - e_8 x_{2m} + h_9
\end{aligned} \tag{3.7}$$

Hipótese 2: Os estados do sistema mestre são limitados (WANG, P. et al., 2011). Mais precisamente,

$$\begin{aligned}
|x_{1m}| &\leq \bar{x}_1 \\
|x_{2m}| &\leq \bar{x}_2 \\
|x_{3m}| &\leq \bar{x}_3 \\
|x_{4m}| &\leq \bar{x}_4 \\
|x_{5m}| &\leq \bar{x}_5 \\
|x_{6m}| &\leq \bar{x}_6 \\
|x_{7m}| &\leq \bar{x}_7 \\
|x_{8m}| &\leq \bar{x}_8 \\
|x_{9m}| &\leq \bar{x}_9
\end{aligned} \tag{3.8}$$

em que $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4, \bar{x}_5, \bar{x}_6, \bar{x}_7, \bar{x}_8$ e $\bar{x}_9$ são constantes positivas.

Hipótese 3: As condições iniciais são suficientemente pequenas de modo que

$$\|e(0)\| \leq \alpha < 1 \tag{3.9}$$

em que α é uma constante positiva que satisfaz $\alpha \geq 0, sendo\theta$ outra costante positiva que depende, entre outros, dos limitantes superiores das pertubaçoes, que será definida posteriormente.

Fato 1: Considere que m, n e p são números naturais quaisquer que variam ente 1 e 9. Note que:

$$\begin{array}{l} (e_m^2 \pm e_n^2) \geq 0 \\ 4e_m e_n e_p \leq 2e_m^2 + 2e_n^2 e_p^2 \\ 2e_n^2 e_p^2 \leq e_n^4 + e_p^4 \\ 2e_m\left(e_p^2\right) = 2\left(e_m e_p\right)\left(e_p\right) \end{array} \tag{3.10}$$

Teorema 1: Considere os sistemas mestre e escravo descritos em (3.2) e (3.3), as hipóteses 1-3 e a seguinte lei de controle.

$$u = -\psi e_4 \tag{3.11}$$

Então, o erro de sincronização converge em tempo finito para o conjunto compacto $\Omega = \{e \in \Re^9 \|e\| \leq \theta\}$, onde $\theta > 0$ e $\psi > 0$.

Prova:

Considere a seguinte candidata a função de Lyapunov

$$V = \frac{1}{2}\left(e_1^2 + e_2^2 + e_3^2 + e_4^2 + e_5^2 + e_6^2 + e_7^2 + e_8^2 + e_9^2\right) \tag{3.12}$$

Derivando (3.12) em relação ao tempo ao longo das trajetórias dos erros resulta:

$$\dot{V} = e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + e_4\dot{e}_4 + e_5\dot{e}_5 + e_6\dot{e}_6 + e_7\dot{e}_7 + e_8\dot{e}_8 + e_9\dot{e}_9 \tag{3.13}$$

Substituindo-se (3.7) e (3.11) em (3.13) tem-se que

$$\begin{aligned}
\dot{V} = &-e_1^2(\sigma b_1) - e_2^2(\sigma) - e_3^2(\sigma b_1) - e_4^2(\Psi + \sigma) - e_5^2(\sigma b_5) - e_6^2(\sigma b_6) - e_7^2(b_1) \\
&- e_8^2(\sigma b_1) - e_9^2(1) + e_1 h_1 + e_2 h_2 + e_3 h_3 + e_4 h_4 + e_5 h_5 + e_6 h_6 + e_7 h_7 + e_8 h_8 \\
&+ e_9 h_9 + 2b_4 x_{4m} e_1 e_4 + b_4 e_1 e_4^2 + b_3 x_{3m} e_1 e_5 - (\sigma b_2 + r) e_1 e_7 + (x_{1m} - x_{3m}) e_2 e_4 \\
&- 0,5 e_2^2 e_5 - x_{5m} e_2^2 - (2x_{6m} + x_{8m} + 0,5\sigma - r) e_2 e_9 + (x_{4m} - 2b_4 x_{2m}) e_2 e_3 \\
&+ x_{4m} e_2 e_5 - b_4 e_2^2 e_3 - b_3 x_{1m} e_3 e_5 + (\sigma b_2 + r) e_3 e_8 - x_{2m} e_4 e_5 + 0,5 e_4^2 e_5 + x_{5m} e_4^2 \\
&+ (0,5\sigma + 2x_{6m} + r + x_{7m}) e_4 e_9 + x_{9m} e_2 e_6 - x_{9m} e_4 e_6 + 2x_{8m} e_5 e_7 - x_{9m} e_4 e_7 \\
&- 2x_{7m} e_5 e_8 + x_{9m} e_2 e_8 - e_2 e_6 e_9 + (x_{4m} - x_{2m}) e_6 e_9 + e_4 e_6 e_9
\end{aligned} \tag{3.14}$$

Definindo-se $\gamma_1 = -(2x_{6m} + x_{8m} + 0,5\sigma - r)$, γ_2=$(x_{4m} - 2b_4 x_{2m})$, $\gamma_3 = \sigma b_2 + r$, $\gamma_4 = 0,5\sigma + 2x_{6m} + r + x_{7m}$, $\gamma_5 = x_{4m} - x_{2m}$, $\gamma_6 = x_{1m} - x_{3m}$, $\gamma_7 = -\sigma b_2 - r$, $\beta = \bar{h}_1^2 + \bar{h}_2^2 + \bar{h}_3^2 + \bar{h}_4^2 + \bar{h}_5^2 + \bar{h}_6^2 + \bar{h}_7^2 + \bar{h}_8^2 + \bar{h}_9^2 + 8\bar{x}_5^2$, em γ é o maior dos coeficientes de quarta ordem dos erros, $\rho_1 = \sigma b_1 - \frac{5}{64}$, $\rho_2 = \sigma - \frac{3}{32}$, $\rho_3 = \sigma b_1 - \frac{1}{32}$, $\rho_4 = \Psi + \sigma - \frac{1}{16} - \bar{x}_5 - 8(1 + \bar{x}_9^2 + \bar{x}_2^2 + \bar{x}_5^2 + b_4^2)$, $\rho_5 = \sigma b_5 - \frac{1}{8}$, $\rho_6 = b_6 - \frac{1}{16}$, $\rho_7 = b_1 - \frac{1}{16}$, $\rho_8 = b_1 - \frac{1}{32}$, $\rho_9 = 1 - \frac{1}{32}$.

Observe, adicinalmente, que

$$\begin{aligned}
&e_1 h_1 \le \tfrac{e_1^2}{32} + 8\bar{h}_1^2, e_2 h_2 \le \tfrac{e_2^2}{32} + 8\bar{h}_2^2, e_3 h_3 \le \tfrac{e_3^2}{32} + 8\bar{h}_3^2, e_4 h_4 \le \tfrac{e_4^2}{32} + 8\bar{h}_4^2 \\
&e_5 h_5 \le \tfrac{e_5^2}{32} + 8\bar{h}_5^2, e_6 h_6 \le \tfrac{e_6^2}{32} + 8\bar{h}_6^2, e_7 h_7 \le \tfrac{e_7^2}{32} + 8\bar{h}_7^2, e_8 h_8 \le \tfrac{e_8^2}{32} + 8\bar{h}_8^2 \\
&e_9 h_9 \le \tfrac{e_9^2}{32} + 8\bar{h}_9^2, -e_2 e_6 e_9 \le \tfrac{e_2^2}{32} + 8e_6^2 e_9^2 \le \tfrac{e_2^2}{32} + 4e_6^4 + 4e_9^4, x_{5m} e_4^2 \le \bar{x}_5 e_4^2 \\
&e_4 e_6 e_9 \le \tfrac{e_4^2}{32} + 8e_6^2 e_9^2 \le \tfrac{e_4^2}{32} + 4e_6^4 + 4e_9^4, b_4 e_1 e_4^2 \le \tfrac{e_1^2}{32} + 8b_4^2 e_4^4, 0,5 e_4^2 e_5 \le \tfrac{e_5^2}{64} + 4e_4^4 \\
&-0,5 e_2^2 e_5 \le \tfrac{e_5^2}{64} + 4e_2^4, -b_4 e_2^2 e_3 \le \tfrac{e_3^2}{32} + 8b_4^2 e_2^4, -x_{2m} e_4 e_5 \le \tfrac{e_5^2}{32} + 8\bar{x}_2^2 e_4^2 \\
&-e_2^2 x_{5m} \le \tfrac{e_2^2}{32} + 8\bar{x}_5^2 h_1^2, 2b_4 x_{4m} e_1 e_4 \le \tfrac{e_1^2}{64} + 64\bar{x}_4^2 e_4^2, -x_{9m} e_4 e_6 \le \tfrac{e_6^2}{32} + 8\bar{x}_9^2 e_4^2 \\
&\gamma_1 e_2 e_9 \le 0,5\gamma_1 (e_1^2 + e_9^2) \le 0,25\gamma_1 (e_1^4 + e_9^4), -x_{9m} e_4 e_7 \le \tfrac{e_7^2}{32} + 8\bar{x}_9^2 e_4^2 \\
&\gamma_2 e_2 e_3 \le 0,5\gamma_2 (e_2^2 + e_3^2) \le 0,25\gamma_2 (e_2^4 + e_3^4), -b_3 x_{1m} e_3 e_5 \le 0,25 b_3 \bar{x}_1 (e_3^4 + e_5^4) \\
&\gamma_3 e_3 e_8 \le 0,5\gamma_2 (e_3^2 + e_8^2) \le 0,25\gamma_2 (e_3^4 + e_8^4), -2x_{7m} e_5 e_8 \le 0,5\bar{x}_7 (e_5^4 + e_8^4) \\
&\gamma_4 e_4 e_9 \le 0,5\gamma_2 (e_4^2 + e_9^2) \le 0,25\gamma_2 (e_4^4 + e_9^4), x_{9m} e_2 e_8 \le 0,25 b_3 \bar{x}_9 (e_2^4 + e_8^4) \\
&\gamma_5 e_6 e_9 \le 0,5\gamma_2 (e_6^2 + e_9^2) \le 0,25\gamma_2 (e_6^4 + e_9^4), b_3 x_{3m} e_1 e_5 \le 0,25 b_3 \bar{x}_3 (e_1^4 + e_5^4) \\
&\gamma_6 e_2 e_4 \le 0,5\gamma_2 (e_2^2 + e_4^2) \le 0,25\gamma_2 (e_2^4 + e_4^4), x_{9m} e_2 e_6 \le 0,25\bar{x}_9 (e_2^4 + e_6^4) \\
&\gamma_7 e_1 e_7 \le 0,5\gamma_2 (e_1^2 + e_7^2) \le 0,25\gamma_2 (e_1^4 + e_7^4), 2x_{8m} e_5 e_7 \le 0,5\bar{x}_8 (e_5^4 + e_7^4)
\end{aligned} \tag{3.15}$$

Então, utilizando as Hipótese 1 e 2, o Fato 1 e (3.15), a equação (3.14) implica

$$\dot{V} \le -\rho_1 e_1^2 - \rho_2 e_2^2 - \rho_3 e_3^2 - \rho_4 e_4^2 - \rho_5 e_5^2 - \rho_6 e_6^2 - \rho_7 e_7^2 - \rho_8 e_8^2 - \rho_9 e_9^2 + \beta + \gamma \|e\|^4 \tag{3.16}$$

Considere que $\rho_{10} = \min\{\rho_1\ ,\ \rho_2\ ,\ \rho_3\ ,\ \rho_4\ ,\ \rho_5\ ,\ \rho_6\ ,\ \rho_7\ ,\ \rho_8\ ,\ \rho_9\}$. Uma vez que $\rho_1, \rho_2, \rho_{3,}\rho_5, \rho_6, \rho_7, \rho_8, \rho_9$ são todos positivos e que Ψ é arbitrário, é possível escolhê-lo de forma que ρ_4 seja positivo e, consequentemente, ρ_{10} também seja positivo, assim

$$\dot{V} \leq -\rho_{10}\|e\|^2 + \beta + \gamma\|e\|^4 \tag{3.17}$$

Com base na Hipótese 3, a desiguladade anterior implica

$$\dot{V} \leq -\rho\|e\|^2 + \beta \tag{3.18}$$

Note que isso é verdadeiro no tempo inicial. No entanto, uma consequência disso é que $\dot{V} \leq 0$ quando $\|e\| > \sqrt{\frac{\beta}{\rho}} := \theta$. Uma vez que ao longo do tempo o erro se mantenha suficientemente pequeno de forma que $-\rho_{10}\|e\|^2 + \gamma\|e\|^4 \leq -\rho\|e\|^2$ permaneça verdadeiro com o passar do tempo, pode-se assumir que (3.18) continuará sendo válido mesmo após os momentos iniciais. Para isso se verdadeiro, é necessário considerar $\theta \leq \alpha$, conforme estabelecido na Hipótese 3.

Observe que como θ é constante, pode-se afirmar que o erro de sincronização é limitado. Definindo o conjunto compacto $\Omega = \{e \in \Re^9 | \|e\| \leq \theta\}$, então se pode afirmar que se por qualquer razão $\|e\|$ deixar o conjunto residual Ω, $\dot{V}$ se torna negativo definido e força a convergência do erro de sincronização para o conjunto residual Ω. Conclui-se dessa maneira que o erro de sincronização é limitado e converge para uma bola com raio igual a θ

Comentário 3: Pode-se observar pela prova que distúrbios limitados já foram considerados. É importante notar que o valor de β poderia ser diminuído na prova caso o valor de ψ for maior, ou seja, o valor ψ pode parcialmente influenciar o valor de β e consequentemente o valor de θ. Desse modo a partir da escolha de parâmetros de projeto do controlador pode se levar a um erro de sincronização próximo de zero, mesmo que na presença de distúrbios limitados.

Comentário 4: Convém ressaltar que o esquema proposto, ao contrário das abordagens precursoras permite o ajuste arbitrário da velocidade da sincronização, o que pode ser feito através do parâmetro psi. Adicionalmente, o algoritmo proposto considera um controle escalar e a presença de distúrbios em todos os estados, o que, até onde os autores conhecem, não é considerado na literatura.

Comentário 5: Para aplicações em telecomunicação segura é necessário que a mensagem seja transmitida a partir de estados onde não haja o sinal de controle. Isso ocorre porque o estado onde está o controle não consegue diferenciar distúrbios no sistema mestre da mensagem e os distúrbios no estado onde está o sinal de controle, se não forem imensos, costumam ser eliminados em função da existência desse sinal de controle.

Comentário 6: A estrutura da prova seguiu na seguinte lógica. O sistema hipercaótico é apresentado na equação (3.1) esse sistema foi retirado (WANG, P. et al., 2011) onde foram realizados os testes necessários para comprovar que de fato esse sistema é hipercaótico. Na equação (3.3) e (3.4) define-se o sistema mestre e escravo respectivamente, no mestre não é acoplado nada em seus estados, no escravo vai o controle no quarto estado e todos os distúrbios limitado em cada um dos estados. Existem outros métodos na literatura em que é usado o sistema mestre para colocar distúrbios e até mesmo o sinal de controle(VARAN; AKGUL, 2018), nesta prova optou-se por usar a mesma metodologia que é usada nas simulações, coloca-se a mensagem, distúrbio e controle no sistema escravo com as condições inicias diferentes, após as sincronização dos sistemas faz-se a diferencia de ambos e recupera-se a mensagem.

Comentário 7: Na hipótese 1 formula-se que o distúrbio deve ser limitado, que é uma hipótese usual na literatura. Em (3.7) apresenta-se a derivada do erro de sincronização, não foi deixado nenhum termo em função do sistema escravo, pois esses termos podem ser resgatados a qualquer momento de acordo com a equação (3.6).

Comentário 8: Na hipótese 2 é desejável que o controlador do quarto estado supra o erro de sincronização dos outros estados. Em (3.10) primeiramente formula-se um método para compensar o peso do controlador com uma equação de proporcionalidade simples derivada de $(a \mp b)^2$, em (3.11) formula-se a lei de controle necessária para esse sistema visto que não existe nenhum erro de sincronização com um termo entre as variáveis de estado maior que um termo cúbico, formula-se uma lei de controle com maior expoente da mesma.

Capítulo 4

Simulações

Neste capítulo são apresentadas simulações computacionais visando validar a lei de controle (3.10) para o sistema (3.3) - (3.4) e a transmissão segura de uma mensagem por codificação/-decodificação. Dentre as validações proporcionadas nessas simulações apresentam-se: Sincronização de dois sistemas hipercaóticos específicos, erro de sincronização para uma região próxima da origem de um sistema com nove estados, transmissão segura de uma mensagem, aplicabilidade da transmissão segura de uma mensagem levando em consideração distúrbios, erro do canal, engenharia reversa.

4.1 Simulação usando Matlab/Simulink

Escolheram-se os parâmetros α e ψ como sendo $\alpha = 1$ e $\psi = 100$ e uma janela de simulação de 100 s.

Para validar o esquema de sincronização foram realizadas simulações computacionais para os sistemas (3.3) - (3.4). Utilizou-se para isso o software Matlab/Simulink com o método ODE 113 com passo variável. Foi considerado como condições iniciais no sistema mestre $x_1m(0) = 0,1; x_2m(0) = -1; x_3m(0) = 1,7; x_4m(0) = 2,5; x_5m(0) = -1,2; x_6m(0) = 1,9; x_7m(0) = 2; x_8m(0) = 2,5; x_9m(0) = 3$ e no sistema escravo $x_1s(0) = 0,8; x_2s(0) = -0,7; x_3s(0) = 1,5; x_4s(0) = 2,2; x_5s(0) = -1,1; x_6s(0) = 2,9; x_7s(0) = 1; x_8s(0) = 1,9; x_9s(0) = 2,9$.

Para sincronização dos sistemas mestre e o escravo utilizou-se a lei de controle (3.10). Os distúrbios considerados foram $h_1 = 0.5cos(6t), h_2 = 3cos(10t), h_3 = sen(7t), h_4 = 0,6sen(t), h_5 = 0,7sen(5t), h_6 = 0,9sen(9t), h_7 = 0,1sen(8t), h_8 = 0,2sen(2t)eh_9 = 8sen(4t)$.

As características dos sistemas dinâmicos caóticos os tornam úteis para codificação de canais em aplicações de comunicação. Para ilustrar isso foi previsto um erro no canal com o objetivo tipicamente de codificar as informações no transmissor de modo a permitir a reconstrução no receptor com o mínimo possível de distorção. Esses distúrbios proporcionam uma maior validez para o sistema pois leva-se em consideração o mundo real. O erro do canal nas simulações foi de $0,0005sen(t)$, inserido no quarto estado do sistema. Simulou-se a codificação e restauração de uma mensagem para que se pudesse analisar a eficiência e a robustez do sistema sigiloso de comunicação proposto. A mensagem criptografada foi uma senoide

As figuras 4.1 - 4.9 mostram os resultados da sincronização obtida no MATLAB. Percebe-se que há na figura 4.1 uma discrepância entre os sinais no mestre e no escravo, isso é esperado uma vez que o sistema escravo sincroniza com o estado mestre sem a mensagem, como a figura 4.1 mostra o sistema mestre com a mensagem, a discrepância mostrada nessa figura é a própria mensagem.

Nas figuras 4.2 – 4.9 mostram-se a sincronização dos outros estados, como não há mensagem sendo transmitida nesses estados, a sincronização, como esperado, teve um desempenho satisfatório, com erros de sincronização muito pequenos tais erros pequenos são esperados pois foi considerado 1) presença de perturbações externas (interferência no canal) e 2) a presença de perturbação interna (dinâmica não modelada). Tais erros que tendem a valores próximo de zero são apresentados nas figuras 4.10 - 4.18.

Na figura 4.19 apresenta-se a mensagem sigilosa uma senoide. Na figura 4.20 pode-se observar a comparação entre a mensagem codificada (sinal do estado x_m acrescentado da mensagem) e a mensagem original (aquela que se quer transmitir). A figura 4.21 mostra a mensagem original e a mensagem recuperada.

A mensagem recuperada é obtida a partir da diferença entre x_s e a mensagem codificada. Como esperado a diferença entre as duas mensagens é muito pequena, demonstrando o correto funcionamento do sincronizador. Repare que é inserido o contexto da engenharia reversa onde tem-se o problema da mensagem que foi criptografada, e para decriptografar é preciso fazer a análise oriunda das técnicas inseridas que nesse caso trata-se da sincronização do sistema em questão.

Na figura 4.22 apresenta-se o erro da mensagem, que é a diferença entre mensagem original e a criptografada, tal erro tende a valores próximo de zero, o que é esperado.

Note que apesar do controle estar presente somente no quarto estado e que há distúrbios em todos os estados, mesmo assim os estados apresentaram desempenho satisfatório em termos de sincronização e que a mensagem no estado x_1 foi corretamente decodificada. Note que se precisasse de um resultado ainda melhor, é possível melhorar o processo de reconstrução da mensagem aumentando o valor do parâmetro ψ. Também é possível escalonar o sistema no tempo para assegurar uma sincronização mais rápida de forma que o ψ não apresente um valor muito alto.

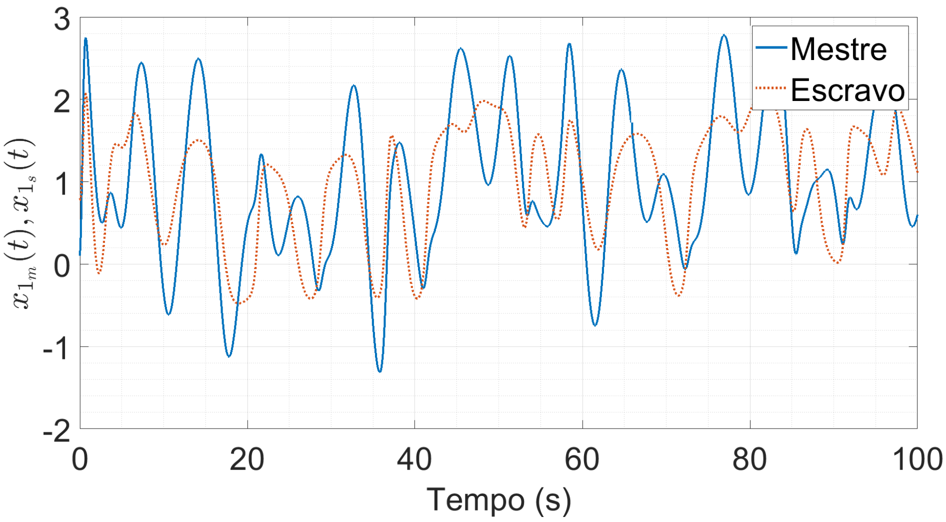

Figura 4.1: Desempenho na sincronização de x_1s.

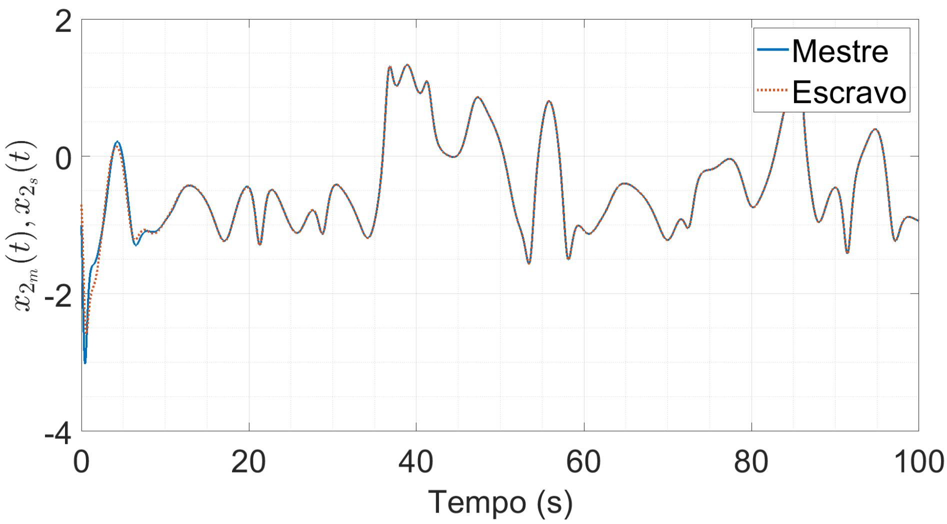

Figura 4.2: Desempenho na sincronização de x_2s.

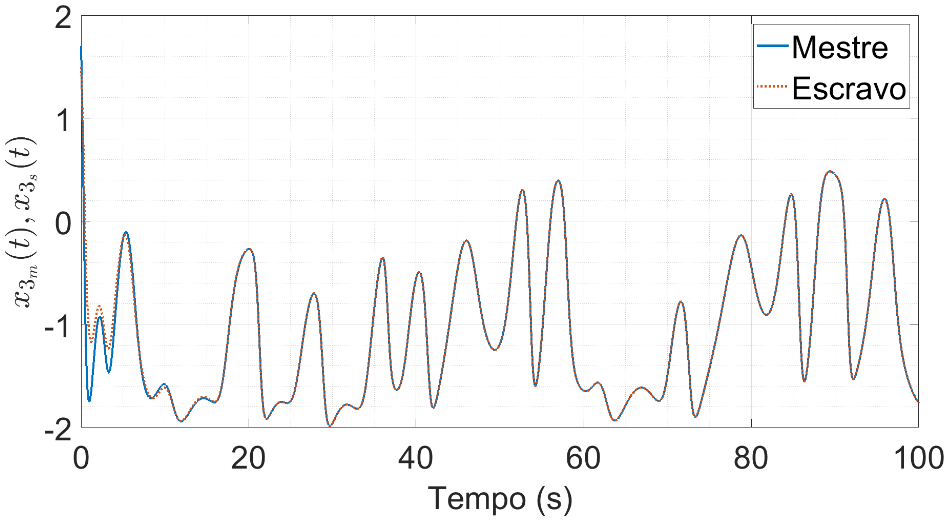

Figura 4.3: Desempenho na sincronização de x_3s.

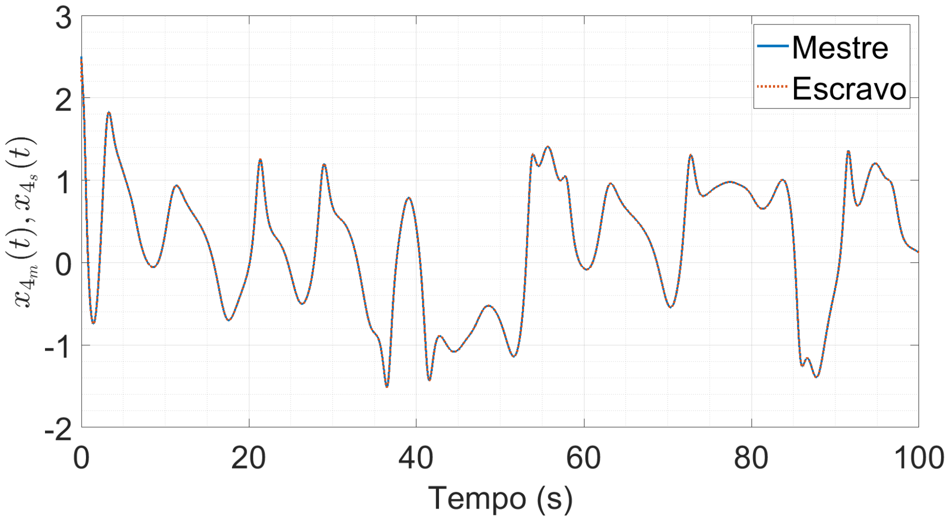

Figura 4.4: Desempenho na sincronização de x_4s.

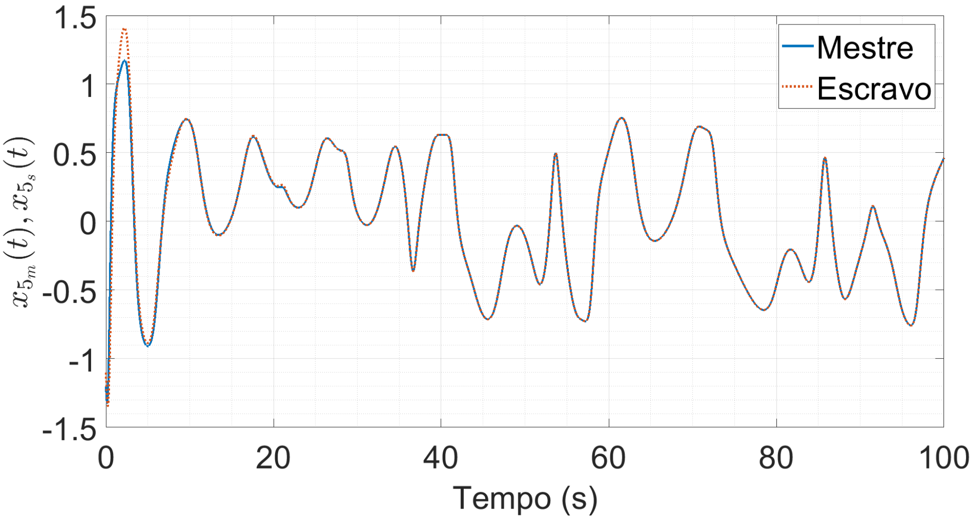

Figura 4.5: Desempenho na sincronização de x_5s.

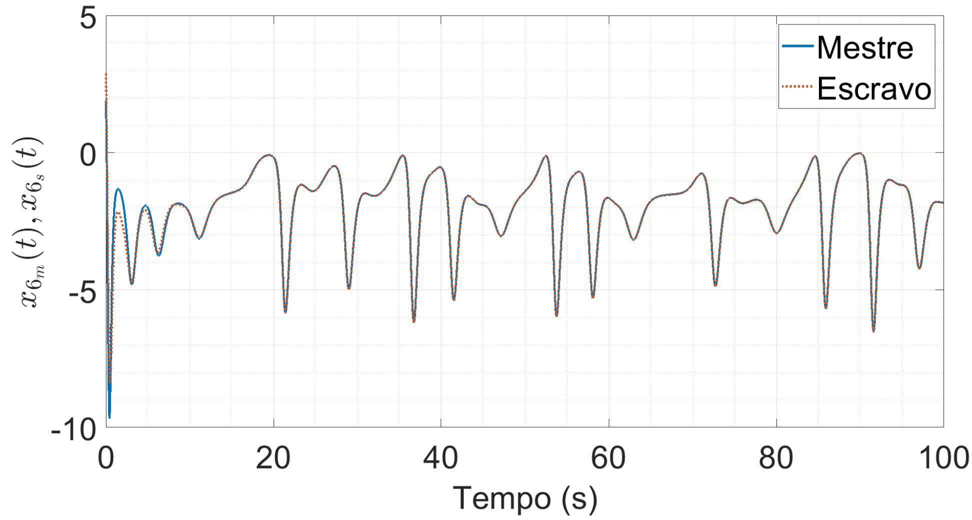

Figura 4.6: Desempenho na sincronização de x_6s.

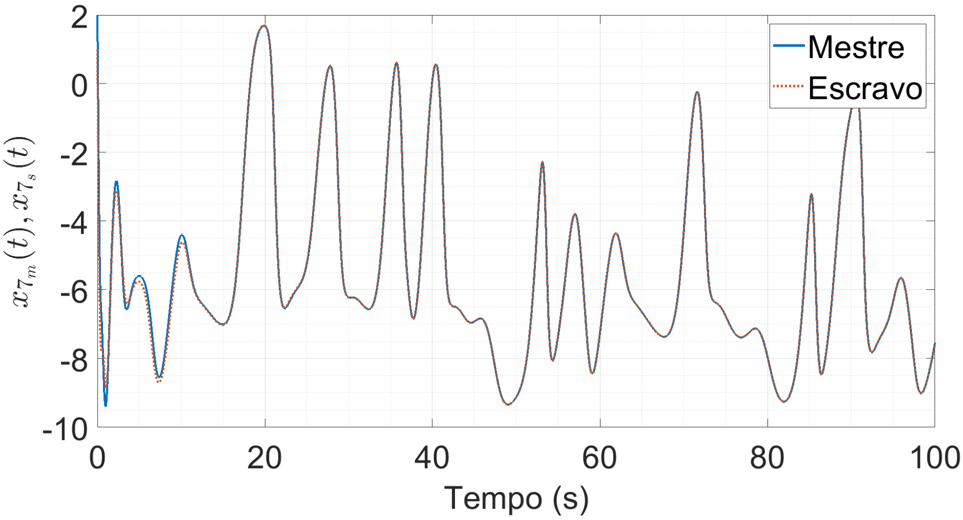

Figura 4.7: Desempenho na sincronização de x_7s.

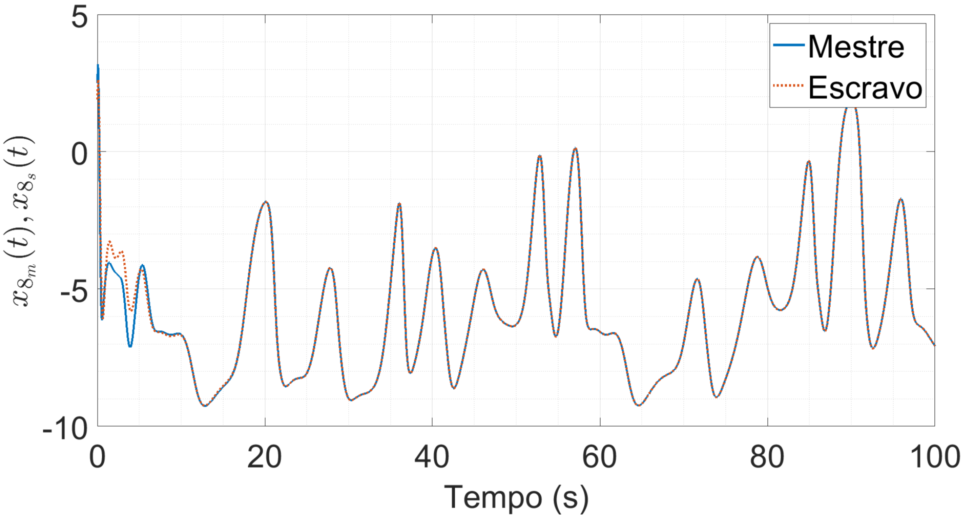

Figura 4.8: Desempenho na sincronização de x_8s.

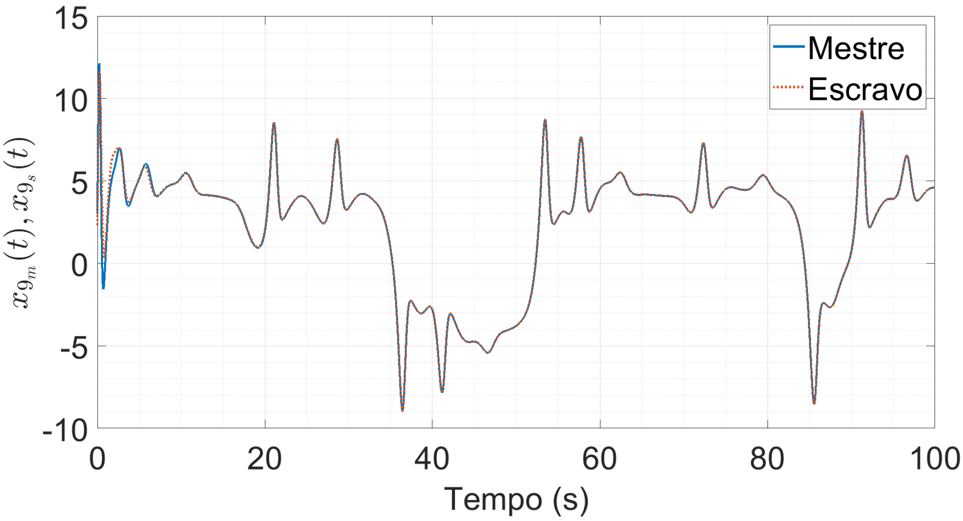

Figura 4.9: Desempenho na sincronização de x_9s.

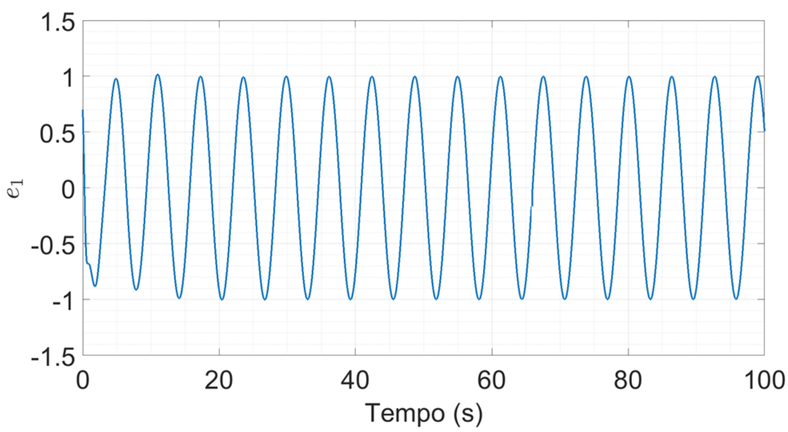

Figura 4.10: Erro de sincronização do primeiro estado e_1.

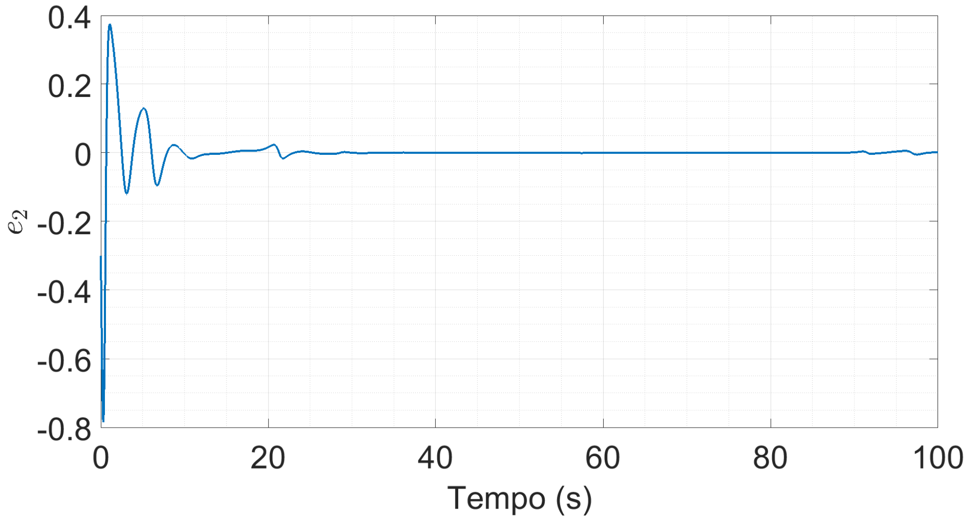

Figura 4.11: Erro de sincronização do segundo estado e_2.

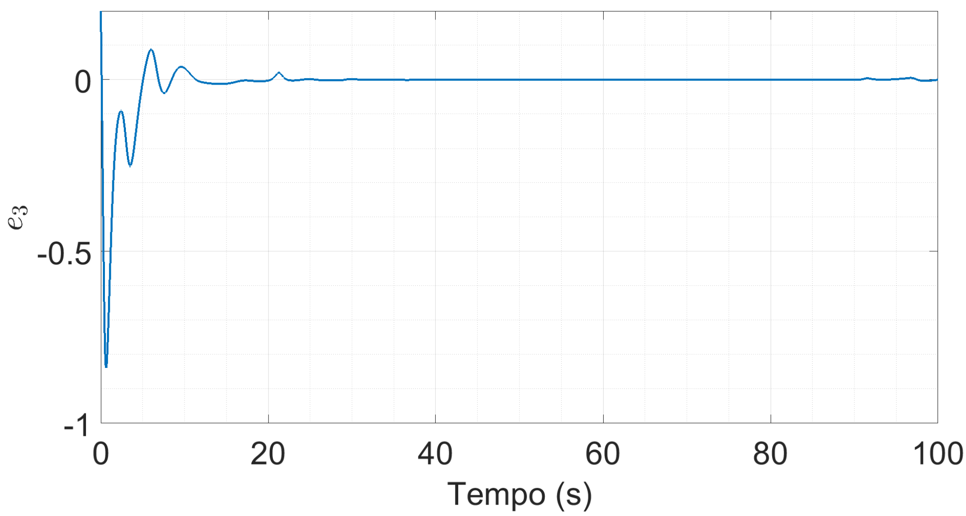

Figura 4.12: Erro de sincronização do terceiro estado e_3.

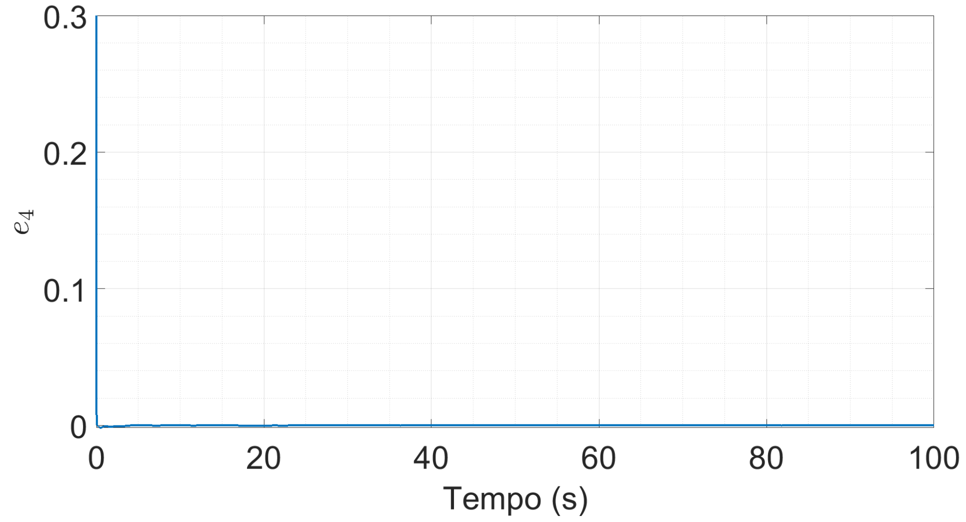

Figura 4.13: Erro de sincronização do quarto estado e_4.

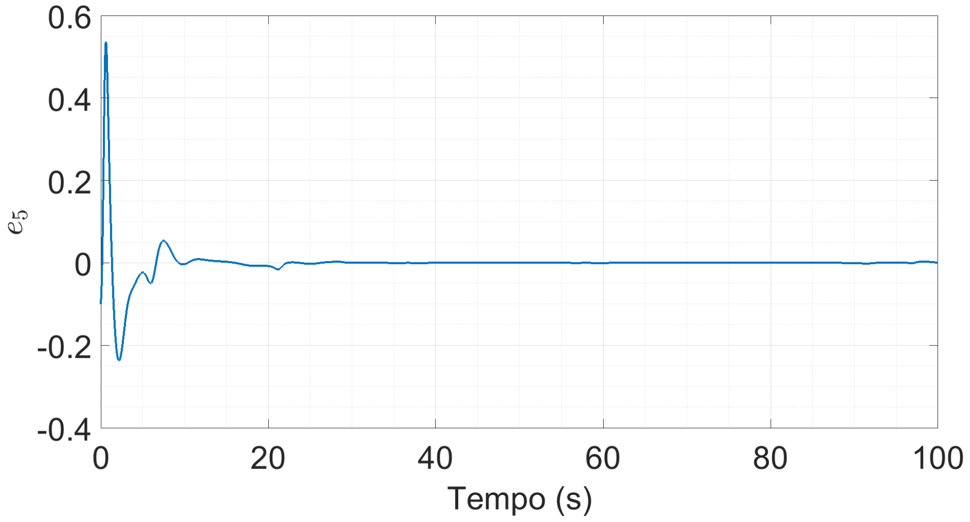

Figura 4.14: Erro de sincronização do quinto estado e_5.

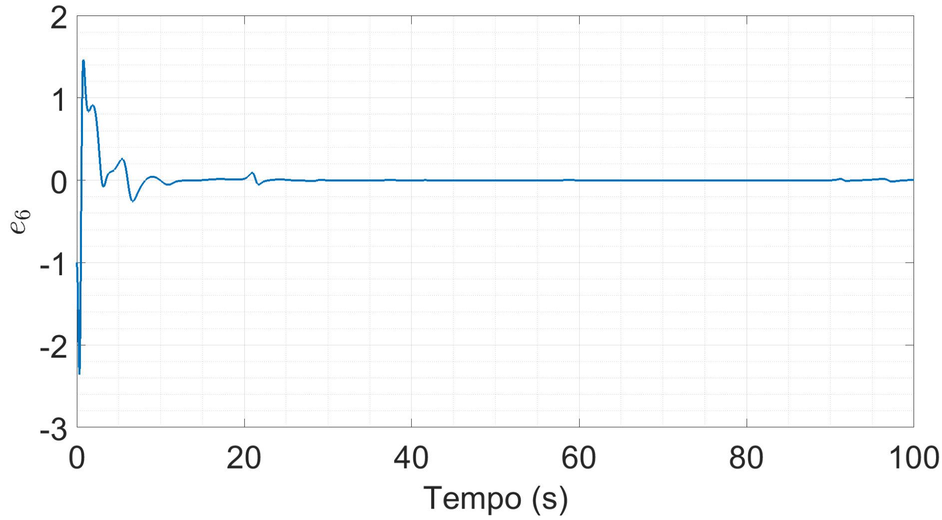

Figura 4.15: Erro de sincronização do sexto estado e_6.

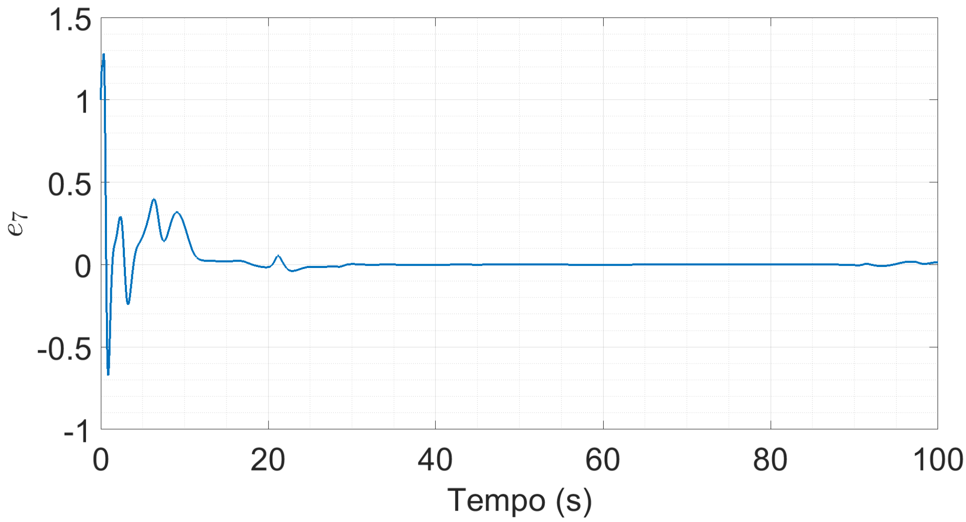

Figura 4.16: Erro de sincronização do sétimo estado e_7.

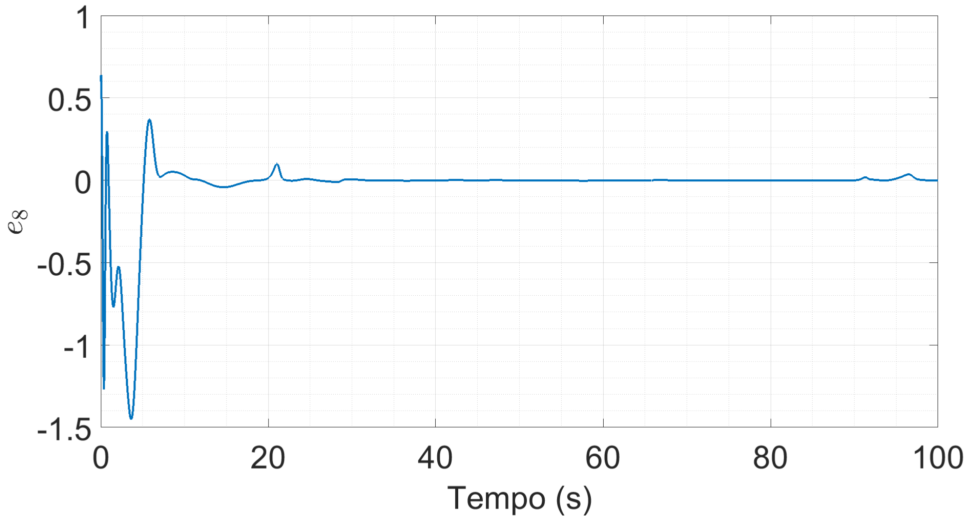

Figura 4.17: Erro de sincronização do oitavo estado e_8.

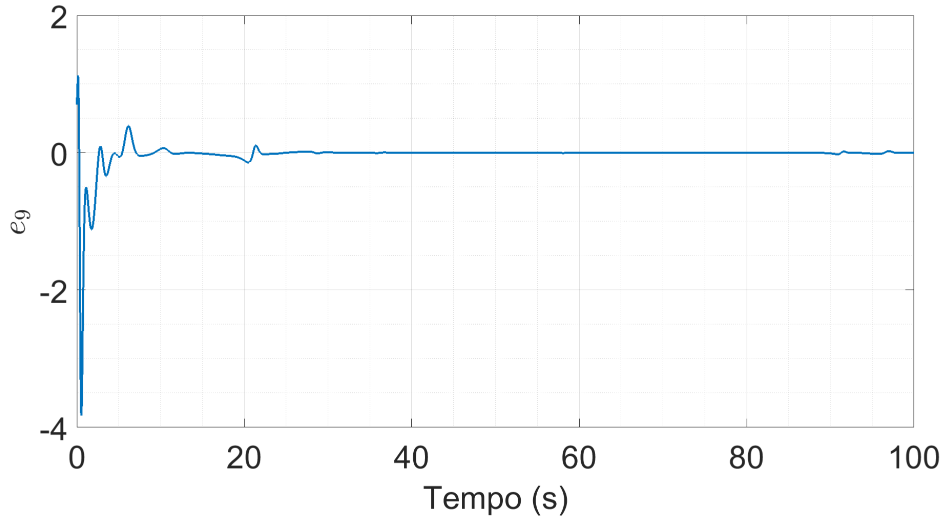

Figura 4.18: Erro de sincronização do nono estado e_9.

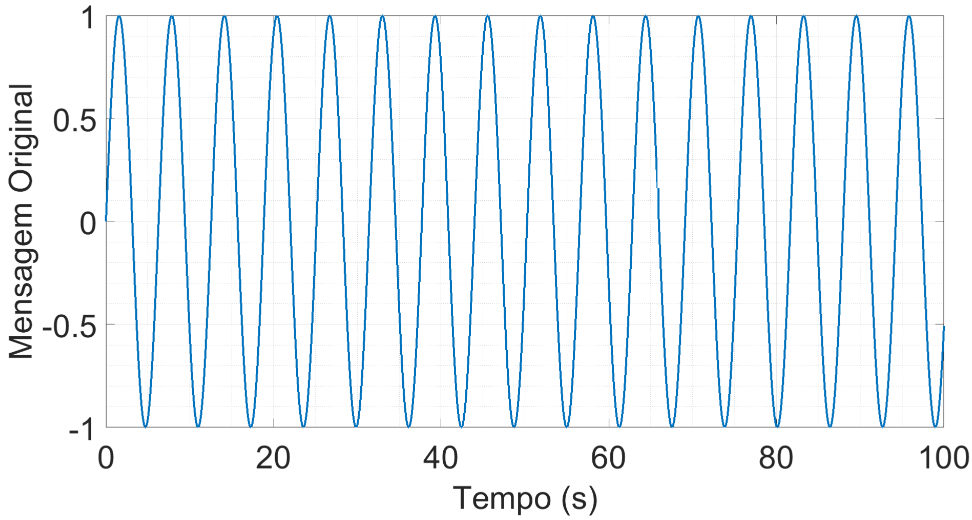

Figura 4.19: Mensagem original.

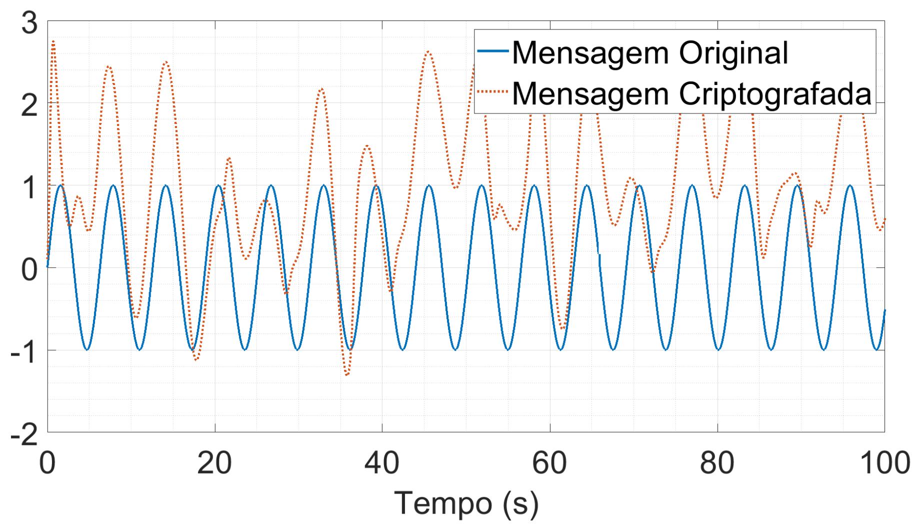

Figura 4.20: Mensagem original e mensagem Criptografada.

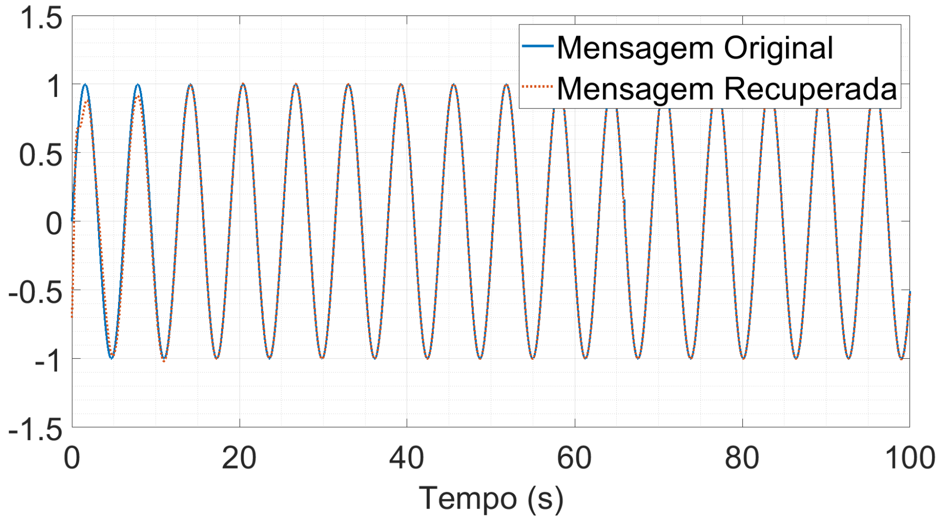

Figura 4.21: Mensagem recuperada.

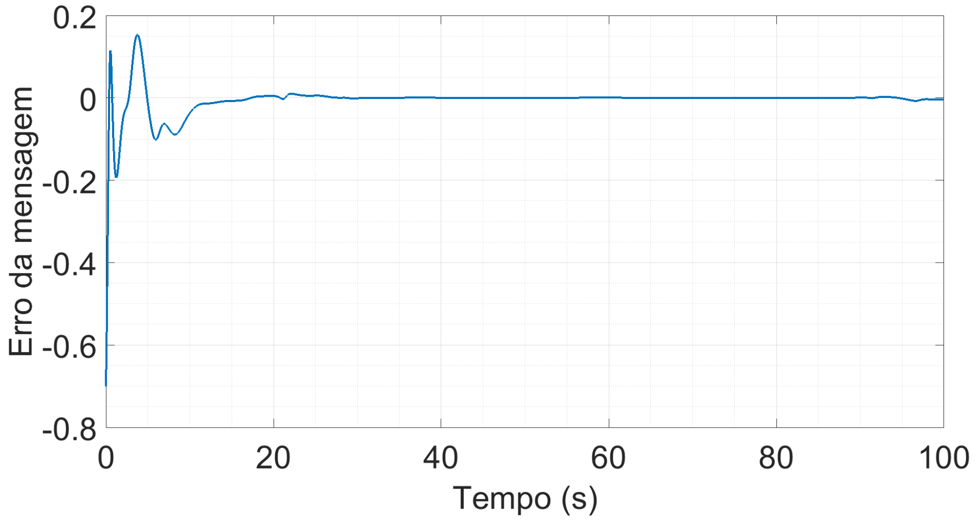

Figura 4.22: Diferencia entre a mensagem recupera e a original.

Capítulo 5

Conclusões

Neste trabalho foi apresentado um tema que vem despertando interesse no meio científico, a criptografia segura baseada em caos. Diversos trabalhos de esquema de comunicação segura, são facilmente encontrados na literatura, poucos como esse, que leva em consideração um sistema nonodimencional que tem um nível de complexidade maior que um caótico. Verifica-se que esse tipo de sistema tecnológico se baseia na sincronização de sistemas hipercaóticos que tem como objetivo criptografar/descriptografar os dados transmitidos por meio de um sistema mestre, usado para codificar, e um decodificador também caótico mas com condições iniciais diferentes do mestre, sendo este escravo.

Para uma certificação prática da sincronização e criptografia caótica, foram realizadas simulações numéricas objetivando-se avaliar a influência de distúrbios e a criptografia de mensagem, os parâmetros dos objetos e desempenho dos algoritmos também foram comprovados. Utilizou-se sistemas caóticos em todas as simulações e nos gráficos foram comparados ambos os sistemas, mestre e escravo. Também foram plotados o erro de sincronização de cada estado tal erro teve a resposta satisfatória convergindo para um valor próximo de zero. A maior contribuição do trabalho está no fato de que foi usado controle em um estado dentre os nove presentes nesse sistema, em outra palavar trata-se da implementação de um sistema subatuado, nenhum resultado como esse foi apresentado dentre os estudos utilizados nesta monografia.

Com base na teoria de estabilidade de Lyapunov no terceiro cápitulo foi provado o erro de sincronização para um sistema particular nonodimensional subatuado sujeito a distúrbios. Provou-se que somente é necessário o ajuste de um controle para a sincronização completa dos sistemas mestre e escravo. Validou-se essa aplicabilidade com simulações computacionais. Assim como aplicação para sistemas seguro de informação.

Todos os resultados apresentados foram reportados no 25$\circ$ Congresso de iniciação cientifica do distrito federal (PIBIC) 2019. O trabalho recebeu a premiação de menção honrosa por sua contribuição na área (ROCHA; VARGAS; GULARTE, Outubro de 2019).

Como sugestão para trabalhos futuros apresenta-se os seguintes

- Para a validação com componentes reais primeiro é preciso fazer a implementação desse sistema com componentes analógicos usando um simulador virtual tal como NI Multisim, Circuito Maker entre outros.
- Simplificação dos algoritmos desse trabalho para que a implementação com circuitos reais não fique com um preço elevado.
- O estudo de novos algoritmos de sincronização mais avançados que estão sendo desenvolvidos no ambiente científico.

Referências

AKEMANN, G.; BURDA, Z.; KIEBURG, M. From integrable to chaotic systems: Universal local statistics of Lyapunov exponents. *EPL (Europhysics Letters)*, IOP Publishing, v. 126, n. 4, p. 40001, 2019.

BARBOZA, R. Hyperchaos in a Chua's circuit with two new added branches. *International Journal of Bifurcation and Chaos*, World Scientific, v. 18, n. 04, p. 1151–1159, 2008.

BOCCALETTI, S. et al. The synchronization of chaotic systems. *Physics reports*, Elsevier, v. 366, n. 1-2, p. 1–101, 2002.

BOWONG, S. Stability analysis for the synchronization of chaotic systems with different order: application to secure communications. *Physics Letters A*, Elsevier, v. 326, n. 1-2, p. 102–113, 2004.

CHAI, X. et al. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Computing and Applications*, Springer, v. 31, n. 1, p. 219–237, 2019.

CHEN, L.; AIHARA, K. Chaotic simulated annealing by a neural network model with transient chaos. *Neural networks*, Elsevier, v. 8, n. 6, p. 915–930, 1995.

CHEN, S.; LÜ, J. Synchronization of an uncertain unified chaotic system via adaptive control. *Chaos, Solitons & Fractals*, Pergamon, v. 14, n. 4, p. 643–647, 2002.

CUOMO, K. M.; OPPENHEIM, A. V. Circuit implementation of synchronized chaos with applications to communications. *Physical review letters*, APS, v. 71, n. 1, p. 65, 1993.

CUOMO, K. M.; OPPENHEIM, A. V.; STROGATZ, S. H. Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on circuits and systems II: Analog and digital signal processing*, IEEE, v. 40, n. 10, p. 626–633, 1993.

FENG, D. et al. The synchronization method for fractional-order hyperchaotic systems. *Physics Letters A*, Elsevier, v. 383, n. 13, p. 1427–1434, 2019.

GONG, L. et al. An image compression and encryption algorithm based on chaotic system and compressive sensing. *Optics & Laser Technology*, Elsevier, v. 115, p. 257–267, 2019.

HASLER, M. Synchronization of chaotic systems and transmission of information. *International Journal of Bifurcation and Chaos*, World Scientific, v. 8, n. 04, p. 647–659, 1998.

HE, R.; VAIDYA, P. Implementation of chaotic cryptography with chaotic synchronization. *Physical Review E*, APS, v. 57, n. 2, p. 1532, 1998.

HUA, C.; GUAN, X. Adaptive control for chaotic systems. *Chaos, Solitons & Fractals*, Elsevier, v. 22, n. 1, p. 55–60, 2004.

IOANNOU, P. A.; SUN, J. *Robust adaptive control*. [S.l.]: Courier Corporation, 2012.

JAKIMOSKI, G.; KOCAREV, L. Chaos and cryptography: block encryption ciphers based on chaotic maps. *Ieee transactions on circuits and systems i: fundamental theory and applications*, IEEE, v. 48, n. 2, p. 163–169, 2001.

JIA, H.-Y.; CHEN, Z.-Q.; QI, G.-Y. Topological horseshoe analysis and the circuit implementation for a four-wing chaotic attractor. *Nonlinear Dynamics*, Springer, v. 65, n. 1-2, p. 131–140, 2011.

JIA, Q. Hyperchaos generated from the Lorenz chaotic system and its control. *Physics Letters A*, Elsevier, v. 366, n. 3, p. 217–222, 2007.

JOVIC, B. *Synchronization techniques for chaotic communication systems*. [S.l.]: Springer Science & Business Media, 2011.

KAI, G. et al. Hopf bifurcation, positively invariant set, and physical realization of a new four-dimensional hyperchaotic financial system. *Mathematical Problems in Engineering*, Hindawi, v. 2017, 2017.

KHALIL, H. K. *Nonlinear Systems*. [S.l.]: Upper Saddle River, 2002.

KOLUMBÁN, G.; KENNEDY, M. P.; CHUA, L. O. The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, IEEE, v. 45, n. 11, p. 1129–1140, 1998.

LI, C.; LIAO, X.; WONG, K.-w. Lag synchronization of hyperchaos with application to secure communications. *Chaos, Solitons & Fractals*, Elsevier, v. 23, n. 1, p. 183–193, 2005.

LI, G.-H. Modified projective synchronization of chaotic system. *Chaos, Solitons & Fractals*, Elsevier, v. 32, n. 5, p. 1786–1790, 2007.

LI, X.; FAN, X. et al. Adaptive Control of a Four-Dimensional Hyperchaotic System. *Asian Research Journal of Mathematics*, p. 1–17, 2019.

MATOUK, A.; ELSADANY, A. Achieving synchronization between the fractional-order hyperchaotic Novel and Chen systems via a new nonlinear control technique. *Applied Mathematics Letters*, Elsevier, v. 29, p. 30–35, 2014.

MEZATIO, B. A. et al. A novel memristive 6D hyperchaotic autonomous system with hidden extreme multistability. *Chaos, Solitons & Fractals*, Elsevier, v. 120, p. 100–115, 2019.

MUKHERJEE, N.; PORIA, S. Preliminary concepts of dynamical systems. *Int. J. Appl. Math. Res*, v. 1, n. 4, p. 751–770, 2012.

AL-OBEIDI, A. S.; AL-AZZAWI, S. F. Complete synchronization of a novel 6-D hyperchaotic Lorenz system with known parameters. *International Journal of Engineering & Technology*, v. 7, n. 4, p. 5345–5349, 2018.

OUANNAS, A.; AZAR, A. T.; VAIDYANATHAN, S. A robust method for new fractional hybrid chaos synchronization. *Mathematical Methods in the Applied Sciences*, Wiley Online Library, v. 40, n. 5, p. 1804–1812, 2017.

PECORA, L. M.; CARROLL, T. L. Synchronization in chaotic systems. *Physical review letters*, APS, v. 64, n. 8, p. 821, 1990.

QI, G. et al. On a new hyperchaotic system. *Physics Letters A*, Elsevier, v. 372, n. 2, p. 124–136, 2008.

ROCHA, D. V.; VARGAS, J. A. R.; GULARTE, K. H. M. Criptografia baseada em caos: aplicação usando um sistema hipercaótico. *Congresso de iniciação cientifica do DF*, p. 1–10, Outubro de 2019.

ROSSLER, O. An equation for hyperchaos. *Physics Letters A*, Elsevier, v. 71, n. 2-3, p. 155–157, 1979.

SABAGHIAN, A.; BALOCHIAN, S. Parameter estimation and synchronization of hyper chaotic Lu system with disturbance input and uncertainty using two under-actuated control signals. *Transactions of the Institute of Measurement and Control*, SAGE Publications Sage UK: London, England, v. 41, n. 6, p. 1729–1739, 2019.

SINGH, J. P.; ROY, B. Hidden attractors in a new complex generalised Lorenz hyperchaotic system, its synchronisation using adaptive contraction theory, circuit validation and application. *Nonlinear Dynamics*, Springer, v. 92, n. 2, p. 373–394, 2018.

SMAOUI, N.; KAROUMA, A.; ZRIBI, M. Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems. *Communications in Nonlinear Science and Numerical Simulation*, Elsevier, v. 16, n. 8, p. 3279–3293, 2011.

STROGATZ, S. H. *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. [S.l.]: CRC Press, 2018.

TANG, Y.; MEES, A.; CHUA, L. Synchronization and chaos. *IEEE Transactions on Circuits and Systems*, IEEE, v. 30, n. 9, p. 620–626, 1983.

TAVAZOEI, M. S.; HAERI, M. An optimization algorithm based on chaotic behavior and fractal nature. *Journal of Computational and Applied Mathematics*, Elsevier, v. 206, n. 2, p. 1070–1081, 2007.

THAMILMARAN, K.; LAKSHMANAN, M.; VENKATESAN, A. Hyperchaos in a modified canonical Chua's circuit. *International Journal of Bifurcation and Chaos*, World Scientific, v. 14, n. 01, p. 221–243, 2004.

TLELO-CUAUTLE, E. et al. Application of a chaotic oscillator in an autonomous mobile robot. *Journal of Electrical Engineering*, De Gruyter Open, v. 65, n. 3, p. 157–162, 2014.

TREJO-GUERRA, R. et al. A survey on the integrated design of chaotic oscillators. *Applied Mathematics and Computation*, Elsevier, v. 219, n. 10, p. 5113–5122, 2013.

UMOH, E. A.; TOLA, O. J. Adaptive Synchronization and Parameter Estimation of a 5D Hyperchaotic System with Unknown System Parameters. *International Conference on Information and Communication Technology and Its Applications*, Springer, v. 2, n. 2, p. 521–527, 2018.

VAIDYANATHAN, S.; VOLOS, C. K.; KYPRIANIDIS, I. et al. Analysis, Adaptive Control and Anti-Synchronization of a Six-Term Novel Jerk Chaotic System with two Exponential Nonlinearities and its Circuit Simulation. *Journal of Engineering Science & Technology Review*, v. 8, n. 2, 2015.

VAIDYANATHAN, S.; VOLOS, C. K.; PHAM, V. Analysis, control, synchronization and SPICE implementation of a novel 4-D hyperchaotic Rikitake dynamo system without equilibrium. *Journal of Engineering Science and Technology Review*, v. 8, n. 2, p. 232–244, 2015.

VAIDYANATHAN, S. Generalised projective synchronisation of novel 3-D chaotic systems with an exponential non-linearity via active and adaptive control. *International Journal of Modelling, Identification and Control*, Inderscience Publishers Ltd, v. 22, n. 3, p. 207–217, 2014.

VAIDYANATHAN, S.; AZAR, A. T. Adaptive control and synchronization of Halvorsen circulant chaotic systems. In: ADVANCES in chaos theory and intelligent control. [S.l.]: Springer, 2016. p. 225–247.

VAIDYANATHAN, S.; SAMPATH, S. Anti-synchronization of four-wing chaotic systems via sliding mode control. *International Journal of Automation and Computing*, Springer, v. 9, n. 3, p. 274–279, 2012.

VARAN, M.; AKGUL, A. Control and synchronisation of a novel seven-dimensional hyperchaotic system with active control. *Pramana*, Springer, v. 90, n. 4, p. 54, 2018.

WANG, C.; ZHANG, H.-l.; FAN, W.-h. Generalized dislocated lag function projective synchronization of fractional order chaotic systems with fully uncertain parameters. *Chaos, Solitons & Fractals*, Elsevier, v. 98, p. 14–21, 2017.

WANG, J. et al. A new six-dimensional hyperchaotic system and its secure communication circuit implementation. *International Journal of Circuit Theory and Applications*, Wiley Online Library, 2019.

WANG, P. et al. Ultimate bound estimation of a class of high dimensional quadratic autonomous dynamical systems. *International Journal of Bifurcation and Chaos*, World Scientific, v. 21, n. 09, p. 2679–2694, 2011.

WANG, R. et al. A New Memristor-Based 5D Chaotic System and Circuit Implementation. *Complexity*, Hindawi, v. 2018, 2018.

WEI, X. et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, Elsevier, v. 85, n. 2, p. 290–299, 2012.

WU, X.; CHEN, G.; CAI, J. Chaos synchronization of the master–slave generalized Lorenz systems via linear state error feedback control. *Physica D: Nonlinear Phenomena*, Elsevier, v. 229, n. 1, p. 52–80, 2007.

YANG, J.; ZHU, F. Synchronization for chaotic systems and chaos-based secure communications via both reduced-order and step-by-step sliding mode observers. *Communications in Nonlinear Science and Numerical Simulation*, Elsevier, v. 18, n. 4, p. 926–937, 2013.

YANG, Q.; ZHU, D.; YANG, L. A new 7D hyperchaotic system with five positive Lyapunov exponents coined. *International Journal of Bifurcation and Chaos*, World Scientific, v. 28, n. 05, p. 1850057, 2018.

YANG, T. A survey of chaotic secure communication systems. *International journal of computational cognition*, v. 2, n. 2, p. 81–130, 2004.

YANG, T.; CHUA, L. O. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, IEEE, v. 43, n. 9, p. 817–819, 1996.

YI, L. et al. Dynamical analysis, circuit implementation and deep belief network control of new six-dimensional hyperchaotic system. *Journal of Algorithms & Computational Technology*, SAGE Publications Sage UK: London, England, v. 12, n. 4, p. 361–375, 2018.

YU, H.; LIU, Y. Chaotic synchronization based on stability criterion of linear systems. *Physics Letters A*, Elsevier, v. 314, n. 4, p. 292–298, 2003.

ZHANG, F. et al. Dynamics of a new 5D hyperchaotic system of lorenz type. *International Journal of Bifurcation and Chaos*, World Scientific, v. 28, n. 03, p. 1850036, 2018.

ZHANG, J. et al. Chaos synchronization using single variable feedback based on backstepping method. *Chaos, Solitons & Fractals*, Elsevier, v. 21, n. 5, p. 1183–1193, 2004.

ZHANG, X.; ZHU, H. Anti-synchronization of two different hyperchaotic systems via active and adaptive control. *International Journal of Nonlinear Science*, v. 6, n. 3, p. 216–223, 2008.

Anexo I

Função do Simulink para o cálculo da saída do filtro estatístico acoplado ao PID.

```
Planta_Master.m

function [sys,x0,str,ts] = Planta_Master(t,x,u,flag)


a=1/2;
c=1;
b1=4*(1 + a^2)/(1 + 2*a^2);
b2=(1 + 2*a^2)/(2*(1 + a^2));
b3=2*(1 - a^2)/(1 + a^2);
b4=(a^2)/(1 + a^2);
b5=(8*a^2)/(1 + 2*a^2);
b6=4/(1 + 2*a^2);
mensagem =c*sin(1*t);

sigma=1/2;
r=15.1;

switch flag,


%%%%%%%%%%%%%%%%%%%%
% Inicializacao
%%%%%%%%%%%%%%%%%%%%
case 0,
sizes = simsizes;
sizes.NumContStates = 9  %numero de estados constantes
sizes.NumDiscStates = 0; %numero de estados discretos
sizes.NumOutputs = 9     %numero de saidas
sizes.NumInputs = 0;     %numero de entradas
sizes.DirFeedthrough = 1;
sizes.NumSampleTimes = 1;
sys = simsizes(sizes);
x0=[0.1 -1 1.7 2.5 -1.2 1.9 2 2.5 3]; %Condicoes iniciais
str=[];
ts=[0 0];
```

```
%%%%%%%%%%%%%%%%%
% Diretivas %
%%%%%%%%%%%%%%%%%
case 1,     %Sistema
sys = [-sigma*b1*x(1) - x(2)*x(4) + b4*(x(4)^2) + b3*x(3)*x(5) - sigma*b2*x(7);
-sigma*x(2) + x(1)*x(4) - x(2)*x(5) + x(4)*x(5) - (sigma*x(9))/2;
-sigma*b1*x(3) + x(2)*x(4) - b4*(x(2)^2) - b3*x(1)*x(5) + sigma*b2*x(8);
-sigma*x(4) - x(2)*x(3) - x(2)*x(5) + x(4)*x(5) + sigma*x(9)/2;
-sigma*b5*x(5) + (x(2)^2)/2 - (x(4)^2)/2;
-b6*x(6) + x(2)*x(9) - x(4)*x(9);
-b1*x(7) - r*x(1) + 2*x(5)*x(8) - x(4)*x(9);
-b1*x(8) + r*x(3) - 2*x(5)*x(7) + x(2)*x(9);
-x(9) - r*x(2) + r*x(4) - 2*x(2)*x(6) + 2*x(4)*x(6) + x(4)*x(7) - x(2)*x(8)];

%%%%%%%%%%
% Saida %
%%%%%%%%%%
case 3,
sys = [x(1)+ mensagem ; x(2) ; x(3);x(4);x(5);x(6);x(7);x(8);x(9)];
%%%%%%%%%%
% End %
%%%%%%%%%%
case {2,4,9},
sys = []; % Nao faz nad+a
otherwise
error(['unhandled flag = ',num2str(flag)]);
end


Planta_slave.m
function [sys,x0,str,ts] = Planta_Slave(t,x,u,flag)

a=1/2;

b1=4*(1 + a^2)/(1 + 2*a^2);
b2=(1 + 2*a^2)/(2*(1 + a^2));
b3=2*(1 - a^2)/(1 + a^2);
b4=(a^2)/(1 + a^2);
b5=(8*a^2)/(1 + 2*a^2);
b6=4/(1 + 2*a^2);

sigma=1/2;
r=15.1;
switch flag,


%%%%%%%%%%%%%%%%%%%
% Inicializacao %
```

```
%%%%%%%%%%%%%%%%%%%%%%%
case 0,
sizes = simsizes;
sizes.NumContStates = 9  %numero de estados constantes
sizes.NumDiscStates = 0; %numero de estados discretos
sizes.NumOutputs = 9     %numero de saidas
sizes.NumInputs = 9;     %numero de entradas
sizes.DirFeedthrough = 1;
sizes.NumSampleTimes = 1;
sys = simsizes(sizes);
x0=[0.8 -0.7 1.5 2.2 -1.1 2.9 1 1.9 2.3]; %Condicoes iniciais
str=[];
ts=[0 0];
%%%%%%%%%%%%%%%%%%%
% Diretivas %
%%%%%%%%%%%%%%%%%%%
case 1,     %Sistema
sys = [-sigma*b1*x(1) - x(2)*x(4) + b4*(x(4)^2) + b3*x(3)*x(5) - sigma*b2*x(7) + u(1);
-sigma*x(2) + x(1)*x(4) - x(2)*x(5) + x(4)*x(5) - (sigma*x(9))/2 + u(2);
-sigma*b1*x(3) + x(2)*x(4) - b4*(x(2)^2) - b3*x(1)*x(5) + sigma*b2*x(8) + u(3);
-sigma*x(4) - x(2)*x(3) - x(2)*x(5) + x(4)*x(5) + sigma*x(9)/2 + u(4);
-sigma*b5*x(5) + (x(2)^2)/2 - (x(4)^2)/2 + u(5);
-b6*x(6) + x(2)*x(9) - x(4)*x(9) + u(6);
-b1*x(7) - r*x(1) + 2*x(5)*x(8) - x(4)*x(9) + u(7);
-b1*x(8) + r*x(3) - 2*x(5)*x(7) + x(2)*x(9) + u(8);
-x(9) - r*x(2) + r*x(4) - 2*x(2)*x(6) + 2*x(4)*x(6) + x(4)*x(7) - x(2)*x(8) + u(9)];

%%%%%%%%%%%%
% Saidas %
%%%%%%%%%%%%
case 3,
sys = x;
%%%%%%%%%%%
% End %
%%%%%%%%%%%
case {2,4,9},
sys = []; % nao faz nada
otherwise
error(['unhandled flag = ',num2str(flag)]);
end

sincronizador.m
function isys,x0,str,ts] = Sincronizador(t,x,u,flag)

psi = 1000;

switch flag,
```

```
%%%%%%%%%%%%%%%%%%%%%
% Inicializacao %
%%%%%%%%%%%%%%%%%%%%%
case 0,

sizes = simsizes;
sizes.NumContStates  = 9;   %Numero de estados constantes
sizes.NumDiscStates  = 0;   %Numero de estados discretos
sizes.NumOutputs     = 9;   %Numero de saidas
sizes.NumInputs      = 18;   %Numero de entradas
sizes.DirFeedthrough = 1;
sizes.NumSampleTimes = 1;
sys = simsizes(sizes);
x0=zeros(3,1);              %Condicoes iniciais
x0(1)=0;
x0(2)=0;
x0(3)=0;
x0(4)=0;
x0(5)=0;
x0(6)=0;
x0(7)=0;
x0(8)=0;
x0(9)=0;
str=[];
ts=[0 0];
%%%%%%%%%%%%%%%%%
% Diretivas  %
%%%%%%%%%%%%%%%%%
case 1, %aqui ficariam estimadores dos pesos de uma rede neural caso
    houvesse, nesse caso nao ha
sys = [0;
0;
0;
0;
0;
0;
0;
0;
0];
%%%%%%%%%%%
% Saidas %
%%%%%%%%%%%
case 3,    %controlador
sys =  [-0*(psi*(u(10) - u(1)));
-0*(psi*(u(11) - u(2)));
-0*(psi*(u(12) - u(3)));
-1*(psi*(u(13) - u(4)));
-0*(psi*(u(14) - u(5)));
-0*(psi*(u(15) - u(6)));
-0*(psi*(u(16) - u(7)));
```

```
-0*(psi*(u(17) - u(8)));
-0*(psi*(u(18) - u(9)))];

case {2,4,9},
sys = [];

otherwise
error(['unhandled flag = ',num2str(flag)]);
end

salvar_dados.m
Salva os dados da simulacao (util em simulacoes muito demoradas)
clc
save Backup_dados.mat t Xmaster Xslave
%Para carregar, usar o comando load Backup_dados.mat (e preciso na
%navegacao do matlab estar na mesma pasta que tem esse arquivo)

Graficosmodif.m
%Executando esse arquivo --> automaticamente mostra os graficos da
%simulacao e salva na pasta em formato png (poderia ser escolhido
%formato jpg tambem)
clc
fsize=30;
c = 1;
mensagem = c*sin(1*t);

%Figura 1
fig=figure;
plot(t,Xmaster(:,1),t, Xslave(:,1),':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{1_{m}}(t), x_{1_{s}}(t)$$','Interpreter','Latex','Fontsize',
    fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG1.png');
close(fig)

%Figura 2
fig=figure;
plot(t,Xmaster(:,2),t, Xslave(:,2),':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
```

```
ylabel('$$x_{2_{m}}(t), x_{2_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG2.png');
close(fig)

%Figura 3
fig=figure;
plot(t,Xmaster(:,3),t, Xslave(:,3) ,':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{3_{m}}(t), x_{3_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG3.png');
close(fig)

%Figura 4
fig=figure;
plot(t,Xmaster(:,4),t, Xslave(:,4) ,':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{4_{m}}(t), x_{4_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG4.png');
close(fig)

%Figura 5
fig=figure;
plot(t,Xmaster(:,5),t, Xslave(:,5) ,':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{5_{m}}(t), x_{5_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG5.png');
close(fig)
```

```
%Figura 6
fig=figure;
plot(t,Xmaster(:,6),t, Xslave(:,6),':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{6_{m}}(t), x_{6_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG6.png');
close(fig)

%Figura 7
fig=figure;
plot(t,Xmaster(:,7),t, Xslave(:,7),':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{7_{m}}(t), x_{7_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG7.png');
close(fig)


%Figura 8
fig=figure;
plot(t,Xmaster(:,8),t, Xslave(:,8),':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{8_{m}}(t), x_{8_{s}}(t)$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG8.png');
close(fig)


%Figura 9
fig=figure;
```

```
plot(t,Xmaster(:,9),t, Xslave(:,9),':','LineWidth',2);
grid on
grid minor
h=legend('Mestre','Escravo','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$x_{9_{m}}(t), x_{9_{s}}(t)$$','Interpreter','Latex','Fontsize',
    fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG9.png');
close(fig)


%Figura 10
fig=figure;
aux = Xslave(:,1) - Xslave(:,1);
plot(t,aux,'LineWidth',2);set(0,'DefaultAxesFontSize',fsize);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_1$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG10.png');
close(fig)

%Figura 11
fig=figure;
aux = Xmaster(:,2) - Xslave(:,2);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_2$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG11.png');
close(fig)

%Figura 12
fig=figure;
aux = Xmaster(:,3) - Xslave(:,3);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_3$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
```

```
saveas(gcf,'FIG12.png');
close(fig)

%Figura 13
fig=figure;
aux = Xmaster(:,4) - Xslave(:,4);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_4$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG13.png');
close(fig)

%Figura 14
fig=figure;
aux = Xmaster(:,5) - Xslave(:,5);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_5$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG14.png');
close(fig)

%Figura 15
fig=figure;
aux = Xmaster(:,6) - Xslave(:,6);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_6$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG15.png');
close(fig)

%Figura 16
fig=figure;
aux = Xmaster(:,7) - Xslave(:,7);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
```

```
ylabel('$$e_7$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG16.png');
close(fig)

%Figura 17
fig=figure;
aux = Xmaster(:,8) - Xslave(:,8);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_8$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG17.png');
close(fig)

%Figura 18
fig=figure;
aux = Xmaster(:,9) - Xslave(:,9);
plot(t,aux,'LineWidth',2);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('$$e_9$$','Interpreter','Latex','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG18.png');
close(fig)


%Figura 19
fig=figure;
aux1 = Xmaster(:,1) - Xslave(:,1);
aux2 = Xmaster(:,2) - Xslave(:,2);
aux3 = Xmaster(:,3) - Xslave(:,3);
plot(t,aux1,t,aux2,'-',t,aux3,':','LineWidth',2);
grid on
grid minor
h=legend('e_1','e_2','e_3','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG19.png');
close(fig)

%Figura 20
fig=figure;
```

```
aux1 = Xmaster(:,4) - Xslave(:,4);
aux2 = Xmaster(:,5) - Xslave(:,5);
aux3 = Xmaster(:,6) - Xslave(:,6);
plot(t,aux1,t,aux2,'-',t,aux3,':','LineWidth',2);
grid on
grid minor
h=legend('e_4','e_5','e_6','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG20.png');
close(fig)

%Figura 21
fig=figure;
aux1 = Xmaster(:,7) - Xslave(:,7);
aux2 = Xmaster(:,8) - Xslave(:,8);
aux3 = Xmaster(:,9) - Xslave(:,9);
plot(t,aux1,t,aux2,'-',t,aux3,':','LineWidth',2);
grid on
grid minor
h=legend('e_7','e_8','e_9','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG21.png');
close(fig)

%Figura 22
fig=figure;
plot(t,mensagem,'LineWidth',2);
set(0,'DefaultAxesFontSize',fsize);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('Mensagem Original','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG22.png');
close(fig)

%Figura 23
fig=figure;
plot(t,mensagem,t, Xmaster(:,1),':','LineWidth',2);
grid on
grid minor
h=legend('Mensagem Original','Mensagem Criptografada','Location','northeast
    ');
```

```
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG23.png');
close(fig)

%Figura 24
fig=figure;
aux = Xmaster(:,1) - Xslave(:,1);
plot(t,mensagem,t, aux,':','LineWidth',2);
set(0,'DefaultAxesFontSize',fsize);
grid on
grid minor
h=legend('Mensagem Original','Mensagem Recuperada','Location','northeast');
set(h,'FontSize',fsize);
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG24.png');
close(fig)

%Figura 25
fig=figure;
aux2 = aux - mensagem;
plot(t,aux2,'LineWidth',2);
set(0,'DefaultAxesFontSize',fsize);
grid on
grid minor
set(0,'DefaultAxesFontSize', fsize);
xlabel('Tempo (s)','Fontsize',fsize);
ylabel('Erro da mensagem','Fontsize',fsize)
set(gcf,'units','normalized','outerposition',[0 0 1 1]);
saveas(gcf,'FIG25.png');
close(fig)
```