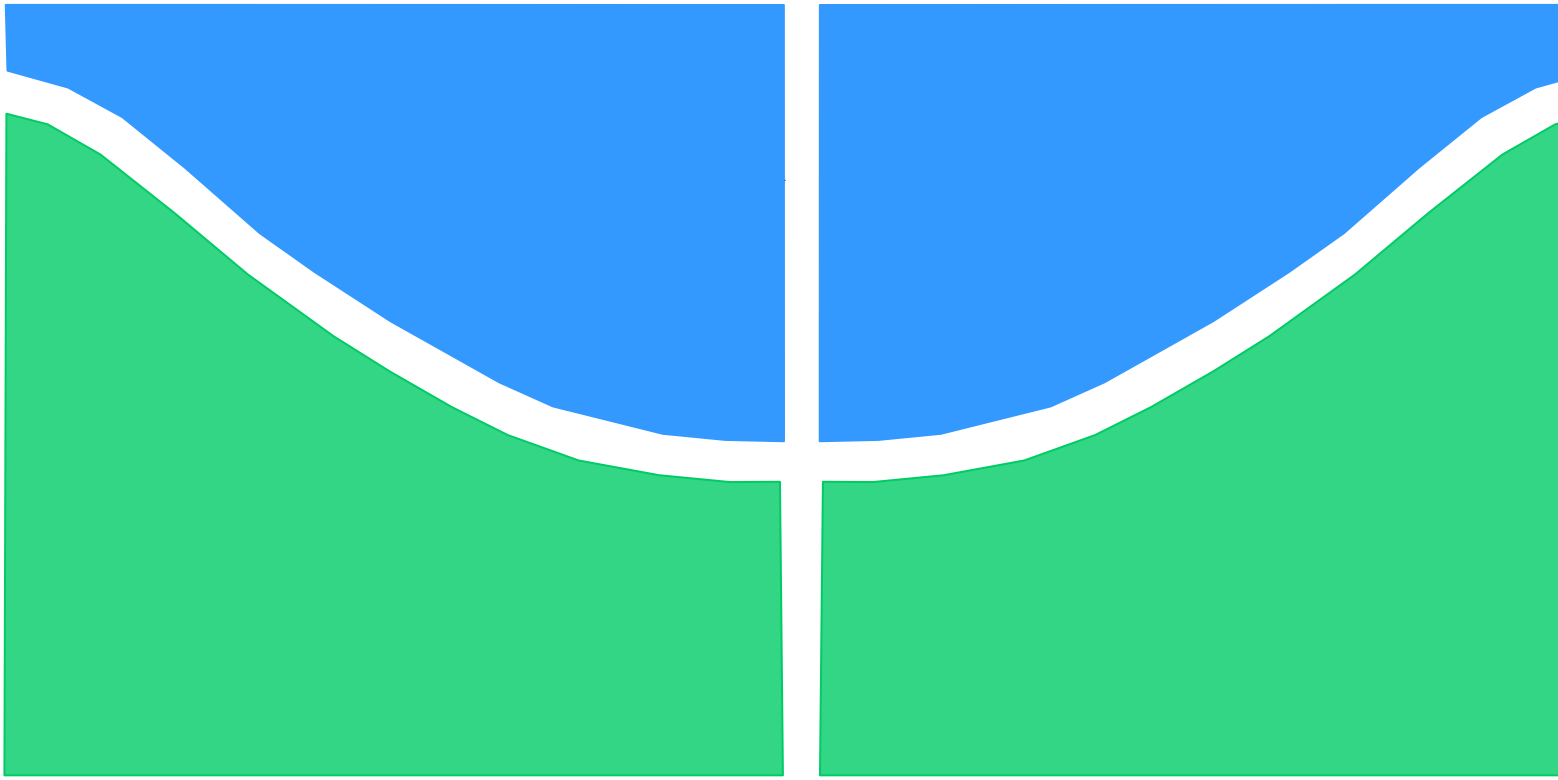


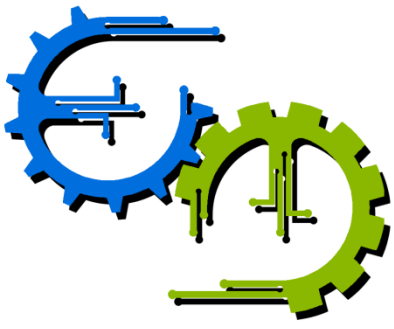
TRABALHO DE GRADUAÇÃO

ESQUEMA DE SINCRONIZAÇÃO ADAPTATIVA DE SISTEMAS CAÓTICOS COM APLICAÇÃO À COMUNICAÇÃO COM SEGURANÇA

Por,

Fábio Vital

Brasília, Julho de 2013



ENGENHARIA MECATRÔNICA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia
Curso de Graduação em Engenharia de Controle e Automação

TRABALHO DE GRADUAÇÃO

ESQUEMA DE SINCRONIZAÇÃO ADAPTATIVA DE SISTEMAS CAÓTICOS COM APLICAÇÃO À COMUNICAÇÃO COM SEGURANÇA

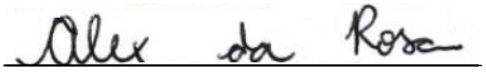
POR,

Fábio Vital

Relatório submetido como requisito parcial para obtenção
do grau de Engenheiro de Controle e Automação.

Banca Examinadora

Prof. José Alfredo Ruiz Vargas
UnB/ENE (Orientador) _____

Prof. Alex da Rosa
UnB/ENE 

Prof. João Yoshiyuki Ishihara
UnB/ENE _____

Brasília, Julho de 2013

FICHA CATALOGRÁFICA

FÁBIO, VITAL
Esquema de Sincronização Adaptativa de Sistemas Caóticos: Com Aplicação à Comunicação com Segurança,

[Distrito Federal] 2013.

x, 80p., 297 mm (FT/UnB, Engenheiro, Controle e Automação, Ano). Trabalho de Graduação – Universidade de Brasília. Faculdade de Tecnologia.

1. Comunicação com Segurança
2. Sincronização Caótica
3. Sistemas Unificados Caóticos
4. Modulação Caótica

I. Mecatrônica/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

VITAL, F., (2013). Esquema de Sincronização Adaptativa de Sistemas Caóticos com Aplicação à Comunicação com Segurança. Trabalho de Graduação em Engenharia de Controle e Automação, Publicação FT.TG-nº 03, Faculdade de Tecnologia, Universidade de Brasília, Brasília, DF, 80p.

CESSÃO DE DIREITOS

AUTOR: Fábio Vital.

TÍTULO DO TRABALHO DE GRADUAÇÃO: Esquema de Sincronização Adaptativa de Sistemas Caóticos com Aplicação à Comunicação com Segurança.

GRAU: Engenheiro ANO: 2013

_____

Fábio Vital

RESUMO

Neste trabalho estudam-se esquemas de comunicação com segurança baseados no mascaramento caótico da mensagem a ser transmitida. Para tanto, uma revisão sobre sistemas caóticos e sua participação nos esquemas de comunicação com segurança é apresentada.

Na sequência, dois esquemas conhecidos na literatura são analisados. No primeiro esquema é utilizada uma sincronização por sinal comum. No segundo esquema é empregada uma sincronização usando um controlador de modos deslizantes.

Objetivando-se suprir as deficiências dos esquemas analisados, é proposto um esquema para comunicação com segurança baseado em sincronização adaptativa de sistemas caóticos unificados em combinação com uma criptografia caótica. O esquema de sincronização é baseado na teoria de estabilidade de Lyapunov, para assegurar limitação e convergência assintótica do erro de sincronização para zero, mesmo na presença de distúrbios limitados e parâmetros incertos. Um exemplo é apresentado objetivando-se mostrar a aplicação do esquema proposto e seu desempenho quando comparado com os dois esquemas analisados previamente. Como esperado da análise teórica, sob as condições propostas, o desempenho do esquema proposto é superior.

Palavras Chave: comunicação com segurança, sincronização caótica, sistemas unificados caóticos, modulação caótica.

ABSTRACT

The present work studies secure communication schemes based on chaotic masking of the transmitted signal. Therefore, a brief review of chaotic systems and their importance to secure communication schemes is presented.

In the sequel, two known, by the engineering community, schemes are analyzed. On the first one, a drive-signal synchronization is proposed, whereas on the second, a sliding-mode control synchronization is proposed.

To extinguish the deficiencies of the analyzed schemes, a new scheme is proposed based on adaptive synchronization of unified chaotic systems in combination with chaotic cryptography. The scheme is based on the Lyapunov Stability Theory, so that ultimately, the asymptotic convergence of the error to zero is proven, even in the presence of limited disturbances e uncertain parameters. An example is presented so that the applications and performance of the proposed scheme can be shown in comparison to the two already analyzed schemes. As expected, the proposed scheme shows an improvement in the synchronization and security of the communications scheme.

Keywords: secure communications, chaotic synchronization, unified chaotic systems, chaotic modulation.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SÍMBOLOS

Símbolos Gregos

$\forall$ “Para qualquer que seja”

$\| \ \|$ Norma

$\| \ \|_F$ Norma de Frobenius

$\Rightarrow$ “Implica que”

$\exists$ “Existe”

$\in$ “É um elemento de”

$\mathbb{R}$ Conjunto dos números reais

∞ Infinito

Subscritos

s escravo

m mestre

Sobrescritos

$\dot{}$ Variação temporal

$\bar{}$ Limitante Superior

$\tilde{}$ Erro entre o valor estimado e o real

$\hat{}$ Valor estimado

* Ponto de equilíbrio

T Transposta

CAPÍTULO 1

INTRODUÇÃO

Caos é um conceito utilizado para descrever o comportamento complexo de sistemas dinâmicos determinísticos quando esse é aperiódico e extremamente sensível às condições iniciais [1]. Por determinístico entende-se que o estado futuro do sistema é determinando inteiramente pelas suas condições iniciais sem a presença de elementos aleatórios. Pequenas diferenças na condição inicial, como por exemplos erros de arredondamento em simulações numéricas, mudam as trajetórias do sistema caótico, tornando, assim, o estado em longo prazo imprevisível.

Inicialmente, o conceito de caos foi empregado como uma ferramenta para auxiliar o entendimento de fenômenos na biologia, química e física. Por muito tempo o caos foi considerado prejudicial na grande maioria das aplicações da engenharia.

Entretanto, desde os estudos de Ott, Grebogi e Yorke (OGY) [2] e, de Pecora e Carrol [3], que consideraram pela primeira vez métodos para controlar o caos, a comunidade científica começou uma busca para achar possíveis aplicações para o caos. Devido ao seu comportamento imprevisível, a comunicação segura despontou como uma de suas principais aplicações.

Em 1993, Cuomo et. al. desenvolveu o método de mascaramento caótico aditivo [4]. Neste método, a informação é adicionada a um estado do sistema caótico e enviada a outro sistema caótico, este sinal é responsável pela sincronização. Devido à imprevisibilidade do comportamento caótico, a informação é considerada encriptada e segura. Ainda em 1993, o método de chave de deslocamento caótico foi proposto por Dedieu e colaboradores [5]. Neste método, a mensagem composta por uma sequencia de bits atuava comutando entre dois circuitos de Chua no transmissor. No receptor, composto também por dois circuitos de Chua, a mensagem era recuperada verificando qual circuito era sincronizado. Entre o final de 1993 e 1996 surgiram mais dois métodos de mascaramento. Yang e Chua [6] introduziram o conceito de modulação caótica de parâmetros, onde a mensagem a ser transmitida era utilizada para modificar os parâmetros do sistema. Wu e Chua [7] apresentaram a modulação caótica não

autônoma, um método onde a mensagem era introduzida no sistema de modo a modificar seu comportamento no espaço de estados. Em 1997, Yang et. al. [8] apresentaram um esquema de segurança que combinava criptografia e caos, gerando assim um criptosistema caótico.

Associado a esses esquemas de comunicação com segurança estão métodos de sincronização, e.g., sincronização por sinal comum [4], sincronização por modos deslizantes [9], sincronização adaptativa [10], etc.

Desde o desenvolvimento do mascaramento caótico aditivo, grande parte da literatura tem ignorado a presença de distúrbios nos sistemas a serem sincronizados [4, 9, 10, 11, 12] Além disso, assumem que os sistemas são inteiramente estruturalmente conhecidos.

Considerando as informações acima, o presente trabalho se encarrega inicialmente de analisar dois tipos de sincronização associados a um esquema clássico de comunicação com segurança. Para isso é estudado um caso de sincronização por sinal comum [7] e um caso de sincronização por modos deslizantes [9]. O objetivo desse estudo é analisar pontos onde, tanto a qualidade e robustez da sincronização podem ser melhoradas como também a segurança do esquema. Em seguida, descarta-se a noção de sistemas idênticos ou perfeitamente conhecidos para o desenvolvimento de um esquema de segurança baseado em sincronização adaptativa com presença de distúrbio e parâmetros desconhecidos. Sendo assim, este trabalho de graduação contribui nos seguintes tópicos:

- Estudo do estado da arte de comunicação com segurança baseada em sincronização caótica (Capítulo 2).
- Análise da estabilidade e convergência de dois esquemas de comunicação com segurança baseados em sincronização (Capítulo 3);
- Análise da segurança e viabilidade de dois esquemas conhecidos de comunicação com segurança (Capítulo 3);
- Estudo de controlador adaptativo que assegura a convergência do erro de sincronização para zero, mesmo na presença de distúrbios internos ou externos (Capítulo 4);
- Proposta de esquema de comunicação com segurança mais seguro e com melhor desempenho que os sistemas analisados (Capitulo 4).

CAPÍTULO 2

DEFINIÇÕES E CONCEITOS PRELIMINARES

Neste capítulo serão apresentados e discutidos definições e conceitos necessários para a compreensão do assunto a ser exposto. O conteúdo é uma compilação de técnicas e considerações feitas ao longo do trabalho e poderá ser encontrado na literatura citada. Desta forma sistemas dinâmicos, retrato de fase, teoria de estabilidade de Lyapunov, o conceito de caos, a sincronização caótica e modos de comunicação com segurança baseados em caos serão abordados.

2.1 SISTEMAS DINÂMICOS

Os conceitos que serão apresentados a seguir foram retirados de [13].

Considere o sistema dinâmico composto por um número finito de equações diferenciais de primeira ordem acopladas

$$\begin{aligned}
\dot{x}_1 &= f_1(t, x_1, \dots, x_n, u_1, \dots, u_p) \\
\dot{x}_2 &= f_2(t, x_1, \dots, x_n, u_1, \dots, u_p) \\
\dot{x}_3 &= f_3(t, x_1, \dots, x_n, u_1, \dots, u_p) \quad , \\
&\vdots \quad \vdots \\
\dot{x}_n &= f_n(t, x_1, \dots, x_n, u_1, \dots, u_p)
\end{aligned} \tag{2.1}$$

onde as variáveis $x_1, x_2, \dots, x_n$ são as variáveis de estado, as quais representam a memória que o sistema dinâmico tem do seu passado, $\dot{x}_i$ representa a derivada de x_i com respeito ao tempo t e $u_1, u_2, \dots, u_p$ são variáveis de entrada específicas. Esse sistema pode também aparecer em sua forma vetorial

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

Dessa forma tem-se

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

que é chamada de equação de estado, $\boldsymbol{x}$ é chamado de vetor de estado e $\boldsymbol{u}$ de entrada. No caso em que a equação (2.3) não depende da variável de tempo t, i.e.

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

dizemos que o sistema é autônomo ou invariante no tempo, dessa mesma forma diz-se que a equação (2.3) representa um sistema não autônomo ou variante no tempo. Deve-se salientar que a entrada $\boldsymbol{u}$ comumente é representada por uma função da seguinte forma

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

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

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

onde a mesma modificação vale para a 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 é 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

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

Pontos de equilíbrio podem ser isolados, i.e., podem não possuir nenhum outro ponto de equilíbrio em seus arredores, ou podem ser um conjunto de pontos de equilíbrios contínuos, e.g, uma reta, esfera, elipse, etc..

Outro conceito importante é o de espaço de fase. O espaço de fase é um espaço onde evoluem todos os possíveis estados do sistema dinâmico. A mudança de um estado ao longo do tempo será então representada por uma trajetória no espaço de fase.

No espaço de fase há a presença de atratores, que são um conjunto de pontos para os quais o estado, se movendo de acordo com o sistema dinâmico, é atraído. Em outras

palavras, os atratores representam os locais para onde um sistema evolui. Estes podem ser um ponto, um conjunto finito de pontos, uma curva, uma órbita fechada ou até um atrator estranho, que é um atrator onde as trajetórias não possuem órbitas periódicas..

2.2 RETRATO DE FASE

O retrato de fase é uma representação geométrica das trajetórias de um sistema dinâmico a partir de diferentes condições iniciais. Cada conjunto de condições iniciais é representado por um conjunto de trajetórias diferentes. Para exemplificar o retrato de fase usou-se um sistema dinâmico bidimensional, o qual dá origem a um plano de fase. De acordo com [1], considere um sistema dinâmico composto por

$$\dot{x}_1 = f_1(x_1, x_2) \tag{2.8}$$

$$\dot{x}_2 = f_2(x_1, x_2) \quad , \tag{2.9}$$

onde $\boldsymbol{x} = [x_1\ x_2]^T$ é um ponto no plano de fase e $\dot{\boldsymbol{x}} = [\dot{x}_1\ \dot{x}_2]^T$ é o vetor velocidade no ponto em questão. Ao fluir pelo campo vetorial, o ponto traça a solução $x(t)$. O plano de fase está repleto de trajetórias, já que cada ponto pode realizar o papel de uma condição inicial. A figura a seguir mostra alguns aspectos importantes de qualquer plano de fase

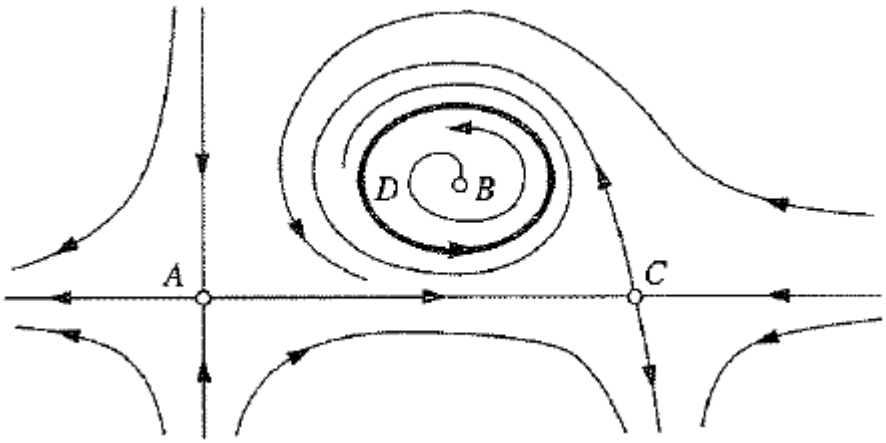


Figura 2.1. Aspectos de um plano de fase [1].

sendo eles:

- Pontos fixos: correspondem a pontos de equilíbrio isolados e são representados na Figura 2.1 por A, B e C;

- Órbitas fechadas: correspondem a soluções periódicas, i.e., soluções onde $x(t+T)=x(t)$ para todo t, para algum $T>0$ e são representadas na Figura 2.1 por D;

- O arranjo das trajetórias nos arredores dos pontos fixos e órbitas fechadas. Neste exemplo, os padrões de fluxo perto de A e C são similares, mas os dois são diferentes do padrão ao redor de B;

- A estabilidade dos pontos fixos e das órbitas fechadas. Neste exemplo, A, B e C são instáveis porque as trajetórias próximas tendem a se afastar destes pontos e D é estável.

2.3 TEORIA DE ESTABILIDADE DE LYAPUNOV

Nesta seção, é apresentada a teoria de estabilidade de Lyapunov somente para sistemas não autônomos, i.e., variantes no tempo. Isso se deve ao fato de que em todas as simulações e considerações apresentadas no trabalho se considera uma dependência explícita do tempo.

O conceito de estabilidade para sistemas variantes no tempo é similar ao para sistemas não variantes. Porém, devido à dependência do sistema não autônomo no tempo inicial t_0, as definições dos conceitos de estabilidade deverão incluir t_0 explicitamente. Além disso, surge aqui o conceito de uniformidade, o qual é necessário para caracterizar sistemas não autônomos que possuem um comportamento dependente do tempo inicial t_0. Todos os conceitos foram retirados de [14].

2.3.1 Definições sobre estabilidade e uniformidade

As definições que virão mais a frente consideram um sistema não autônomo da forma

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(t, \boldsymbol{x}) \ , \tag{2.10}$$

onde os pontos de equilíbrio $\boldsymbol{x}^*$ são definidos por

$$\dot{\boldsymbol{x}}^* = \boldsymbol{f}(t, \boldsymbol{x}^*) \equiv \boldsymbol{0} \quad , \forall t \geq t_0. \tag{2.11}$$

Nota-se que a equação (2.11) deve ser satisfeita $\forall t \geq t_0$, i.e., o sistema deve ser capaz de se manter no ponto $\boldsymbol{x}^*$ durante todo o tempo a partir de t_0. A seguir são definidos os conceitos de estabilidade, instabilidade, estabilidade assintótica, estabilidade exponencial, estabilidade uniforme estável e estabilidade uniforme assintótica. Nota-se que todas as soluções consideram o ponto de equilíbrio $\mathbf{0}$. Caso o sistema em questão tenha um ponto de equilíbrio diferente faz-se um deslocamento do mesmo de forma que o ponto de equilíbrio seja $\mathbf{0}$ na nova representação.

Definição 2.3.1.1: O ponto de equilíbrio $\mathbf{0}$ é estável em t_0 se para qualquer $R > 0$, existir um $r(R, t_0)$ escalar positivo de modo que

$$\|x(t_0)\| < r \quad \Longrightarrow \quad \|x(t)\| < R \qquad \forall t \geq t_0 \ . \tag{2.12}$$

Caso contrário, o ponto de equilíbrio $\mathbf{0}$ é instável. Essa definição diz que se for possível manter o estado em uma bola com um raio pequeno arbitrário R iniciando a trajetória to estado em uma bola de raio suficientemente pequeno r, o ponto de equilíbrio será estável.

Definição 2.3.1.2: O ponto de equilíbrio $\mathbf{0}$ é assintoticamente estável em t_0 se:

- O ponto de equilíbrio $\mathbf{0}$ for estável em t_0;
- $\exists r(t_0)$ de modo que $\|x(t_0)\| < r(t_0) \quad \Longrightarrow \quad \|x(t)\| \to 0$ quando $t \to \infty$.

Em outras palavras, é necessária a existência de uma região de atração para cada tempo inicial t_0.

Definição 2.3.1.3: O ponto de equilíbrio $\mathbf{0}$ é exponencialmente estável se existir dois números positivos, α e λ, de forma que para um $x(t_0)$ suficientemente pequeno,

$$\|x(t)\| \leq \alpha \|x(t_0)\| e^{-\lambda(t-t_0)} \qquad \forall t \geq t_0 \ . \tag{2.13}$$

Definição 2.3.1.4: O ponto de equilíbrio $\mathbf{0}$ é globalmente assintoticamente estável se $\forall \boldsymbol{x}(t_0) \in \mathbb{R}^n$

$$\boldsymbol{x}(t) \to \mathbf{0} \text{ quando } t \to \infty \ . \tag{2.14}$$

Definição 2.3.1.5: O ponto de equilíbrio $\mathbf{0}$ é localmente uniformemente estável se o escalar r da definição 2.3.1.2 puder ser escolhido independentemente de t_0, i.e., se

$r = r(R)$. A introdução da uniformidade é para desconsiderar sistemas que perdem sua estabilidade para valores maiores de t_0.

Definição 2.3.1.6: O ponto de equilíbrio na origem é localmente assintoticamente uniformemente estável se

- se for uniformemente estável,
- Se existir um bola (região) de atração B_{R_0} com um raio independente de t_0, de forma que qualquer trajetória do sistema com estados iniciais em B_{R_0} convergir para zero uniformemente em t_0.

Nota-se que a estabilidade assintótica uniforme implica em estabilidade assintótica, porém o inverso não é necessariamente verdadeiro. Além disso, se B_{R_0} for substituído por todo o espaço de estados, provar-se-á que o ponto de equilíbrio é globalmente assintoticamente uniformemente estável.

2.3.2 Teorema de Lyapunov

No estudo de sistema não autônomos utilizando o Método Direto de Lyapunov, funções escalares com uma dependência explícita do tempo $V(t, \boldsymbol{x})$ podem ser usadas. A seguir são definidas algumas propriedades que essas funções escalares deverão possuir quando as utilizarmos na análise de Lyapunov.

Definição 2.3.2.1: Uma função escalar variante no tempo $V(\boldsymbol{x}, t)$ é localmente positiva definida se $V(\mathbf{0}, t) = 0$ e existir uma função positiva definida $V_0(\boldsymbol{x})$ tal que $\forall t \geq t_0$,

$$V(\boldsymbol{x}, t) \geq V_0(\boldsymbol{x}) \ . \tag{2.15}$$

A função $V(\boldsymbol{x}, t)$ é negativa definida se $-V(\boldsymbol{x}, t)$ é positiva definida.

Definição 2.3.2.2: Uma função escalar $V(\boldsymbol{x}, t)$ é decrescente se $V(\mathbf{0}, t) = 0$ e existir uma função positiva definida não dependente do tempo $V_l(\boldsymbol{x})$ tal que $\forall t \geq t_0$,

$$V(\boldsymbol{x}, t) \leq V_l(\boldsymbol{x}) \ . \tag{2.16}$$

Definição 2.3.2.3: Uma função escalar $V: \mathbb{R}^n \to \mathbb{R}$ é radialmente ilimitada se $\lim_{\|x\| \to \infty} V(\boldsymbol{x}) = +\infty$.

Os principais resultados acerca de estabilidade para sistemas não autônomos são sumarizados no seguinte teorema [14].

Teorema 2.3.2.1: Teorema de Lyapunov para sistemas não autônomos

- **Estabilidade:** Se, em uma bola B_{R_0} ao redor do ponto de equilíbrio $\mathbf{0}$, existir uma função $V(\boldsymbol{x}, t)$ com derivadas parciais contínuas de forma que

    1. V é positiva definida

    2. $\dot{V}$ é negativa semidefinida,

    então o ponto de equilíbrio $\mathbf{0}$ é estável no sentido de Lyapunov. Ao cumprir as duas condições acima a função $V(\boldsymbol{x}, t)$ é chamada de função de Lyapunov do sistema não autônomo.

- **Estabilidade uniforme e estabilidade assintótica uniforme:** Se, além de cumprir a definição acima

    3. V for decrescente,

    então a origem é uniformemente estável. A condição 2 pode ser fortalecida pela exigência de que $\dot{V}$ seja negativa definida, dessa for o ponto de equilíbrio é uniformemente assintoticamente estável.

- **Estabilidade assintótica uniforme global:** Se a bola B_{R_0} for substituída por todo espaço de estados e a condição 1, a condição 2 fortalecida, a condição 3 e a condição

    4. $V(\boldsymbol{x}, t)$ for radialmente ilimitada,

    todas forem satisfeitas, então o ponto de equilíbrio em $\mathbf{0}$ é globalmente uniformemente assintoticamente estável.

A análise de Lyapunov pode ser usada para mostrar a limitação da solução da equação de estado mesmo quando o ponto de equilíbrio não possa ser encontrado. Nesse caso utiliza-se a seguinte definição [13].

Definição 2.3.2.4: As soluções de um sistema não autônomo são

- Uniformemente limitadas se existe um constante positiva c, independente de $t_0 \geq 0$, e se $\forall a \in (0, c), \exists \beta = \beta(a) > 0$, independente de t_0, de forma que

$$\|\boldsymbol{x}(t_0)\| \leq a \Longrightarrow \|\boldsymbol{x}(t)\| \leq \beta, \forall t \geq t_0 \ . \tag{2.17}$$

- Globalmente uniformemente limitada se a Eq. 2.17 se mantiver para um a arbitrariamente grande.

- Uniformemente finalmente limitadas com limitante final b se existir duas constantes b e c, independentes de $t_0 \geq 0$, e se $\forall a \in (0, c), \exists T = T(a, b) \geq 0$, independente de t_0, de forma que

$$\|x(t_0)\| \leq a \Longrightarrow \|x(t)\| \leq b, \forall t \geq t_0 + T \ . \tag{2.18}$$

- Globalmente uniformemente finalmente limitada se a Eq. 2.18 se mantiver para um a arbitrariamente grande.

2.3.3 Lema de Barbalat e análise *Lyapunov-like*

A obtenção de funções de Lyapunov com derivada negativa definida é geralmente bastante trabalhosa, portanto a análise de estabilidade assintótica se torna difícil. Para facilitar esta análise utiliza-se o Lema de Barbalat.

Definição 2.3.3.1: Uma função g é uniformemente contínua em $[0, \infty)$ se

$$\forall\, R > 0,\ \exists \eta(r) > 0,\ \ \forall t_1 \geq 0,\ \ \forall t \geq 0,\ \ |t - t_1| < \eta \implies |g(t) - g(t_1)| < R \ . \tag{2.19}$$

Lema 2.3.3.1: (Barbalat) Se uma função diferenciável $f(t)$ tem um limitante finito quando $t \to \infty$, e se $\dot{f}$ for uniformemente contínua, então $\dot{f}(t) \to 0$ quando $t \to \infty$.

Para aplicar o lema 2.3.3.1 na análise de sistemas dinâmicos usualmente utiliza-se o seguinte lema.

Lema 2.3.3.2: ("Lema Lyapunov Like") Se a função escalar $V(\boldsymbol{x}, t)$ satisfaz as seguintes condições

- $V(\boldsymbol{x}, t)$ é limitada inferiormente
- $\dot{V}(\boldsymbol{x}, t)$ é negativa semidefinida

- $\dot{V}(\boldsymbol{x}, t)$ é uniformemente continua no tempo

então $\dot{V}(\boldsymbol{x}, t) \to 0$ quando $t \to \infty$.

2.4 O CONCEITO DE CAOS

Embora se tenha observado o comportamento caótico desde o século XV [1], a primeira vez que a palavra caos foi utilizada em conexão com sistemas dinâmicos foi em 1975, por Li e Worke [15]. Desde então sistemas dinâmicos com comportamento caótico tem recebido, cada vez mais, atenção dos pesquisadores [16,17,18]. Strogatz em [1], define caos do seguinte modo.

Definição 2.4.1: Caos é notado quando um sistema determinístico exibe um comportamento aperiódico que depende sensivelmente das condições iniciais, dessa forma tornando impossível a previsão de seu estado futuro.

Antes de seguir, devemos inicialmente conceituar cada uma das características acima estabelecidas.

- Sistema determinístico: Implica que as equações do sistema dinâmico não possuem entradas ou parâmetros aleatórios, i.e., o comportamento irregular do sistema advém de sua dinâmica não linear.

- Comportamento aperiódico: Implica na inexistência de trajetórias no espaço de fase que se acomodam em pontos fixos ou órbitas periódicas. Além disso, as trajetórias devem ser limitadas, i.e., não devem tender ao infinito.

- Sensibilidade às condições iniciais: Implica que trajetórias que estejam próximas umas das outras no espaço de fase se separam inicialmente exponencialmente rápido no tempo, i.e., o sistema tem um expoente de Lyapunov positivo.

O expoente de Lyapunov caracteriza a taxa de separação das trajetórias ao longo do tempo. Considerando que $\delta Z(t)$ representa a distância no tempo t entre duas trajetórias que começaram a uma distância δZ_0 no tempo t_0, se $\delta Z(t)$ crescer exponencialmente com o tempo tem-se

$$|\delta Z(t)| \approx |\delta Z_0| e^{\lambda(t-t_0)} \quad , \tag{2.20}$$

onde λ representa o maior expoente de lyapunov. Sabe-se, além disso, que em um sistema n-dimensional existem n diferentes expoentes de Lyapunov. Aliado aos três fatores acima expostos, o teorema de Poincaré-Bendixson estabelece que para sistemas dinâmicos contínuos o caos pode somente surgir naqueles com três ou mais dimensões [1].

2.5 SINCRONIZAÇÃO CAÓTICA

Desde 1990 a sincronização caótica tem recebido bastante atenção, e.g. [19,20,21]. Acredita-se que o primeiro a observar e documentar o fenômeno de sincronização tenha sido o pesquisador Christiaan Huygens [22], o qual é mais conhecido pelos trabalhos nos campos da óptica e da construção de telescópios e relógios. Ele notou que dois relógios de pêndulo pendurados em um mesmo suporte tinham sincronizado i.e., suas oscilações coincidiam perfeitamente enquanto os pêndulos se moviam em direções opostas. Ao trabalhar com sistemas dinâmicos é dito, usualmente, que eles estão sincronizados se a distância entre seus estados converge para zero quando $t \to \infty$ [23].

Pecora e Carroll [3] comentam que sistemas caóticos por si só são sistemas que aparentam desafiar a sincronização. Dois sistemas autônomos idênticos, que possuam praticamente as mesmas condições iniciais no espaço de fase, têm trajetórias que rapidamente se tornam não correlacionáveis apesar de os dois sistemas mapearem o mesmo atrator no espaço de fase. Aliado ao problema das condições iniciais tem-se a impossibilidade da construção de dois sistemas caóticos idênticos em um laboratório. Esse é um problema de relevância prática que será abordado neste trabalho.

Ao lidarmos com a sincronização caótica existem vários modelos de sincronização que são utilizados, dentre outros [22], temos:

- Sincronização por fase: Seu conceito remete a sistemas nos quais a fase $\theta(t)$ flutua caoticamente e a amplitude do sinal evolui livremente e sem se relacionar [24, 25]. A sincronização por fase ocorre quando a diferença instantânea das fases $\theta_0(t)$ e $\theta_1(t)$ dos sinais caóticos são limitadas no tempo:

$$|\theta_1(t) - \theta_0(t)| < C \ , \ C = cte \ . \tag{2.21}$$

- Sincronização completa: Implica na exata congruência entre estados vetores de sistemas que estão interagindo entre si, seja unidirecionalmente ou reciprocamente: $v(t) \equiv u\,(t)$, onde estes são os vetores de estados de dois sistemas diferentes. Isso ocorre somente em sistemas com elementos idênticos, i.e., cada componente possui a mesma dinâmica e parâmetros [23, 21, 26];

- Sincronização por atraso: Ocorre quando os sistemas interagindo possuem oscilações praticamente idênticas só que deslocadas por um intervalo de tempo T, i.e., $v(t) \approx u(t+T)$ [24, 27]. Essa sincronização é utilizada quando o intervalo de tempo T advém do tempo de deslocamento entre o transmissor e o receptor;

- Sincronização generalizada: é caracterizada pela existência de uma relação funcional entre os estados dos dois sistemas, i.e., o sistema receptor representa uma função do sistema transmissor, $v(t) = F(u(t))$ [21, 26].

A maioria das comunicações baseadas em caos utiliza a sincronização completa, a sincronização por atraso quando o intervalo de deslocamento do sinal é considerado ou a sincronização generalizada quando o sistema receptor não é idêntico ao transmissor.

No escopo deste trabalho utilizaremos para as simulações autorais, a sincronização adaptativa [28], a qual é um modo de sincronização generalizada. Para formular o problema da sincronização consideramos dois sistemas dinâmicos compostos por equações diferenciais ordinárias. Inicialmente consideramos um sistema dinâmico caótico expresso por

$$\dot{\boldsymbol{x}}_m = \boldsymbol{f}_m(\boldsymbol{x}_m, \boldsymbol{d}_m(.)) \,, \tag{2.22}$$

onde $\boldsymbol{x}_m$ é o estado do sistema mestre, $\boldsymbol{f}_m(.)$ é uma função de mapeamento conhecida e $\boldsymbol{d}_m(.)$ é um distúrbio desconhecido. O sistema acima é chamado de sistema mestre. A seguir, definimos o seguinte sistema escravo.

$$\dot{\boldsymbol{x}}_s = \boldsymbol{f}_s(\boldsymbol{x}_s, \boldsymbol{d}_s(.), \boldsymbol{u}) \quad , \tag{2.23}$$

onde $\boldsymbol{x}_s$ é o estado do sistema escravo, $\boldsymbol{f}_s(.)$ é uma função de mapeamento conhecida, $\boldsymbol{d}_s(.)$ é um distúrbio desconhecido e $\boldsymbol{u}$ é o sinal de controle. Com base nas equações (2.22) e (2.23), o erro dinâmico de sincronização é definido como

$$\boldsymbol{e} = \boldsymbol{x}_s - \boldsymbol{x}_m \tag{2.24}$$

e assim

$$\dot{\boldsymbol{e}} = \dot{\boldsymbol{x}}_s - \dot{\boldsymbol{x}}_m \ , \tag{2.25}$$

que é definido como erro dinâmico de sincronização. A sincronização dos sistemas representados pelas equações (2.22) e (2.23) será obtida somente se $\boldsymbol{e}(t) \to 0$ quando $t \to \infty$, i.e., se as trajetórias do sistema escravo convergirem para as do sistema mestre.

2.6 MODOS DE COMUNICAÇÃO COM SEGURANÇA BASEADOS EM CAOS

Como sistemas caóticos são extremamente sensíveis às condições iniciais e a parâmetros, estes passaram a ser usados em esquemas de comunicação com segurança. Diferentes modos de transmitir sinais de informação utilizando uma dinâmica caótica já foram propostos. Os modos mais utilizados para encriptar a informação são:

- Mascaramento Caótico Aditivo: Do inglês *Additive Chaotic Masking* [4], mostrado na Figura 2.2. Consiste em dois sistemas caóticos idênticos. A máscara caótica $x_{mi}(t)$ representa um dos estados do sistema caótico do transmissor. A mensagem $m(t)$, a qual tem uma amplitude menor em 20dB a 30dB que $x_{mi}(t)$, é adicionada à máscara caótica, dando origem ao sinal transmitido $s(t)$. Como o sinal caótico $x_{mi}(t)$ é muito complexo e $m(t)$ é muito menor que o sinal, espera-se que a mensagem não possa ser separada de $s(t)$ sem que alguém tenha o conhecimento exato de $x_{mi}(t)$.

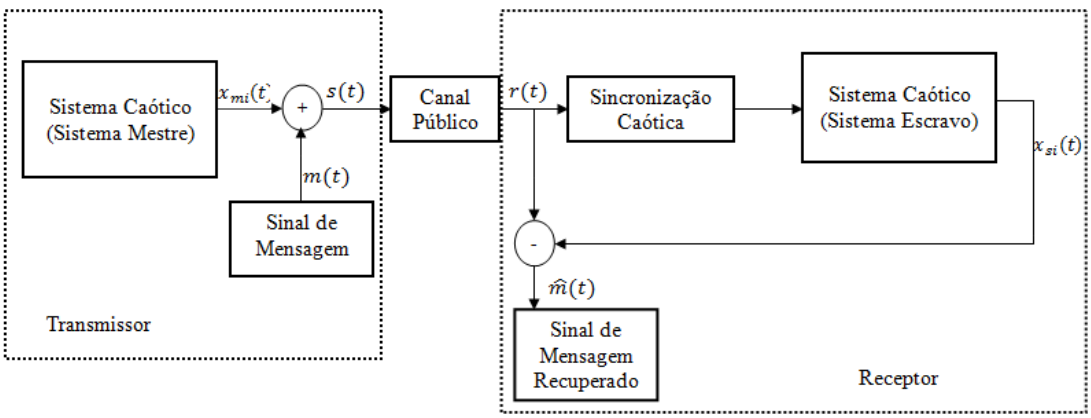


Figura 2.2. Esquema do mascaramento caótico aditivo representado em diagrama de blocos.

- Chaveamento de Deslocamento Caótico: Do inglês *Chaotic Shift Keying* [5], mostrada na Figura 2.3. Esse esquema foi desenvolvido objetivando a transmissão de sinas digitais de mensagem. O sinal de mensagem $m(t)$ é utilizado como a entrada de um multiplexador que possuí como opção de saída dois sistemas caóticos de mesma estrutura, mas com diferentes parâmetros. O sinal recebido $r(t)$ leva à sincronização com o sistema escravo e a mensagem é recuperada utilizando um filtro passa-baixa e depois *thresholding* no sinal de erro de sincronização $e(t)$.

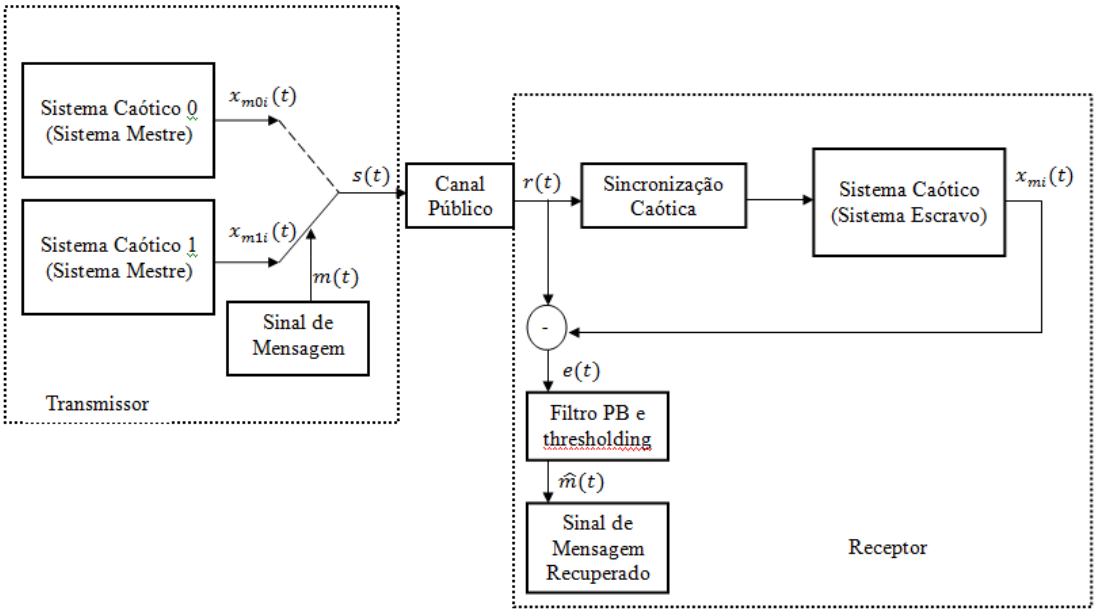


Figura 2.3. Esquema de chaveamento de deslocamento caótico representado em diagrama de blocos.

- Modulação Caótica de Parâmetros: Do inglês *Chaotic Parameter Modulation* [6], mostrada na Figura 2.4. Este método utiliza o sinal de mensagem para alterar os parâmetros do sistema caótico mestre de modo a mudar constantemente a dinâmica do sistema. No receptor, uma lei de adaptação proporcional é usada para estimar os parâmetros do sistema escravo de modo que o erro de sincronização se aproxime ao máximo de zero. Dessa forma a mensagem original é recuperada com base nos parâmetros estimados.

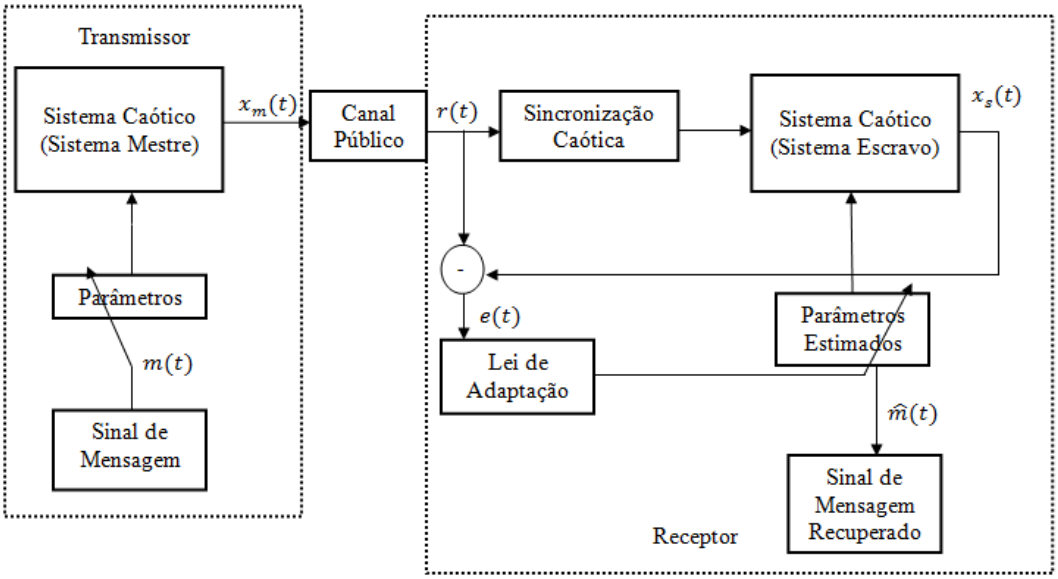


Figura 2.4. Esquema de modulação caótica de parâmetros representado em diagrama de blocos.

- Modulação Caótica Não Autônoma: Do inglês *Chaotic Non-autonomous Modulation* [7], mostrada na Figura 2.5. Este método utiliza o sinal de mensagem para alterar diretamente as trajetórias que o sistema segue no atrator do sistema caótico mestre. Neste caso a mensagem não deve ser tão menor que o necessário no esquema de máscara caótica aditiva. A mensagem não é adicionada somente a um estado do sistema caótico e sim adicionada com o uso de uma função de codificação a todos os estados do sistema. A mensagem é recuperada tendo em mente que o receptor possui uma função de decodificação.

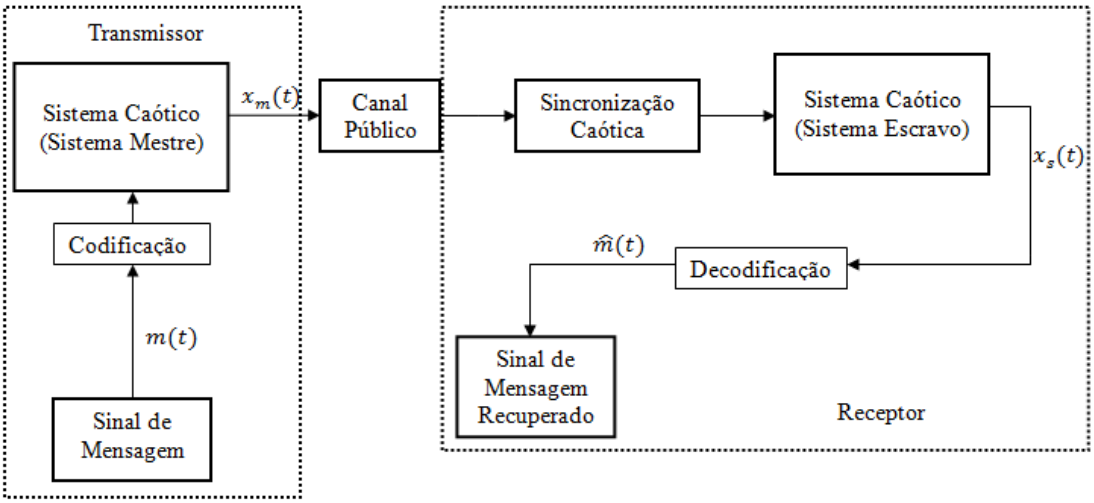


Figura 2.5. Esquema de modulação caótica não autônoma representado em diagrama de blocos.

- Criptosistema Caótico: Do inglês *Chaotic Cryptosystem* [8], mostrado na Figura 2.6. Nesse esquema há uma mistura entre criptografia e sincronização. O sinal de mensagem $m(t)$ é encriptado antes de sua adição ao sistema caótico por meio de um sinal $k(t)$, o qual representa um dos estados do sistema caótico mestre. O sinal encriptado $m_c(t)$ muda a dinâmica do sistema mestre deixando ainda mais complexo. Considerando a possibilidade de quebra de segurança no canal público, sem a regra de decriptação não há modo de obter a mensagem. Nota-se a presença de ruídos $n(t)$ no canal. Assim, após a sincronização serão recuperados no receptor $k(t)$ e $m_c(t)$, mas com alguns ruídos. Utilizando os dois na decriptação obtém-se o sinal de mensagem estimado.

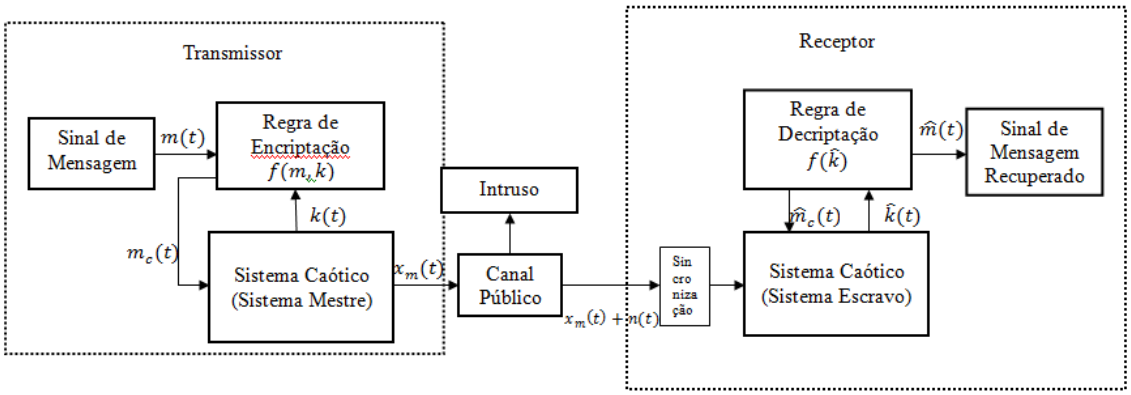


Figura 2.6. Esquema de criptosistema representado em diagrama de blocos.

CAPÍTULO 3

ESQUEMAS DE SINCRONIZAÇÃO CAÓTICA COM APLICAÇÃO À COMUNICAÇÃO BASEADA EM MODULAÇÃO CAÓTICA NÃO AUTÔNOMA

Este capítulo tem como objetivo aprofundar conhecimentos apresentados no capítulo anterior, descrever o sistema dinâmico caótico que será usado no decorrer deste trabalho e apresentar trabalhos já publicados a respeito de comunicação com segurança baseada em modulação caótica não autônoma [7,9]. Os estudos a serem apresentados são de importância fundamental para o desenvolvimento do presente trabalho, não só como motivação, mas também como parâmetro de comparação para os resultados expostos no capítulo seguinte. As propostas estabelecidas nas publicações [7,9] serão aplicadas e simuladas utilizando sistemas unificados caóticos, apresentados na seção a seguir.

3.1 SISTEMA CAÓTICO UNIFICADO

O sistema caótico unificado é um sistema cujo comportamento está relacionado com a variação de apenas um parâmetro. Sistemas caóticos na literatura como os sistemas de Chen, Lorenz e Lü podem ser considerados casos particulares do sistema caótico unificado. Historicamente, no início da década de 1960, Lorenz, em sua publicação "*Deterministic Nonperiodic Flow"* [29], estudou sistemas de equações determinísticas que representavam idealizações de sistemas hidrodinâmicos. Seu estudo era direcionado a encontrar soluções não periódicas, i.e., soluções que nunca repetem com exatidão o seu passado. Como resultado, Lorenz obteve o seguinte sistema de três dimensões

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= cx - y - xz \\ \dot{z} &= -bz + xy \ , \end{aligned} \tag{3.1}$$

onde, se os parâmetros forem estabelecidos como $a = 10, b = 8/3$ e $c = 28$ e observar-se-á no retrato de fase o Atrator de Lorenz, i.e., o sistema exibirá comportamento caótico.

Na busca de parâmetros que tornem sistemas dinâmicos em caóticos, Chen e Ueta [30] encontraram no seguinte sistema

$$\begin{aligned}\dot{x} &= a(y-x)\\ \dot{y} &= (c-a)x - cy - xz\\ \dot{z} &= -bz + xy\ ,\end{aligned} \tag{3.2}$$

um novo atrator quando os parâmetros são estabelecidos como $a = 35$, $b = 3$ e $c = 28$. A esse, deu-se o nome de Atrator de Chen. Apesar da similaridade aparente dos sistemas descritos por (3.1) e (3.2), os sistemas não são topologicamente equivalentes, i.e., não há transformação, linear ou não linear, de coordenadas que consiga converter o sistema (3.1) em (3.2) e vice-versa.

Os sistemas (3.1) e (3.2) podem ser representados da seguinte forma

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix} = \begin{bmatrix}a_{11} & a_{12} & 0\\ a_{21} & a_{22} & 0\\ 0 & 0 & a_{33}\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} + \begin{bmatrix}0\\ -xz\\ xy\end{bmatrix}\ . \tag{3.3}$$

onde o segundo termo do lado direito é composto dos termos não lineares do sistema e os elementos $a_{ij},\ i,j = 1,2,3$ pertencem ao conjunto dos números reais. No caso do Atrator de Lorenz temos que $a_{12}a_{21} > 0$, enquanto o Atrator de Chen exibe $a_{12}a_{21} < 0$.

Em 2002, Lü e Chen [31] indagaram a possibilidade de existência de um sistema caótico intermediário entre os sistemas Lorenz e Chen exibindo $a_{12}a_{21} = 0$.

Assim surge o seguinte sistema, chamado de sistema de Lü,

$$\begin{aligned}\dot{x} &= a(y-x)\\ \dot{y} &= cy - xz\\ \dot{z} &= -bz + xy\ ,\end{aligned} \tag{3.4}$$

que exibe comportamento caótico quando $a = 36,\ b = 3$ e $\{c \in \mathbb{R} \mid 12 < c < 17 \vee 18 < c < 22 \vee 23 < c < 28{,}5 \vee 28{,}6 < c < 29 \vee 29{,}334 < c < 29{,}345\}$. Esse novo sistema é não topologicamente equivalente aos sistemas (3.1) e (3.2).

No mesmo ano, Lü et. al. [32], na intenção preencher as lacunas entre os três sistemas caóticos e representá-los na forma 3.3, propôs o sistema unificado caótico,

$$\dot{x} = (25\alpha + 10)(y - x)$$
$$\dot{y} = (28 - 35\alpha)x - xz + (29\alpha - 1)y \quad (3.5)$$
$$\dot{z} = xy - \frac{\alpha+8}{3}z \ ,$$

o qual pode ser classificado da seguinte forma:

- Quando $0 \leq \alpha < 0{,}8$, o sistema (3.5) pertence ao sistema generalizado de Lorenz, e se $\alpha = 0$ o sistema será equivalente ao sistema (3.1);
- Quando $\alpha = 0{,}8$, o sistema (3.5) representa o sistema de Lü (3.4);
- Quando $0{,}8 \leq \alpha < 1$, o sistema (3.5) pertence ao sistema generalizado de Chen, e se $\alpha = 1$ o sistema será equivalente ao sistema (3.2).

Algumas propriedades relevantes desse sistema são expostas a seguir.

1. O sistema (3.5) é caótico quando $\alpha \in [0{,}1]$;
2. Conecta os sistemas Lorenz (3.1) e Chen (3.2) e estabelece um espectro de transição entre eles;
3. O controle do parâmetro α mostra a evolução do comportamento dinâmico do Atrator de Lorenz até o Atrator de Chen.

Na subseção seguinte serão expostas simulações numéricas para auxiliar em uma melhor compreensão do comportamento dinâmico do sistema caótico unificado.

3.1.1 Simulações Numéricas

Na seção anterior, o conceito de sistema unificado caótico e sua estrutura foram abrangidos. Considerando que esse sistema possui os sistemas Lorenz e Chen como extremos e o sistema Lü como um sistema intermediário, as simulações a seguir pretendem expor os atratores dos três sistemas para demonstrar seus comportamentos caóticos além de considerar em uma das simulações o que acontece caso o parâmetro α exceda os limites impostos. As simulações foram realizadas e os atratores obtidos são expostos nas Figuras 3.1 a 3.4.

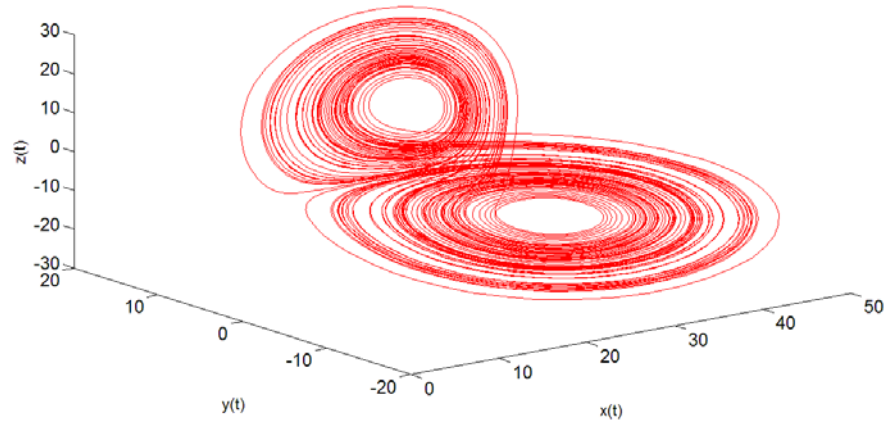


Figura 3.1. Atrator de Lorenz.

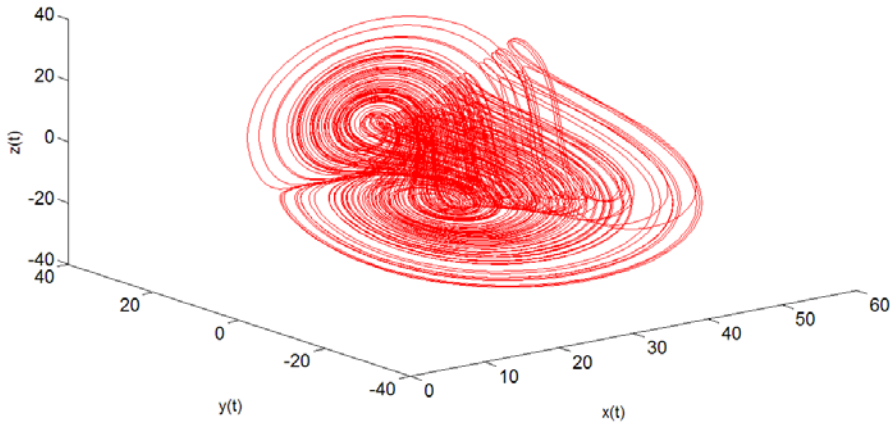


Figura 3.2. Atrator de Lü.

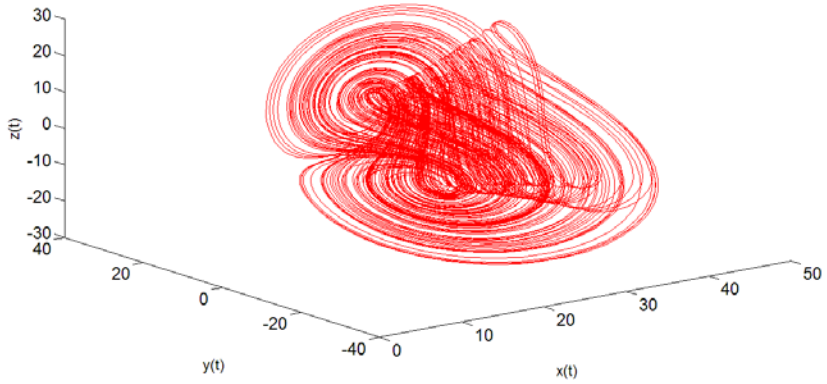


Figura 3.3. Atrator de Chen.

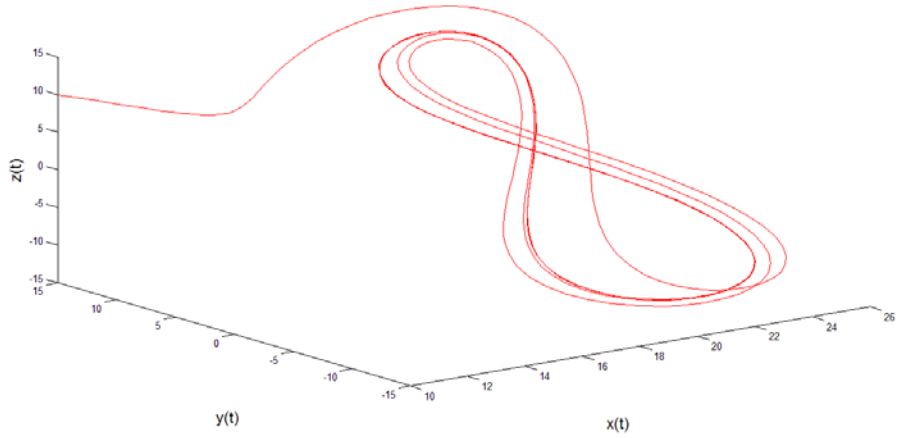


Figura 3.4. Atrator quando $\alpha = 1{,}5$.

Analisando as Figuras 3.1 a 3.4, percebe-se que apenas com a variação do parâmetro α o sistema adota novos atratores, passando pelos atratores de Lorenz ($\alpha = 0$), Lü ($\alpha = 0{,}8$) e Chen ($\alpha = 1$). No caso em que $\alpha = 1.5$, o atrator não é mais um atrator estranho e agora representa uma trajetória periódica. As três primeiras simulações foram realizadas utilizando $x(0) = 15,\ y(0) = 20,\ z(0) = 30$ e $t \in [0{,}100]$. Na última simulação as condições iniciais foram $x(0) = 15,\ y(0) = 10,\ z(0) = 10$ e $t \in [0{,}500]$ e utilizou-se um período maior de teste para mostrar a periodicidade da solução.

3.2 SINCRONIZAÇÃO POR SINAL COMUM

Em 1993, Wu e Chua [7] propuseram um esquema de comunicação com segurança que pode ser classificado como modulação caótica não autônoma. Nesse esquema, representado pela Figura 3.5, o sistema mestre é representado por

$$\dot{\boldsymbol{x}}_m = \boldsymbol{A}\boldsymbol{x}_m + \boldsymbol{f_1}(\boldsymbol{x_p}) \ , \tag{3.6}$$

onde $\boldsymbol{x}_m$ é o vetor estado do sistema mestre, $\boldsymbol{A}$ representa a matriz de parâmetros do sistema e $\boldsymbol{x_p}$ um subvetor do vetor estado $\boldsymbol{x}_m$. O sistema escravo é definido como

$$\dot{\boldsymbol{x}}_s = \boldsymbol{A}\boldsymbol{x}_s + \boldsymbol{f_2}(\boldsymbol{x_p}) \ , \tag{3.7}$$

onde $\boldsymbol{x}_s$ é o vetor estado do sistema escravo, $\boldsymbol{A}$ e $\boldsymbol{x_p}$ são os mesmos que em (3.6).

Tem-se então como erro dinâmico de sincronização

$$\dot{e} = \dot{x}_s - \dot{x}_m = \boldsymbol{A}(x_s - x_m) + \boldsymbol{\eta}(x_p). \quad (3.8)$$

onde $\boldsymbol{\eta} = \boldsymbol{f_2} - \boldsymbol{f_1}$. Objetiva-se provar que $x_s \to x_m$ à medida que $t \to \infty$. Desta forma, os sistemas sincronizarão.

No esquema proposto na Figura 3.5 o sinal de informação a ser transmitido $m(t)$ é codificado pelo sinal caótico $x_p(t)$ utilizando a função de encriptação $s(t) = c(x_p(t), m(t))$ de forma que a informação só possa ser decriptada por $m(t) = d\left(x_p(t), s(t)\right) = d\big(x_p(t), c(x_p(t), m(t))\big)$. A escolha de $c(.,.)$ e de $d(.,.)$ deve satisfazer $s(t) \approx x_p(t)$ por dois motivos. Necessita-se primeiramente que o sistema transmissor (mestre) (3.6) mantenha seu comportamento caótico quando ele é realimentado ao sistema. Por último, é necessário que $m(t)$ não seja identificável quando avaliarmos $s(t)$ que é disponível em um canal público de transmissão. Como $x_s \to x_m$, $\hat{m}(t) \to m(t)$ quando $t \to \infty$.

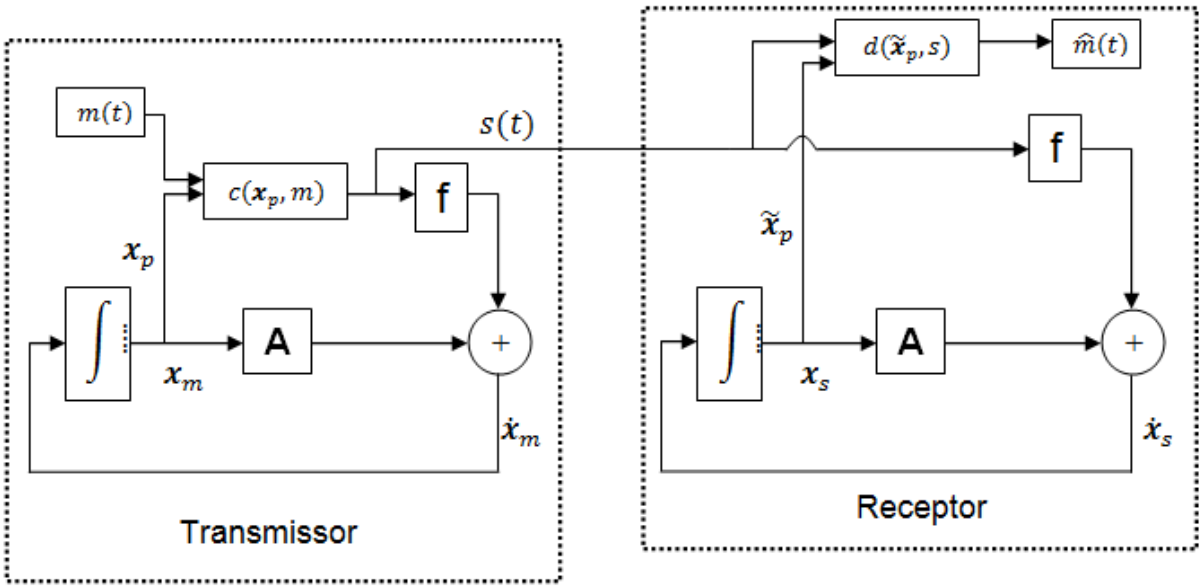


Figura 3.5. Diagrama de blocos do esquema proposto em [7].

Deve-se notar que o esquema proposto não considera a presença de distúrbios, nem da incerteza de parâmetros, o que pode tornar o esquema proposto inviável em condições práticas.

Na subseção a seguir, a viabilidade do esquema de sincronização proposto nessa seção será avaliada considerando que os sistemas mestre e escravo sejam representados por sistemas unificados caóticos.

3.2.1 Esquema de sincronização

Considerando os sistemas mestre e escravo da forma (3.5) com $\alpha = 0{,}02$, obtém-se o seguinte sistema mestre-escravo

$$\begin{aligned}
\dot{x}_{m1} &= 10{,}5(x_{m2} - x_{m1}) \\
\dot{x}_{m2} &= 27{,}3x_{m1} - x_{m1}x_{m3} - 0{,}48x_{m2} \\
\dot{x}_{m3} &= x_{m1}x_{m2} - \tfrac{8{,}02}{3}x_{m3} \\
\dot{x}_{s1} &= 10{,}5(x_{s2} - x_{s1}) \\
\dot{x}_{s2} &= 27{,}3x_{s1} - x_{s1}x_{s3} - 0{,}48x_{s2} \\
\dot{x}_{s3} &= x_{s1}x_{s2} - \tfrac{8{,}02}{3}x_{s3}
\end{aligned} \quad . \tag{3.9}$$

Na sequência, os sistemas anteriores são colocados na forma (3.6)-(3.7). Para tanto x_{s1} e x_{m1} dos termos não lineares em (3.9) são substituídos por $s(t) = x_{m1} + m(t)$. Temos, assim, a inserção do sinal de um dos estados do sistema mestre no sistema escravo e sua conseguinte realimentação no sistema mestre

$$\begin{aligned}
\dot{x}_{m1} &= 10{,}5(x_{m2} - x_{m1}) \\
\dot{x}_{m2} &= 28\big(x_{m1} + m(t)\big) - 0{,}7x_{m1} - (x_{m1} + m(t))x_{m3} - 0{,}48x_{m2} \\
\dot{x}_{m3} &= (x_{m1} + m(t))x_{m2} - \tfrac{8{,}02}{3}x_{m3} \\
\dot{x}_{s1} &= 10{,}5(x_{s2} - x_{s1}) \\
\dot{x}_{s2} &= 28\big(x_{m1} + m(t)\big) - 0{,}7x_{s1} - (x_{m1} + m(t))x_{s3} - 0{,}48x_{s2} \\
\dot{x}_{s3} &= (x_{m1} + m(t))x_{s2} - \tfrac{8{,}02}{3}x_{s3}
\end{aligned} \quad . \tag{3.10}$$

Hipótese 1: Na região [0,∞)

$$\|m(t)\| \leq m_0 \quad , \tag{3.11}$$

onde m_0 é uma constante positiva.

Comentário 1: A hipótese 1 é natural uma vez que a mensagem é previamente determinada.

Comentário 2: No caso em que $\alpha = 0{,}02$ o sistema (3.5) torna-se um sistema generalizado de Lorenz quando $m(t) = 0$.

Definindo o erro de sincronização como $\boldsymbol{e} = \boldsymbol{x}_s - \boldsymbol{x}_m$, temos, a partir de (3.10),

$$\dot{\boldsymbol{e}} = \begin{bmatrix} 10{,}5(e_2 - e_1) \\ -0{,}7e_1 - \big(x_{m1} + m(t)\big)e_3 - 0{,}48e_2 \\ \big(x_{m1} + m(t)\big)e_2 - \frac{8{,}02}{3}e_3 \end{bmatrix} \quad , \tag{3.12}$$

onde $e_1 = x_{s1} - x_{m1}$, $e_2 = x_{s2} - x_{m2}$ e $e_3 = x_{s3} - x_{m3}$.

Prova da sincronização: Considere a seguinte função decrescente e positiva definida

$$V = \frac{1}{2}\left(\frac{1}{10{,}5}{e_1}^2 + {e_2}^2 + {e_3}^2\right) . \tag{3.13}$$

Derivando (3.13) em relação ao tempo resulta

$$\dot{V} = \left(\frac{1}{10{,}5}e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3\right) \quad . \tag{3.14}$$

Avaliando (3.14) ao longo da trajetória de (3.12), obtém-se

$$\begin{aligned} \dot{V} &= e_2e_1 - {e_1}^2 - 0{,}7e_1e_2 - \big(x_{m1} + m(t)\big)e_3e_2 - 0{,}48{e_2}^2 + \big(x_{m1} + m(t)\big)e_2e_3 - \frac{8{,}02}{3}{e_3}^2 \\ &= -{e_1}^2 + 0{,}3e_1e_2 - 0{,}48{e_2}^2 - \frac{8{,}02}{3}{e_3}^2 \\ &\leq -{e_1}^2 + 2\sqrt{0{,}48}e_1e_2 - 0{,}48{e_2}^2 - \frac{8{,}02}{3}{e_3}^2 = -(e_1 - \sqrt{0{,}48}e_2)^2 - 0{,}48{e_2}^2 - \frac{8{,}02}{3}{e_3}^2 . \end{aligned} \tag{3.15}$$

Logo, os erros são uniformemente limitados. Desta forma, $\dot{V}$ é uniformemente contínua. Portando, aplicando o Lema de Barbalat, conclui-se que $\lim_{t\to\infty} \boldsymbol{e}(t) = 0$, i.e., os sistemas mestre e escravo vão sincronizar com a evolução do tempo t.

3.2.2 Simulações

Nesta subseção avaliamos a viabilidade do esquema de comunicação proposto por meio de dois experimentos. O primeiro serve para confirmar o esquema de sincronização por sinal comum proposto em (3.10). O segundo experimento é para confirmar a transmissão da mensagem e sua decriptação, sendo que a mensagem é recuperada utilizando o sinal transmitido $s(t) = x_{m1} + m(t)$ e x_{s1}. Em outras palavras, como $\boldsymbol{x}_s \to \boldsymbol{x}_m$ quando $t \to \infty$, tem-se $\widehat{m}(t) = x_{m1} + m(t) - x_{s1} \approx m(t)$. As simulações foram realizadas utilizando o software MatLab® Simulink e o método analítico Bogacki-Shampine com um passo fixo de 0.0001 para resolver as equações diferenciais.

Foi considerado que $\boldsymbol{x}_m(0) = [1\ 2\ 3]^T$, $\boldsymbol{x}_s(0) = [5\ 7\ 0]^T$ e $\alpha = 0{,}02$. A mensagem transmitida é da forma

$$m(t) = 0{,}01sen(\pi t) \quad . \tag{3.16}$$

As Figuras 3.6 a 3.8 mostram os desempenhos de sincronização obtidos com o esquema proposto e as Figuras 3.9 a 3.11 mostram os erros de sincronização. Deve ser observado que a sincronização do sistema levou 3,034s considerando que o sistema só está sincronizado quando o erro de sincronização entra na faixa de $\pm 0{,}05$. Já a Figura 3.12 representa o sinal de mensagem recuperado.

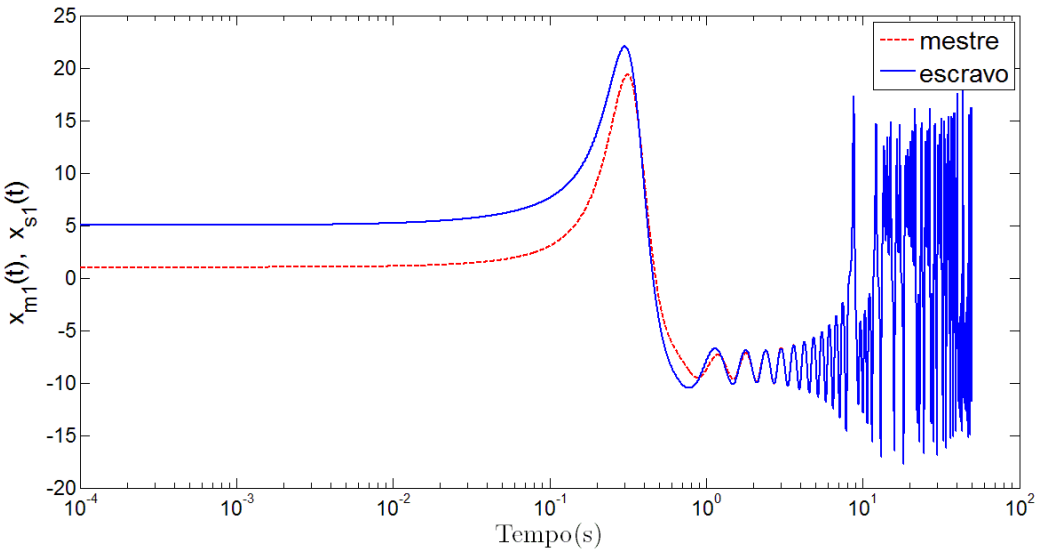


Figura 3.6. Desempenho da sincronização de x_{s1}.

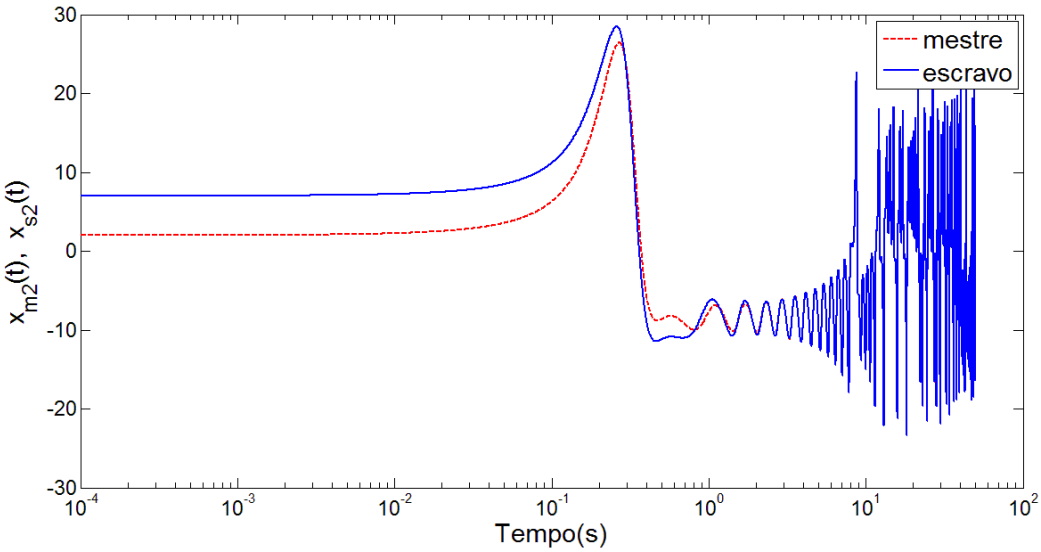


Figura 3.7. Desempenho da sincronização de x_{s2}.

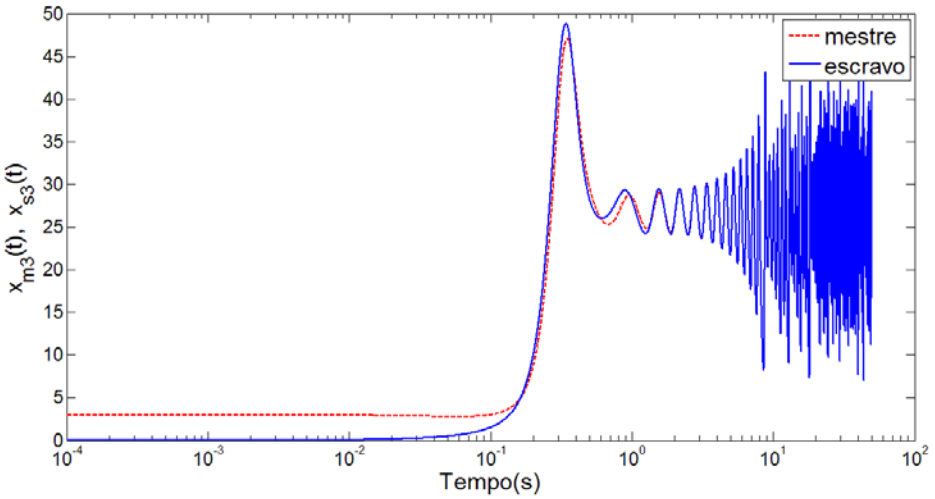


Figura 3.8. Desempenho da sincronização de x_{s3}.

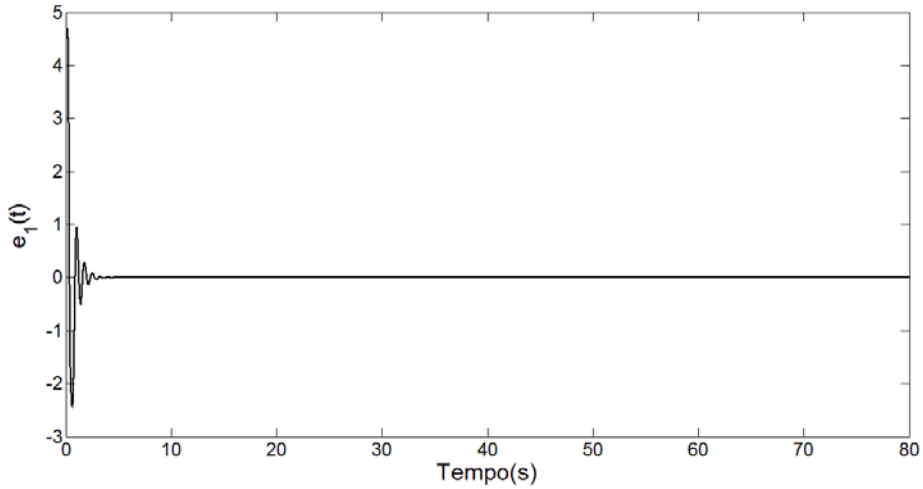


Figura 3.9. Erro de sincronização de $(x_{m1} - x_{s1})$.

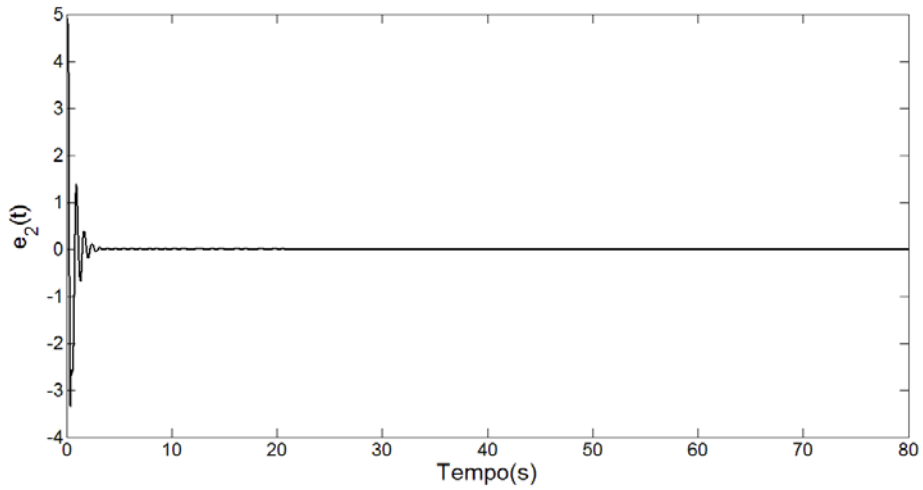


Figura 3.10. Erro de sincronização de $(x_{m2} - x_{s2})$.

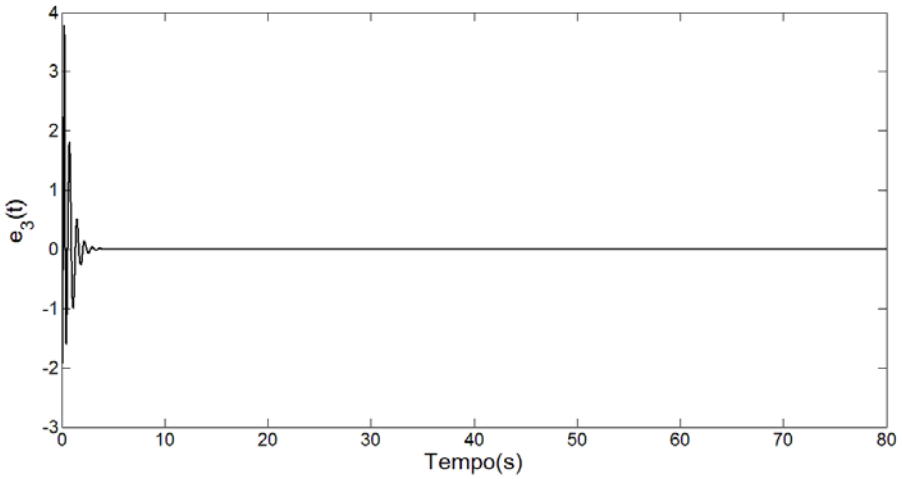


Figura 3.11. Erro de sincronização de $(x_{m3} - x_{s3})$.

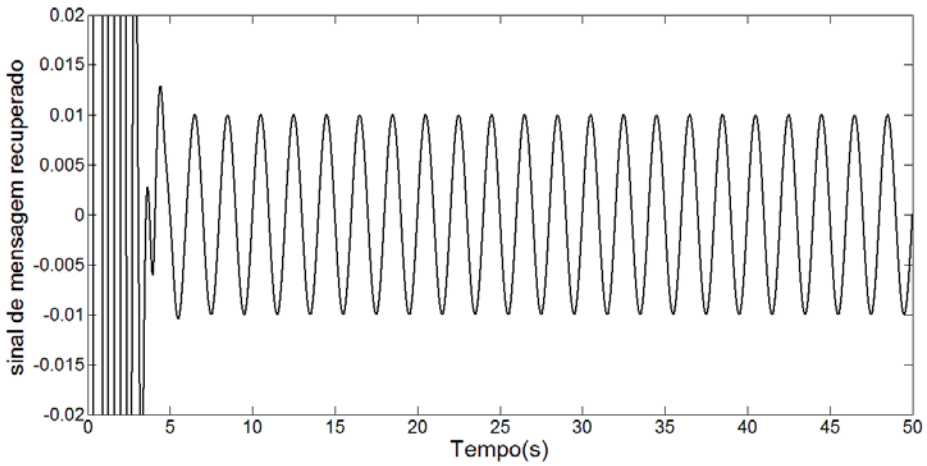


Figura 3.12. Sinal de mensagem recuperado.

3.3 SINCRONIZAÇÃO ATRAVÉS DE CONTROLE POR MODOS DESLIZANTES

Em 2012 Hou et. al., em seu trabalho [9], propuseram um método de comunicação com segurança baseado em sistemas dinâmicos caóticos utilizando sincronização por meio de controle por modos deslizantes. Este esquema de comunicação com segurança, representado pela Figura 3.13, é similar ao exposto na figura 3.5 e é considerado do tipo modulação caótica não autônoma devido à forma como a mensagem é mascarada pelo sistema. A mensagem $m(t)$ altera o atrator do sistema caótico mestre como exposto na seção 2.6.

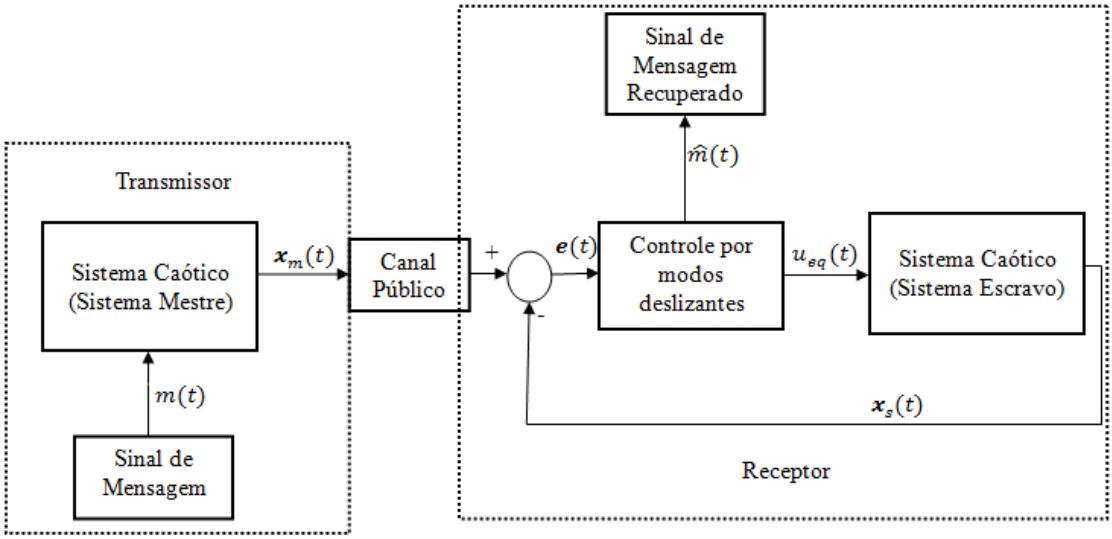


Figura 3.13. Diagrama de blocos do esquema proposto em [9].

As variáveis $\boldsymbol{x}_m(t)$, $\boldsymbol{x}_s(t)$, $e(t)$, $u_{eq}(t)$, $m(t)$ e $\hat{m}(t)$ representam respectivamente: o estado do sistema mestre, o estado do sistema escravo, o erro de sincronização, a saída do controlador, a mensagem a ser transmitida e a mensagem recuperada.

Na subseção a seguir, a viabilidade do esquema de sincronização proposto por Hou et.al. será avaliada considerando que os sistemas mestre e escravo são representados por sistemas unificados caóticos. Deve-se notar durante o processo que o esquema proposto em [9] não considera a presença de distúrbios, nem incerteza de parâmetros, o que pode tornar o esquema proposto inviável em condições práticas.

3.3.1 Esquema de sincronização

Considerando sistemas da forma (3.5), define-se como sistema mestre-escravo o seguinte sistema

$$\begin{aligned}
\dot{x}_{m1} &= (25\alpha + 10)(x_{m2} - x_{m1}) \\
\dot{x}_{m2} &= (28 - 35\alpha)x_{m1} + (29\alpha - 1)x_{m2} - x_{m1}x_{m3} + m(t) \\
\dot{x}_{m3} &= x_{m1}x_{m2} - \frac{(8+\alpha)}{3}x_{m3} \\
\dot{x}_{s1} &= (25\alpha + 10)(x_{s2} - x_{s1}) \\
\dot{x}_{s2} &= (28 - 35\alpha)x_{s1} + (29\alpha - 1)x_{s2} - x_{m1}x_{s3} + u(t) \\
\dot{x}_{s3} &= x_{m1}x_{s2} - \frac{(8+\alpha)}{3}x_{s3} \ ,
\end{aligned} \tag{3.17}$$

onde $u(t)$ é a saída do controlador utilizada para sincronizar os sistemas mestre e escravo (3.17) e $m(t)$ é a mensagem a ser transmitida.

Hipótese 2: Na região [0,∞)

$$\|m(t)\| \leq \bar{\psi} \ , \tag{3.18}$$

onde $\bar{\psi}$ é uma constante positiva.

Comentário 3: A hipótese 2 é natural uma vez que a mensagem é previamente determinada.

Definindo o vetor erro de sincronização como $\boldsymbol{e} = \boldsymbol{x}_m - \boldsymbol{x}_s$, temos, a partir de (3.17),

$$\dot{\boldsymbol{e}} = \begin{bmatrix} (25\alpha + 10)(e_2 - e_1) \\ (28 - 35\alpha)e_1 + (29\alpha - 1)e_2 - x_{m1}e_3 + m(t) - u(t) \\ x_{m1}e_2 - \frac{(8+\alpha)}{3}e_3 \end{bmatrix} \ , \tag{3.19}$$

onde $e_1 = x_{m1} - x_{s1}$, $e_2 = x_{m2} - x_{s2}$ e $e_3 = x_{m3} - x_{s3}$.

Desta forma, o controlador por modos deslizantes deve ser desenvolvido para que o vetor de erro $\boldsymbol{e}$ satisfaça

$$\lim_{t\to\infty} \|\boldsymbol{e}(t)\| = 0. \tag{3.20}$$

Para estabilizar o erro dinâmico (3.19) e alcançar a sincronização é necessário escolher uma superfície de deslizamento apropriada e estabelecer uma lei de controle por modos deslizantes que faça os estados convergirem para a superfície deslizante $s(t) = 0$. Para garantir a estabilidade assintótica do modo deslizante, a superfície $s(t)$ é definida como

$$s(t) = e_2(t) + \int_0^t \big((25\alpha + 10)e_1(\tau) + x_{m1}e_3(\tau) + \beta e_2(\tau)\big)d\tau, \tag{3.21}$$

onde $\beta > 0$ é dado. Para que o sistema opere no modo de deslizamento $s(t) = 0$ deve ser satisfeito. Com isso, temos

$$\dot{s}(t) = \dot{e}_2(t) + \big((25\alpha + 10)e_1(t) + x_{m1}e_3(t) + \beta e_2(t)\big) = 0, \tag{3.22}$$

A partir de (3.22) a dinâmica do modo deslizante é estabelecida como

$$\begin{aligned} \dot{e}_1 &= (25\alpha + 10)(e_2 - e_1) \\ \dot{e}_2 &= -\big((25\alpha + 10)e_1(t) + x_{m1}e_3(t) + \beta e_2(t)\big) \end{aligned} \tag{3.23}$$

$\dot{e}_3 = x_{m1}e_2 - \frac{(8+\alpha)}{3}e_3$,

A estabilidade da dinâmica do modo deslizante (3.23) é analisada, baseada na teoria de estabilidade de Lyapunov, abaixo.

Prova da estabilidade de (3.23): Considere a seguinte função de Lyapunov

$$V = \frac{1}{2}({e_1}^2 + {e_2}^2 + {e_3}^2) \ , \tag{3.24}$$

que é uma função diferenciável, decrescente e positiva definida. Derivando (3.24) em relação ao tempo resulta

$$\dot{V} = (e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3) \quad . \tag{3.25}$$

Avaliando (3.25) ao longo da trajetória de (3.23), obtém-se

$$\dot{V} = -(25\alpha + 10){e_1}^2 - \beta{e_2}^2 - \frac{(8+\alpha)}{3}{e_3}^2$$
$$\leq 0 \ . \tag{3.26}$$

Logo, os erros são uniformemente limitados e convergem assintóticamente para zero.

O próximo passo é desenvolver o controlador por modo deslizante que faça com que as trajetórias do sistema entrem no modo deslizante $s(t) = 0$. Para isso propõe-se um controlador da forma

$$u(t) = u_1(t) + \eta\psi\left(sign\big(s(t)\big)\right), \quad \eta > 1, \tag{3.27}$$

onde $u_1(t) = (38 - 10\alpha)e_1(t) + (29\alpha - 1 + \beta)e_2(t)$.

Teorema 1: Considerando o erro dinâmico (3.19), se o sistema for controlado por $u(t)$ (3.27), então a trajetória do sistema ira convergir para a superfície deslizante $s(t) = 0$ e irá satisfazer $\lim_{t\to\infty}\|\boldsymbol{e}(t)\| = 0$.

Prova: Considerando a seguinte função de Lyapunov

$$V = \frac{1}{2}s^2. \tag{3.28}$$

que é uma função diferenciável, decrescente e positiva definida, prova-se a convergência do erro para zero (para maiores informações vide [2]).

A partir de $\dot{\boldsymbol{e}}_2 = 0$, pode ser inferido que $\lim_{t\to\infty}\big(m(t) - u(t)\big) = 0$. Para não permitir a descontinuidade em (3.27) o controle $u(t)$ pode ser aproximado por

$$u(t) = u_1(t) + \eta\psi\left(\frac{s(t)}{|s(t)|+\sigma}\right), \tag{3.29}$$

onde σ é arbitrariamente pequeno e positivo. Entretanto esta substituição destrói as propriedades ideais de convergência do esquema.

3.3.2 Simulações

Nesta subseção avaliamos a viabilidade do esquema de comunicação proposto por meio de dois experimentos. O primeiro serve para confirmar o esquema de sincronização através de controle por modos deslizantes proposto em (3.17). O segundo experimento é para confirmar a transmissão da mensagem e sua decriptação, sendo que a mensagem é recuperada utilizando o sinal de controle $u(t)$. As simulações foram realizadas utilizando o software MatLab® Simulink e o método analítico Bogacki-Shampine com um passo fixo de 0.0001 para resolver as equações diferenciais.

Foi considerado que $\boldsymbol{x}_m(0) = [1\ 2\ 3]^T$, $\boldsymbol{x}_s(0) = [5\ 7\ 0]^T$ e $\alpha = 0$. A mensagem transmitida é da forma

$$m(t) = 0{,}5sen(5t). \tag{3.32}$$

As Figuras 3.14 a 3.16 mostram os desempenhos de sincronização obtidos com o esquema proposto e as Figuras 3.17 a 3.19 mostram os erros de sincronização. Deve ser observado que a sincronização do sistema levou 0,987s considerando que o sistema só está sincronizado quando o erro de sincronização entra na faixa de $\pm 0{,}05$. A Figura 3.20 representa o sinal de mensagem recuperado.

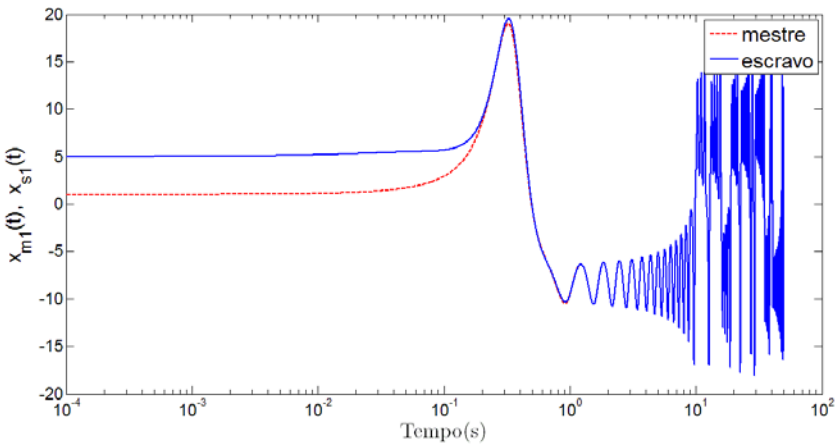


Figura 3.14. Desempenho da sincronização de x_{s1}.

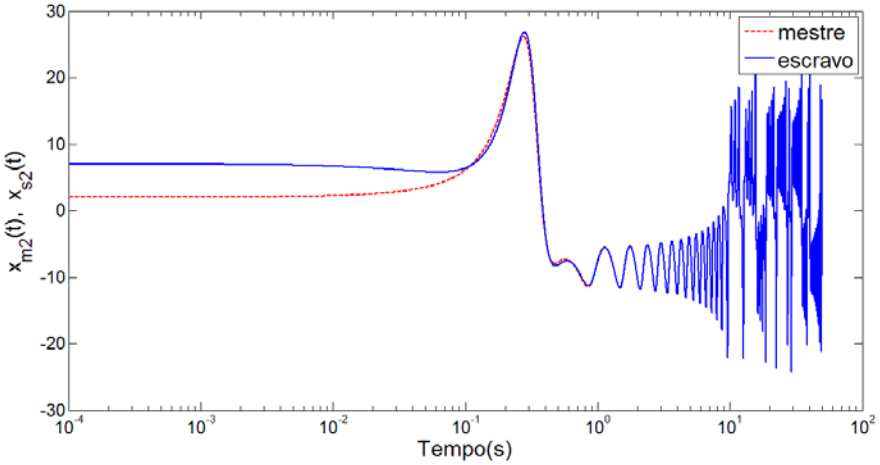


Figura 3.15. Desempenho da sincronização de x_{s2}.

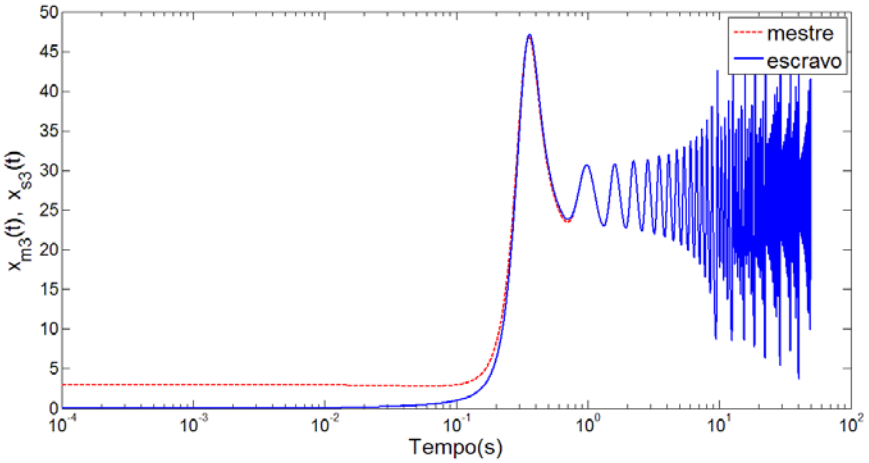


Figura 3.16. Desempenho da sincronização de x_{s3}.

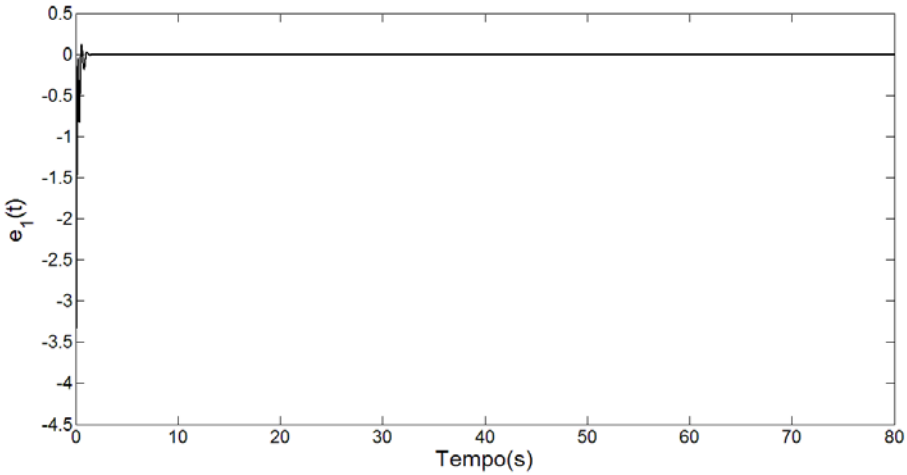


Figura 3.17. Erro de sincronização de $(x_{m1} - x_{s1})$.

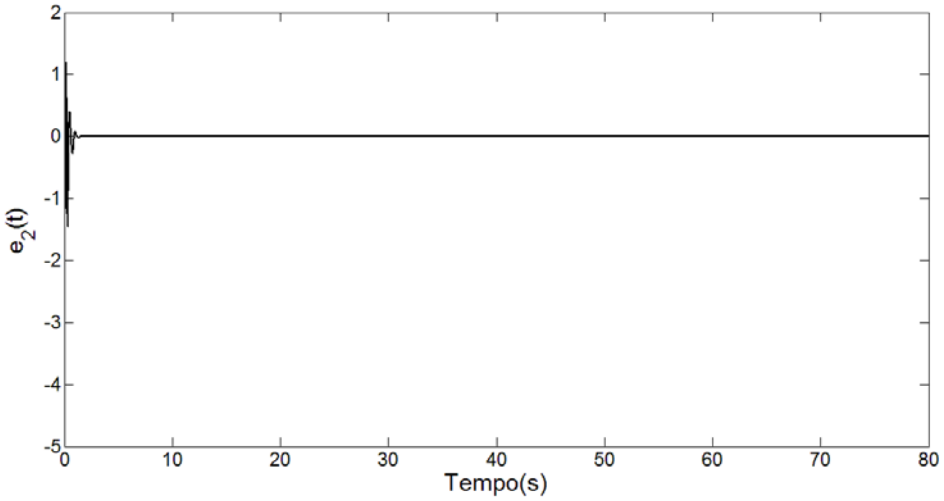


Figura 3.18. Erro de sincronização de $(x_{m2} - x_{s2})$.

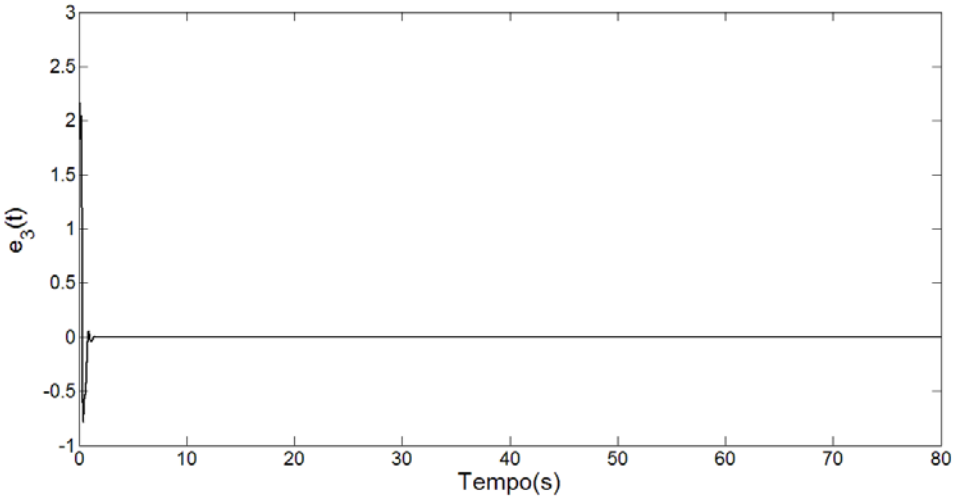


Figura 3.19. Erro de sincronização de $(x_{m3} - x_{s3})$.

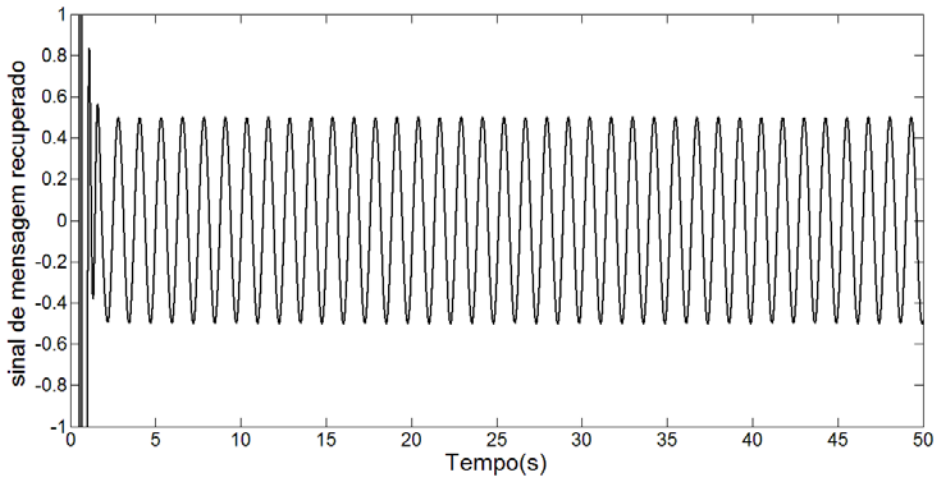


Figura 3.20. Sinal de mensagem recuperado.

3.4 CONCLUSÃO

Este capítulo apresentou além de conceitos importantes para o capítulo seguinte, dois modelos diferentes de sincronização de sistemas caóticos. Cada um dos modelos estava envolvido com uma variação diferente do método modulação caótica não autônoma. As condições e considerações propostas pelos autores de [7,9] foram utilizadas para testes de comunicação segura onde é possível avaliar a fidelidade da mensagem reconstruída e a rapidez da sincronização. As duas sincronizações foram testadas em sistemas unificados caóticos e suas viabilidades comprovadas através de extensivas simulações.

CAPÍTULO 4

ESQUEMA DE COMUNICAÇÃO COM SEGURANÇA BASEADO EM SINCRONIZAÇÃO ADAPTATIVA DE SISTEMAS CAÓTICOS UNIFICADOS

Neste capítulo, um esquema para comunicação com segurança baseado em sincronização adaptativa de sistemas caóticos unificados é proposto. O esquema de sincronização é baseado na teoria de estabilidade de Lyapunov, objetivando garantir a convergência assintótica do erro de sincronização para zero, mesmo na presença de distúrbios limitados e parâmetros incertos. Seu desenvolvimento objetiva melhorar os esquemas apresentados no capítulo anterior.

4.1 INTRODUÇÃO

Recentemente vários esquemas para comunicação com segurança baseados em sincronização de sistemas caóticos têm sido propostos na literatura [10, 33, 34, 35, 36]. Nestes esquemas, o objetivo básico é mascarar a informação transmitida, de forma que esta não seja acessível nas redes públicas de transmissão. Para tanto, é necessário embutir os dados a serem transmitidos em um sistema caótico (sistema mestre/transmissor), de forma que o sinal transmitido não possa ser decifrado por terceiros. No receptor, constituído por outro sistema caótico (sistema escravo), através de um processo de sincronização caótica, os dados são recuperados. Desta forma, espera-se que a confidencialidade da informação transmitida seja assegurada. Os canais de transmissão típicos incluem, por exemplo, telefonia celular e comunicação por satélite.

Entretanto, esquemas existentes na literatura, vide por exemplo [36,10], assumem que o sistema mestre e escravo são exatamente iguais ou, pelo menos estruturalmente conhecidos. Hipóteses que limitam sua aplicação em situações reais, onde dinâmica não modelada, diferentes condições de operação e alteração das características físicas dos dispositivos de transmissão por envelhecimento ou falhas são inevitáveis. Embora a

proposta de ausência de distúrbios seja interessante do ponto de vista teórico, na prática, esquemas que ignoram tais fatores podem ter seu desempenho prejudicado.

Além disso, esquemas como os introduzidos em [7] e [9] possuem apenas um nível de segurança, i.e., há apenas a presença da dinâmica caótica mascarando o sinal, não há criptografia adicional. Esquemas desse tipo são mais suscetíveis a quebras de segurança bem sucedidas no canal público.

Motivado pelos fatores expostos acima, propõe-se a utilização de um esquema para comunicação com segurança baseado na sincronização adaptativa de dois sistemas caóticos unificados. Assume-se a presença de parâmetros incertos e distúrbios limitados internos ou externos. Neste cenário, ao contrário da maioria dos resultados existentes na literatura, é assegurada a convergência assintótica para zero do erro de sincronização, o que tem um impacto positivo na recuperação do sinal transmitido e segurança da transmissão. Pois é assegurada uma perfeita recuperação do sinal na ausência de ruído de canal. Adicionalmente, a segurança do esquema é melhorada, pois são empregados outros dois sistemas caóticos para mascarar e desmascarar dois dos três estados que serão transmitidos pelo canal público. Para a prova de estabilidade e convergência é usada uma análise *Lyapunov-like*. O esquema é validado através de um estudo computacional e comparado com outras propostas da literatura.

4.2 ESQUEMA DE COMUNICAÇÃO PROPOSTO

A arquitetura do esquema de comunicação com segurança proposto, que é motivado por [10], é estabelecida por quatro sistemas unificados caóticos diferentes e sujeitos a distúrbios como mostrado na Figura 4.1.

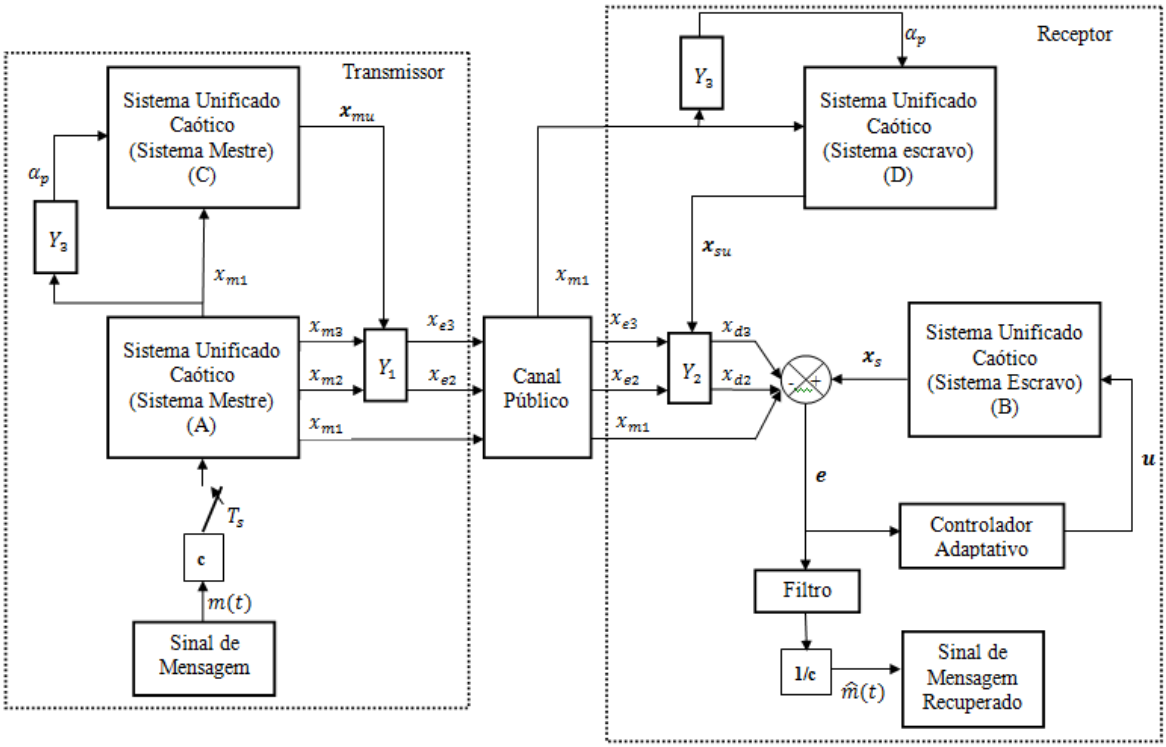


Figura 4.1. Esquema de comunicação com segurança proposto.

No transmissor tem-se o Sistema Unificado Caótico (A) com parâmetro α e no receptor têm-se o Sistema Unificado Caótico (B), o qual utiliza uma estimativa $\hat{\alpha}$ do valor de α e um controlador adaptativo $\boldsymbol{u}$. A mensagem original $m(t)$ é multiplicada por um fator constante c antes de ser inserida no sistema caótico mestre e altera o atrator do sistema (A) após um tempo T_s, que é maior que o tempo necessário para que todo circuito atinja a sincronização. Por isso, esse esquema é do tipo modulação caótica não autônoma. O fator c é escolhido de modo a reduzir a mensagem ao ponto onde ela se torne imperceptível quando mascarada por (A). Simultaneamente, o sistema (C) recebe a componente de estado x_{m1} de (A) diretamente e também através da modulação de α_p pelo bloco Y_3. Os sinais de estado de (C) são então utilizados para mascarar dois estados do sistema (A) utilizando o bloco Y_1. Os sinais resultantes da encriptação x_{e2}, x_{e3} são então enviados junto à x_{m1} através do canal público. No receptor, (D) recebe a componente de estado x_{m1} a qual será responsável não só por sincronizar os sistemas (C) e (D) por sinal comum, mas também reconstruir o parâmetro α_p. Os sinais de estados resultantes de (D) serão responsáveis por decriptar os sinais x_{e2}, x_{e3} utilizando bloco Y_2. Os sinais resultantes da decriptação x_{d2}, x_{d3}, juntos a x_{m1} e o vetor de estados de (B) $\boldsymbol{x}_s$ geram o vetor de erro de sincronização $\boldsymbol{e}$. O erro atua como entrada no controlador adaptativo e este faz com que (A) e (B) atinjam a sincronia. O mesmo sinal de erro passa

por um processo de filtragem e dá origem a $\widehat{m}(t)$. As fórmulas que compõe os blocos Y_1, Y_2 e Y_3 serão definidas pelas equações (4.37)-(4.41).

4.3 SINCRONIZAÇÃO DOS SISTEMAS CAÓTICOS PRINCIPAIS

4.3.1 Formulação do problema

Considere o sistema caótico unificado descrito pela seguinte equação diferencial

$$\dot{x}_m = (\alpha A + B)x_m + f_m(x_m) + cm(t) \tag{4.1}$$

onde $x_m \in \mathbb{R}^3$ é o estado do sistema mestre, c é uma constante positiva conhecida, $m(t)$ é a mensagem a ser enviada, α é um parâmetro conhecido,

$$A = \begin{bmatrix} -25 & 25 & 0 \\ -35 & 29 & 0 \\ 0 & 0 & -\frac{1}{3} \end{bmatrix}, \tag{4.2}$$

$$B = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -\frac{8}{3} \end{bmatrix} \tag{4.3}$$

e

$$f_m(x_m) = \begin{bmatrix} 0 \\ -x_{m1}x_{m3} \\ x_{m1}x_{m2} \end{bmatrix}. \tag{4.4}$$

Assume-se que o seguinte possa ser estabelecido.

Hipótese 3: Na região $[0, \infty)$

$$\|m(t)\| \leq m_0 \tag{4.5}$$

onde m_0 é uma constante conhecida positiva.

Hipótese 4: O parâmetro α é limitado superiormente por uma constante positiva conhecida $\bar{\alpha}$, tal que $\bar{\alpha} \geq \alpha$.

Comentário 4: A hipótese 4 é natural uma vez que a mensagem é previamente determinada.

Comentário 5: No caso em que $\alpha = 0$, $\alpha = 0.8$ e $\alpha = 1$, o sistema (4.1) torna-se os sistemas Lorenz, Lü e Chen respectivamente quando $m(t) = 0$.

A fim de ter um problema bem colocado, sem perda de generalidade, considere o seguinte sistema escravo

$$\dot{x}_s = (\hat{\alpha}A + B)x_s + f_s(x_s) + d(x_s, t) + u, \tag{4.6}$$

onde $x_s \in \mathbb{R}^3$ é o estado do sistema escravo, $u \in \mathbb{R}^3$ é o sinal de controle, $d(x_s, t)$ é um distúrbio desconhecido e $\hat{\alpha}$ é a estimação do parâmetro α do sistema mestre que se assume desconhecido para o sistema escravo,

$$f_s(x_s) = \begin{bmatrix} 0 \\ -x_{s1}x_{s3} \\ x_{s1}x_{s2} \end{bmatrix}. \tag{4.7}$$

Assume-se que o seguinte possa ser estabelecido.

Hipótese 5: Na região $\mathbb{R}^3 \times [0, \infty)$

$$\|d(x_s, t)\| \leq d_{s0} \tag{4.8}$$

onde d_{s0} é uma constante positiva, tal que $d_{s0} \leq \bar{d}_0$ e $\bar{d}_0$ é uma constante conhecida.

Comentário 6: A hipótese 5 é natural uma vez que sistemas caóticos evoluem em um conjunto compacto.

Portanto, nosso objetivo é projetar um controlador por realimentação u, tal que o estado x_s do sistema caótico escravo (4.6) sincronize com o estado x_m do sistema mestre (4.1), isto é, $\lim_{t\to\infty}[x_s - x_m] = \mathbf{0}$.

Defina o erro de sincronização como $\boldsymbol{e} = \boldsymbol{x}_s - \boldsymbol{x}_m$. Então, de (4.1) e (4.6), obtém-se a equação de erro de sincronização

$$\dot{e} = \hat{\alpha}Ae + \tilde{\alpha}Ax_m + Be + f_s(x_s) - f_m(x_m) + D(t) + u \tag{4.9}$$

onde

$$D(t) = d(t) - cm(t)$$
$$\tilde{\alpha} = \hat{\alpha} - \alpha. \tag{4.10}$$

Comentário 7: Note que nesta formulação, por simplicidade, foi considerado que $f_m(.)$ e $f_s(.)$ tem a mesma estrutura. Entretanto, esses mapeamentos não lineares podem não estar relacionados entre si, por exemplo, para incluir o conhecimento prévio de distúrbios.

4.3.2 Sincronização adaptativa

Considerando as limitações físicas da maioria das aplicações do mundo real, este estudo abandona a suposição irreal de que os dois sistemas, mestre e escravo, são idênticos. Assim, objetiva-se a sincronização de dois sistemas unificados caóticos diferentes considerando distúrbios e a presença de parâmetros desconhecidos. Nesta seção, desenvolver-se-á um esquema de sincronização adaptativa para os dois sistemas caóticos. Prova-se usando uma análise *Lyapunov-like*, que o erro de sincronização converge assintoticamente para zero.

Teorema 2: Considere os sistemas escravo (4.6) e mestre (4.1), que satisfazem as hipóteses 1-3, a lei de controle

$$u = -(\hat{\alpha}Ae + \tilde{\alpha}Ax_m + Be + f_s(x_s) - f_m(x_m)) - Le - u_r \tag{4.11}$$

com

$$u_r = \frac{le}{\lambda_{min}(K)[\|e\| + \gamma_1 \exp(-\gamma_0 t)]} \tag{4.12}$$

$$\dot{\hat{\alpha}} = -\gamma_\alpha[\gamma_2\|e\|\hat{\alpha} + e^T KAx_m] \tag{4.13}$$

onde

$$\begin{aligned} &Q = L^T P + PL,\ P = P^T > 0,\ Q > 0,\ K = P + P^T \\ &\gamma_2 > 0,\ \gamma_1 > 0,\ \gamma_0 \geq 0,\ \gamma_\alpha > 0 \\ &\|\alpha\| \leq \bar{\alpha},\ \|D(t)\| \leq D_0,\ \ \forall t \geq 0. \\ &\frac{l}{2} = \|K\|_F D_0 + \frac{\gamma_2}{2}\bar{\alpha}^2, \end{aligned} \tag{4.14}$$

e $\|K\|_F$ é a norma de Frobenius de K. Então, os sistemas mestre e escravo sincronizam, i.e., $\lim_{t\to\infty}\|e(t)\| = 0$.

Prova: Considere a seguinte candidata a função de Lyapunov

$$V = e^T Pe + \frac{\gamma_\alpha{}^{-1}\tilde{\alpha}^2}{2} \quad . \tag{4.15}$$

Derivando (4.15) em relação ao tempo resulta

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + \gamma_\alpha{}^{-1} \tilde{\alpha} \dot{\tilde{\alpha}} \ . \tag{4.16}$$

Utilizando (4.11), o erro de sincronização em malha fechada pode ser escrito como

$$\dot{e} = -Le + \tilde{\alpha} A x_m + D(t) - u_r \ \ . \tag{4.17}$$

Avaliando (4.16) ao longo da trajetória de (4.17), obtém-se

$$\dot{V} = -e^T (L^T P + PL) e + e^T (P + P^T) \tilde{\alpha} A + e^T (P + P^T)(D(t) - u_r) + \gamma_\alpha{}^{-1} \tilde{\alpha} \dot{\tilde{\alpha}}. \tag{4.18}$$

Substituindo (4.13) e (4.14) em (4.18) resulta

$$\dot{V} = -e^T Q e + e^T K D(t) - e^T K u_r - \gamma_2 \tilde{\alpha} \hat{\alpha} \|e\| \ . \tag{4.19}$$

Adicionalmente, pode-se estabelecer que

$$\tilde{\alpha}\hat{\alpha} = \frac{1}{2}\tilde{\alpha}^2 + \frac{1}{2}\dot{\alpha}^2 - \frac{1}{2}\alpha^2 \ , \tag{4.20}$$

$$\lambda_{\text{mín}}(\text{Q}) \|e\|^2 \leq e^T Q e \leq \lambda_{\text{máx}}(\text{Q}) \|e\|^2 \ \ . \tag{4.21}$$

Deste modo, empregando as hipóteses 1-3, as equações (4.14), (4.20)-(4.21), (4.19) implica

$$\dot{V} \leq -\gamma_3 \|e\|^2 + \|K\|_F D_0 \|e\| - e^T K u_r + \frac{\gamma_2}{2} \alpha^2 \|e\| - \frac{\gamma_2}{2} \tilde{\alpha}^2 \|e\| \tag{4.22}$$

onde $\gamma_3 = \lambda_{mín}(Q)$. A substituição de (4.12) em (4.22) resulta

$$\dot{V} \leq -\gamma_3 \|e\|^2 + \left(\|K\|_F D_0 + \frac{\gamma_2}{2} \bar{\alpha}^2 \right) \|e\| - \frac{l \|e\|^2}{[\|e\| + \gamma_1 \exp(-\gamma_0 t)]} - \frac{\gamma_2}{2} \tilde{\alpha}^2 \|e\|. \tag{4.23}$$

Utilizando-se (4.14) em (4.23), tem-se

$$\dot{V} \leq -\gamma_3 \|e\|^2 - \frac{\frac{l}{2}\|e\|[\|e\| - \gamma_1 \exp(-\gamma_0 t)]}{[\|e\| + \gamma_1 \exp(-\gamma_0 t)]} - \frac{\gamma_2}{2} \tilde{\alpha}^2 \|e\| \ \ . \tag{4.24}$$

Note que a expressão anterior implica

$$\dot{V} \leq -\|e\| (\gamma_3 \|e\| - \frac{l}{2} + \frac{\gamma_2}{2} \tilde{\alpha}^2) \ . \tag{4.25}$$

Portanto $\dot{V} \leq 0$ sempre que $\|e\| \geq \frac{l}{2\gamma_3} = \alpha_1$ ou $|\tilde{\alpha}| \geq \sqrt{\frac{l}{\gamma_2}} = \alpha_2$.

Então, uma vez que α_1 e α_2 são constantes, empregando-se os argumentos usuais de Lyapunov ([14]), conclui-se que $e(t)$ e $\tilde{\alpha}(t)$ são uniformemente limitadas.

Por outro lado, a desigualdade (4.24) implica

$$\dot{V} \leq -\gamma_3\|e\|^2 - \frac{\frac{l}{2}\|e\|[\|e\|-\gamma_1\exp(-\gamma_0 t)]}{[\|e\|+\gamma_1\exp(-\gamma_0 t)]}. \tag{4.26}$$

Para mostrar que o erro de sincronização converge para zero define-se uma região Ω como:

$$\Omega = \{e(t) \mid \|e(t)\| \leq \gamma_1\exp(-\gamma_0 t), t \geq 0\}. \tag{4.27}$$

Então, no caso em que $\|e(t)\| > \gamma_1\exp(-\gamma_0 t)$ ou $e \in \Omega^C$ tem-se:

$$\dot{V} \leq -\gamma_3\|e\|^2 \tag{4.28}$$

Logo, os erros são uniformemente limitados. Além disso, uma vez que V é limitada inferiormente e não crescente com o tempo, advém

$$\lim_{t\to\infty}\int_0^t\|e(\tau)\|^2\,d\tau \leq \frac{V(0)-V_\infty}{\gamma_3} < \infty \tag{4.29}$$

onde $\lim_{t\to\infty} V(t) = V_\infty < \infty$. Note que, baseado em (4.17), com os limites de e, $\tilde{\alpha}$ e $D(t)$, u_r também é limitada. Então, $\dot{V}$ é uniformemente continua. Portanto, aplicando o Lema de Barbalat presente na subseção 2.3.3, conclui-se que $\lim_{t\to\infty} e(t) = 0$.

4.4 SINCRONIZAÇÃO DOS SISTEMAS CAÓTICOS AUXILIARES

4.4.1 Formulação do problema

Considere o sistema caótico unificado descrito pelo seguinte sistema mestre-escravo com sinal comum x_{m1} inserido e $\alpha = \alpha_p$

$$\begin{aligned}
\dot{x}_{mu1} &= (25\alpha_p + 10)(x_{mu2} - x_{mu1})\\
\dot{x}_{mu2} &= (28 - 35\alpha_p)x_{m1} - x_{m1}x_{mu3} + (29\alpha_p - 1)x_{mu2}\\
\dot{x}_{mu3} &= x_{m1}x_{mu2} - \frac{8+\alpha_p}{3}x_{mu3}\\
\dot{x}_{su1} &= (25\alpha_p + 10)(x_{su2} - x_{su1}) + d_{s1}(\boldsymbol{x}_{su}, t)
\end{aligned} \quad . \tag{4.30}$$

$$\dot{x}_{su2} = (28 - 35\alpha_p)x_{m1} - x_{m1}x_{su3} + (29\alpha_p - 1)x_{su2} + d_{s2}(\boldsymbol{x}_{su}, t)$$

$$\dot{x}_{su3} = x_{m1}x_{su2} - \frac{8+\alpha_p}{3}x_{su3} + d_{s3}(\boldsymbol{x}_{su}, t)$$

onde $\boldsymbol{x}_{mu}$ representa o sistema mestre, $\boldsymbol{x}_{su}$ representa o sistema escravo e $\boldsymbol{d}_s(\boldsymbol{x}_{su}, t)$ um distúrbio desconhecido.

Hipótese 6: Na região $\Re^3 \times [0, \infty)$

$$d_{s1}(\boldsymbol{x}_{su}, t) \leq d_{su0}$$

$$d_{s2}(\boldsymbol{x}_{su}, t) \leq d_{su0} \tag{4.31}$$

$$d_{s3}(\boldsymbol{x}_{su}, t) \leq d_{su0}$$

onde d_{su0} é uma constante positiva, tal que $d_{su0} \leq \bar{d}_{u0}$ e $\bar{d}_{u0}$ é uma constante conhecida.

Comentário 8: A hipótese 1 é natural uma vez que sistemas caóticos evoluem em um conjunto compacto.

Definindo o erro de sincronização como $\boldsymbol{e}_u = \boldsymbol{x}_{su} - \boldsymbol{x}_{mu}$, temos, a partir de (4.30),

$$\dot{\boldsymbol{e}}_u = \begin{bmatrix} (25\alpha_p + 10)(e_{u2} - e_{u1}) + d_{s1}(\boldsymbol{x}_{su}, t) \\ -x_{m1}e_{u3} + (29\alpha_p + 1)e_{u2} + d_{s2}(\boldsymbol{x}_{su}, t) \\ x_{m1}e_{u2} - \frac{8+\alpha_p}{3}e_{u3} + d_{s3}(\boldsymbol{x}_{su}, t) \end{bmatrix} \tag{4.32}$$

onde $e_{u1} = x_{su1} - x_{mu1}$, $e_{u2} = x_{su2} - x_{mu2}$ e $e_{u3} = x_{su3} - x_{mu3}$.

4.4.2 Sincronização por sinal comum

Considerando as limitações físicas da maioria das aplicações do mundo real, este estudo abandona a suposição irreal de que os dois sistemas, mestre e escravo, são idênticos. Assim, objetiva-se a sincronização de dois sistemas unificados caóticos diferentes considerando distúrbios. Nesta seção, desenvolver-se-á um esquema de sincronização por sinal comum para os dois sistemas caóticos.

Fato 1: Tem-se que

$$\sqrt{3}\|\boldsymbol{e}_u\| \geq (e_{u1} + e_{u2} + e_{u3}) \tag{4.33}$$

Teorema 3: Considerando o sistema mestre-escravo definido por (4.30), o erro de sincronização será estável e limitado.

Prova: Considere a seguinte função decrescente e positiva definida

$$V = \frac{1}{2}\left(\left(\frac{1-29\alpha_p}{25\alpha_p+10}\right){e_{u1}}^2 + {e_{u2}}^2 + {e_{u3}}^2\right) \tag{4.34}$$

Derivando (4.34) em relação ao tempo resulta

$$\dot{V} = \left(\frac{1-29\alpha_p}{25\alpha_p+10}\right)e_{u1}\dot{e}_{u1} + e_{u2}\dot{e}_{u2} + e_{u3}\dot{e}_{u3}\ . \tag{4.35}$$

Avaliando (4.35) ao longo da trajetória de (4.32) e considerado $L = 1 - 29\alpha_p$, obtém-se

$$\begin{aligned}
\dot{V} &= \left(\frac{L}{25\alpha_p+10}\right)e_{u1}d_{s1} + e_{u2}d_{s2} + e_{u3}d_{s3} - (L)({e_{u1}}^2 - e_{u1}e_{u2} + {e_{u2}}^2) - \frac{8+\alpha_p}{3}e_{u3} \\
&= -(L)(e_{u1} - e_{u2})^2 - \left(\frac{8+\alpha_p}{3} - \frac{L}{2}\right)e_{u3} - \left(\frac{L}{2}\right)\|\boldsymbol{e}\|^2 + \left(\frac{L}{25\alpha_p+10}\right)e_{u1}d_{s1} + e_{u2}d_{s2} + e_{u3}d_{s3} \\
&\leq -(L)(e_{u1} - e_{u2})^2 - \left(\frac{8+\alpha_p}{3} - \frac{L}{2}\right)e_{u3} - \left(\frac{L}{2}\right)\|\boldsymbol{e}\|^2 + e_{u1}d_{s1} + e_{u2}d_{s2} + e_{u3}d_{s3} \qquad (4.35) \\
&\leq -(L)(e_{u1} - e_{u2})^2 - \left(\frac{8+\alpha_p}{3} - \frac{L}{2}\right)e_{u3} - \left(\frac{L}{2}\right)\|\boldsymbol{e}\|^2 + \bar{d}_{su0}(e_{u1} + e_{u2} + e_{u3}) \\
&\leq -(L)(e_{u1} - e_{u2})^2 - \left(\frac{8+\alpha_p}{3} - \frac{L}{2}\right)e_{u3} - \left(\frac{1}{2}\right)\|\boldsymbol{e}\|^2 + \sqrt{3}\bar{d}_{su0}\|e\|
\end{aligned}$$

onde o fato 1 foi utilizado para a obtenção da última desigualdade. Portanto $\dot{V} \leq 0$ sempre que $\|e\| \geq 2\sqrt{3}\bar{d}_{su0}$ e $\alpha_p \in [0, \frac{1}{29})$.

Então uma vez que $2\sqrt{3}\bar{d}_{u0}$ é constante, empregando os argumentos usuais de Lyapunov presentes na subseção 2.3.2, conclui-se que o erro $\boldsymbol{e}$ uniformemente limitado. Adicionalmente, na ausência de distúrbios, considerado que $\alpha_p \in [0, \frac{1}{29})$, $\dot{V} < 0$ e $\lim_{t\to\infty} \boldsymbol{e}(t) = 0$.

4.5 SIMULAÇÕES

Nesta seção, se valida o sistema de comunicação proposto e verifica-se suas melhorias em relação aos trabalhos [7,9]. O primeiro experimento serve para validar o esquema de sincronização adaptativa proposto em 4.3 e o esquema de sincronização por sinal comum proposto em 4.4. Confirmar o esquema de sincronização por sinal comum

proposto em 4.6 e confirmar a sincronização do sistema de comunicação com segurança como um todo. O segundo experimento é para confirmar a transmissão da mensagem e sua decriptação, além de mostrar as melhorias em relação aos esquemas analisados. A mensagem transmitida é uma sequência de bits que compõe a imagem escolhida em escala de cinza (8 *bits* por pixel). Vide figura 4.2 para maiores detalhes. As simulações foram realizadas utilizando o software MATLAB e o método numérico analítico Bogacki-Shampine com um passo fixo de 0.0001 para resolver as equações diferenciais presentes neste estudo.

Figura 4.2. Imagem digital Lena em escala de cinza.

Foi considerado que $x_m(0) = [1\ 2\ 3]^T$, $x_s(0) = [5\ 7\ 0]^T$, $x_{mu}(0) = [3\ 3\ 3]^T$ e $x_{su}(0) = [3.5\ 3.5\ 3.5]^T$. Para obter a sincronização do sistema escravo (B) (4.6) e o sistema mestre (A) (4.1), foram utilizadas as leis de controle (4.11)-(4.12) e a lei de adaptação (4.13). A sincronização dos sistemas escravo (D) e mestre (C) ocorre por meio de sinal comum.

Os parâmetros utilizados nas simulações foram $\alpha = 1$, $\hat{\alpha}(0)$ =0.8, $l = 0.0001$, $\gamma_0 = 0.01$, $\gamma_1 = 1$, $\gamma_2 = 20$, $\gamma_\alpha = 0.05$ e $P = diag(0.0001, 0.1, 0.05)$. O parâmetro α_p é obtido por

$$\alpha_p = \frac{|x_{m1}|}{29(|x_{m1}|+1)} \tag{4.37}$$

e as chaves de encriptação e decriptação foram consideradas respectivamente como

$$x_{e2} = \frac{(x_{m2}+x_{mu2})}{|x_{mu2}|+1} \tag{4.38}$$

$$x_{e3} = \frac{(x_{m3}+x_{mu3})}{|x_{mu3}|+1} \tag{4.39}$$

e

$$x_{d2} = x_{e2}(|x_{mu2}| + 1) - x_{mu2} \tag{4.40}$$

$$x_{d3} = x_{e3}(|x_{mu3}| + 1) - x_{mu3} \tag{4.41}$$

As equações (4.37-4.41) são motivadas por [10].

4.5.1 Primeiro experimento

Inicialmente considera-se que não há a presença de distúrbio ou incertezas nos sistemas (A), (B), (C) e (D). Desta forma $d(x_s, t) = 0$ e $d_s(\boldsymbol{x}_{su}, t) = 0$. As Figuras 4.3 a 4.5 e 4.9 a 4.11 mostram o desempenho da sincronização dos sistemas mestre escravo (A)-(B) e (C)-(D). Já as Figuras 4.6 a 4.8 e 4.12 a 4.14 mostram os erros de sincronização dos sistemas mestre escravo (A)-(B) e (C)-(D). Utilizou-se uma escala logarítmica para mostrar o rápido transiente alcançado. Pode-se observar que as simulações confirmam os resultados teóricos. Observa-se que a sincronização do sistema A levou 0,0023s e a do sistema C 2,063s considerando que o sistema só está sincronizado quando o erro de sincronização entra na faixa de $\pm 0{,}05$.

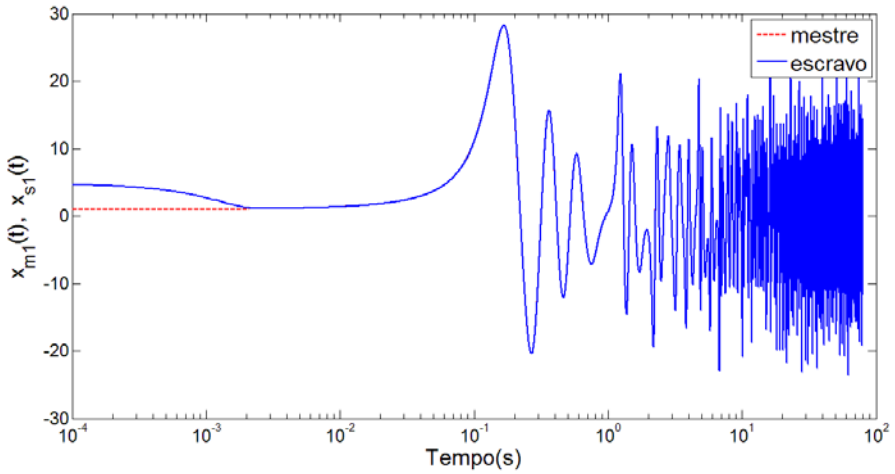


Figura 4.3. Desempenho da sincronização de x_{s1} (A-B).

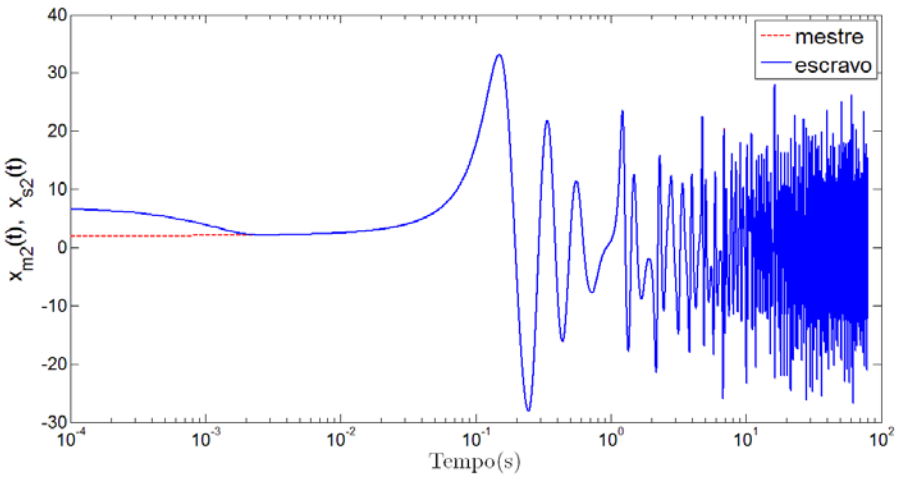


Figura 4.4. Desempenho da sincronização de x_{s2} (A-B).

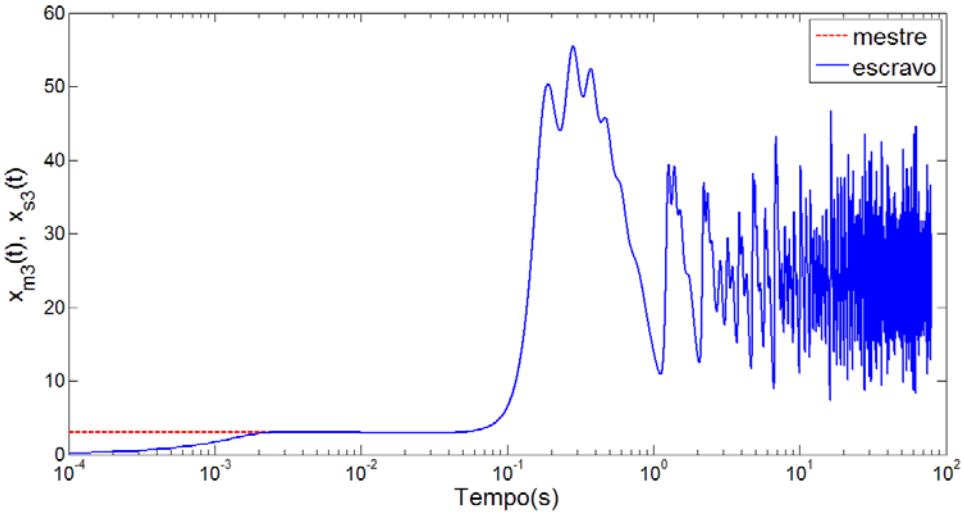


Figura 4.5. Desempenho da sincronização de x_{s3} (A-B).

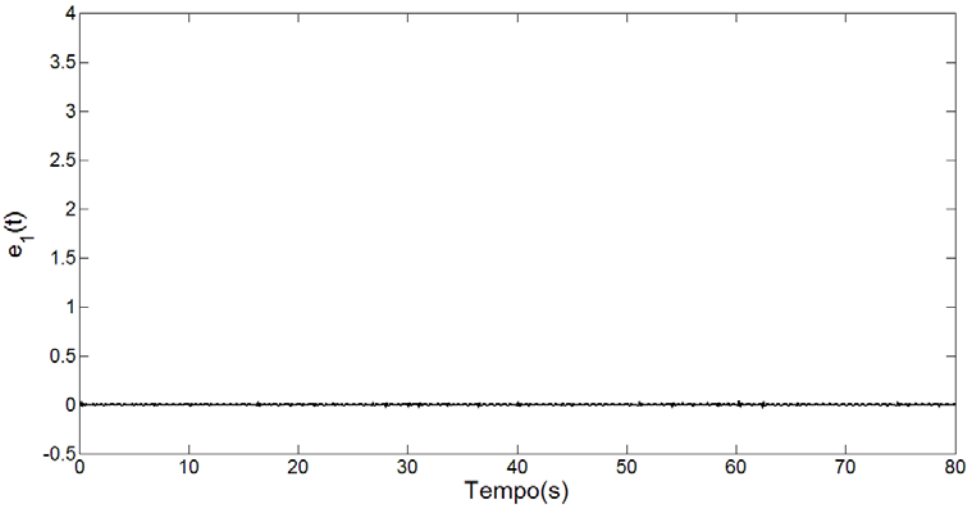


Figura 4.6. Erro de sincronização $(x_{m1} - x_{s1})$ de (A-B).

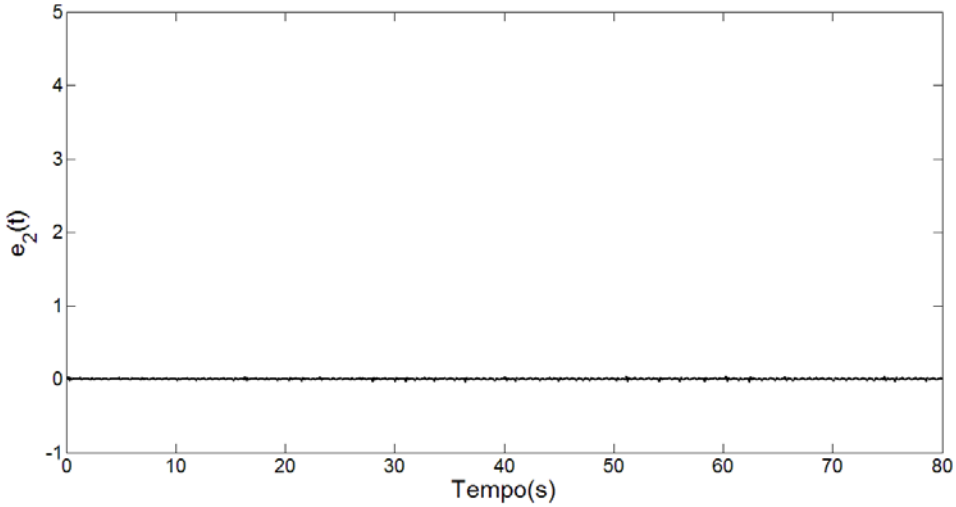


Figura 4.7. Erro de sincronização $(x_{m2} - x_{s2})$ de (A-B).

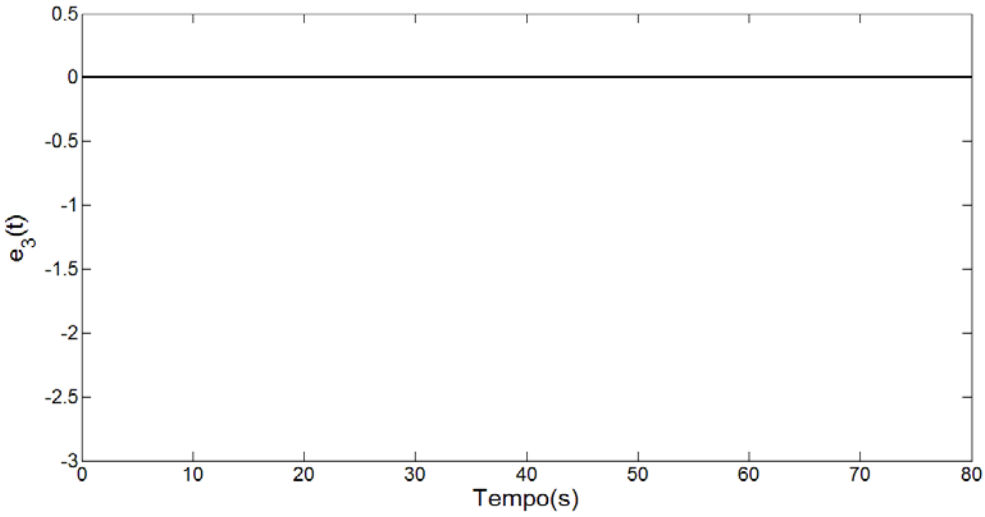


Figura 4.8. Erro de sincronização $(x_{m3} - x_{s3})$ de (A-B).

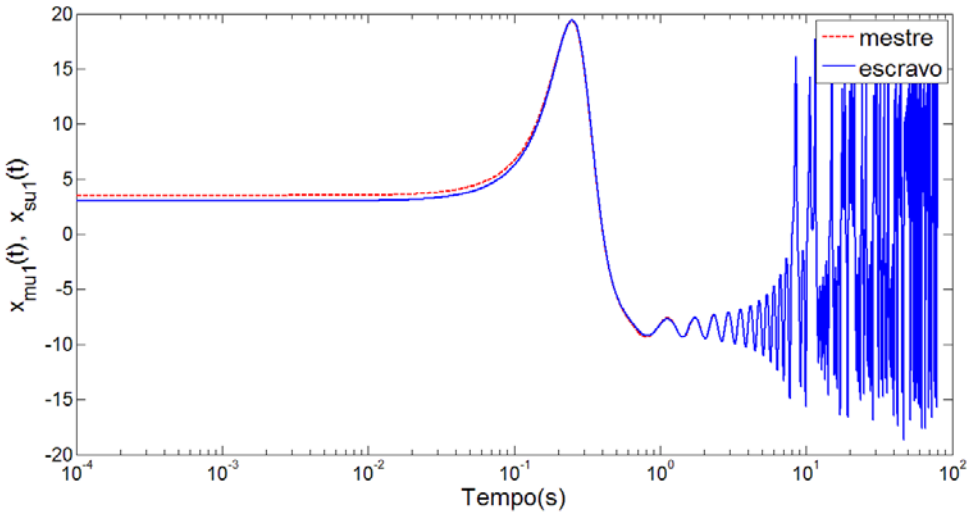


Figura 4.9. Desempenho da sincronização de x_{su1} (C-D).

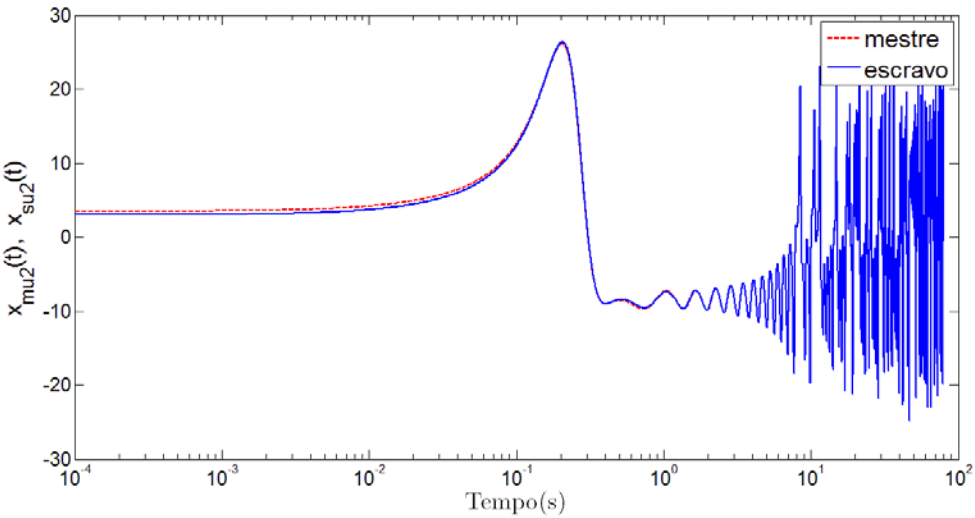


Figura 4.10. Desempenho da sincronização de x_{su2} (C-D).

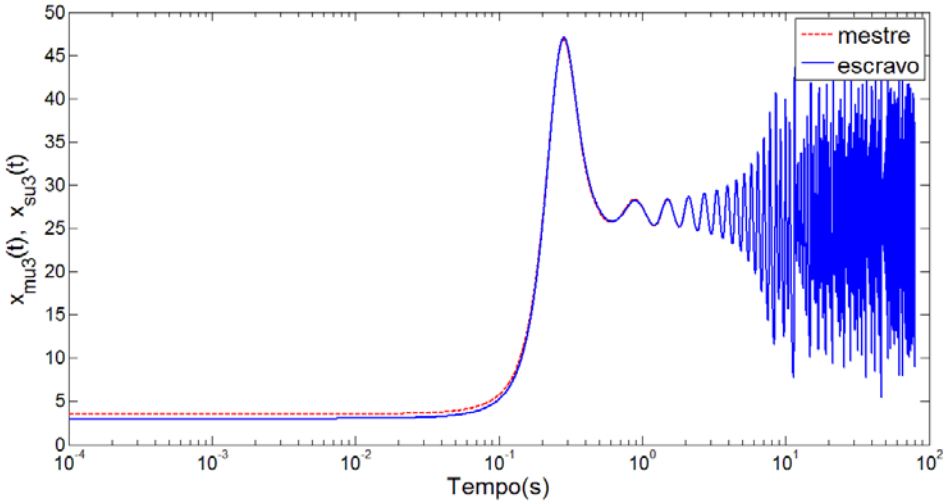


Figura 4.11. Desempenho da sincronização de x_{su3} (C-D).

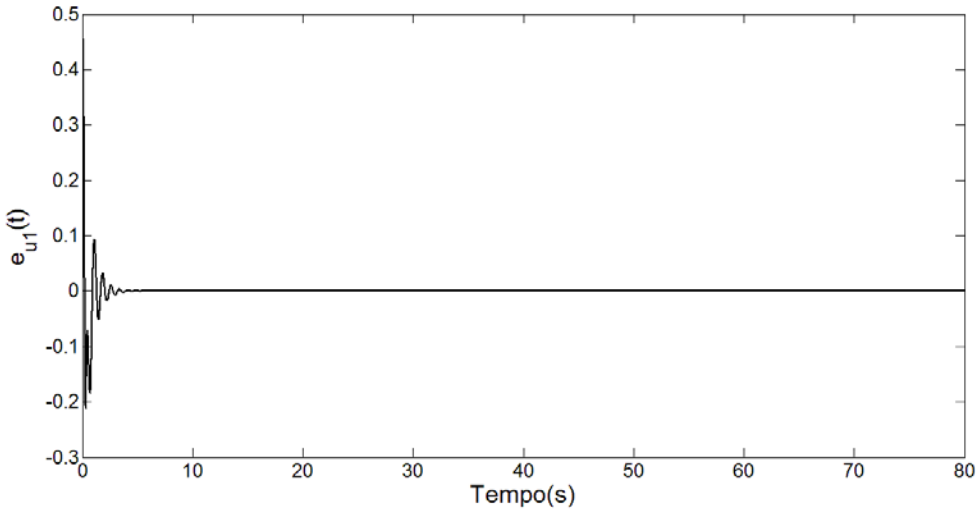


Figura 4.12. Erro de sincronização $(x_{mu1} - x_{su1})$ de (C-D).

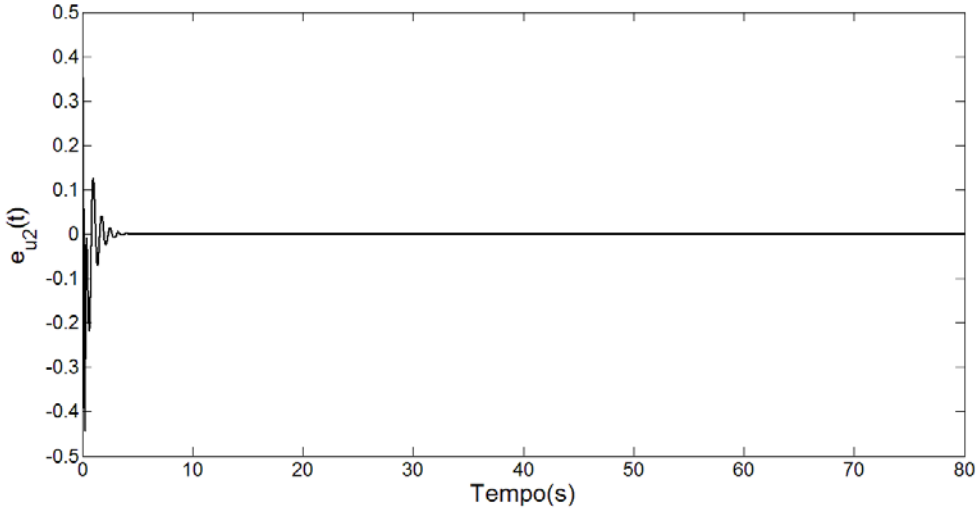


Figura 4.13. Erro de sincronização $(x_{mu2} - x_{su2})$ de (C-D).

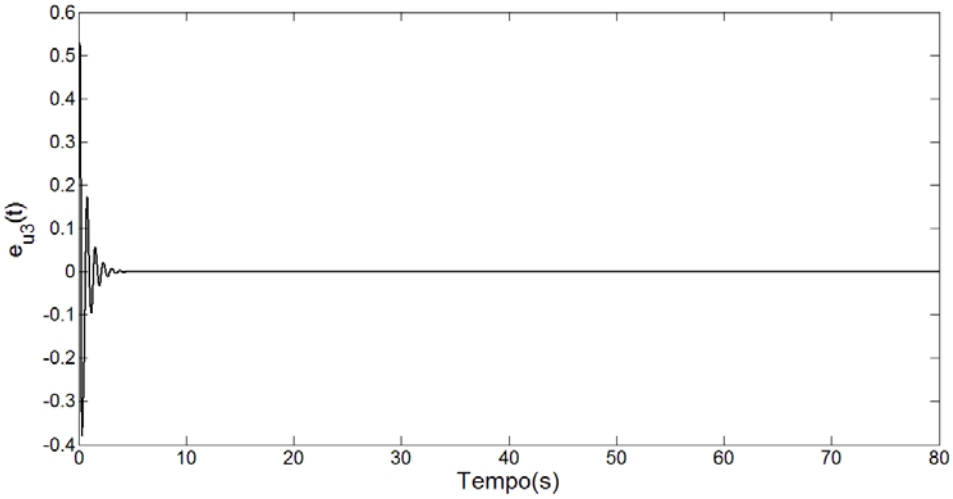


Figura 4.14. Erro de sincronização $(x_{mu3} - x_{su3})$ de (C-D).

Após comprovar a estabilidade dos algoritmos de sincronização, considera-se agora a presença de distúrbios nos sistemas (A), (B), (C) e (D). Desta forma utilizou-se

$$d(x_s, t) = \begin{bmatrix} 0.3 * x_{s1}(t) \\ 0.1 * x_{s2}(t) \\ 0.1 * x_{s3}(t) \end{bmatrix} \quad \text{e} \quad d_{su}(\boldsymbol{x}_{su}, t) = \begin{bmatrix} -0.01 * x_{su1}(t) \\ +0.01 * x_{su2}(t) \\ -0.01 * x_{su3}(t) \end{bmatrix}. \tag{4.42}$$

As Figuras 4.15 a 4.17 e 4.21 a 4.23 mostram o desempenho da sincronização dos sistemas principais e auxiliares (A)-(B) e (C)-(D). Já as Figuras 4.18 a 4.20 e 4.24 a 4.26 mostram os erros de sincronização dos sistemas mestre escravo (A)-(B) e (C)-(D). Utilizou-se uma escala logarítmica para mostrar o rápido transiente alcançado. Pode-se observar que as simulações confirmam os dados teóricos. Observa-se que a sincronização total do sistema A levou 0.578s e a do sistema C 2,486s considerando que o sistema só está sincronizado quando o erro de sincronização entra na faixa de $\pm 0{,}05$.

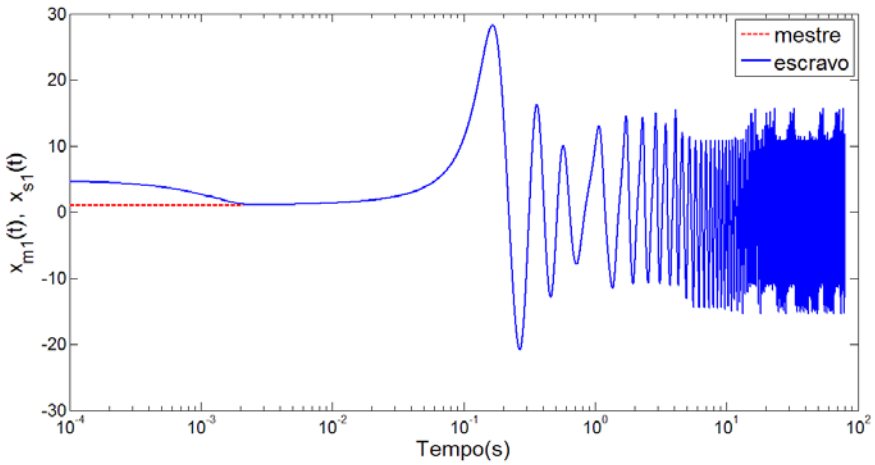


Figura 4.15. Desempenho da sincronização de x_{s1} (A-B) com distúrbios.

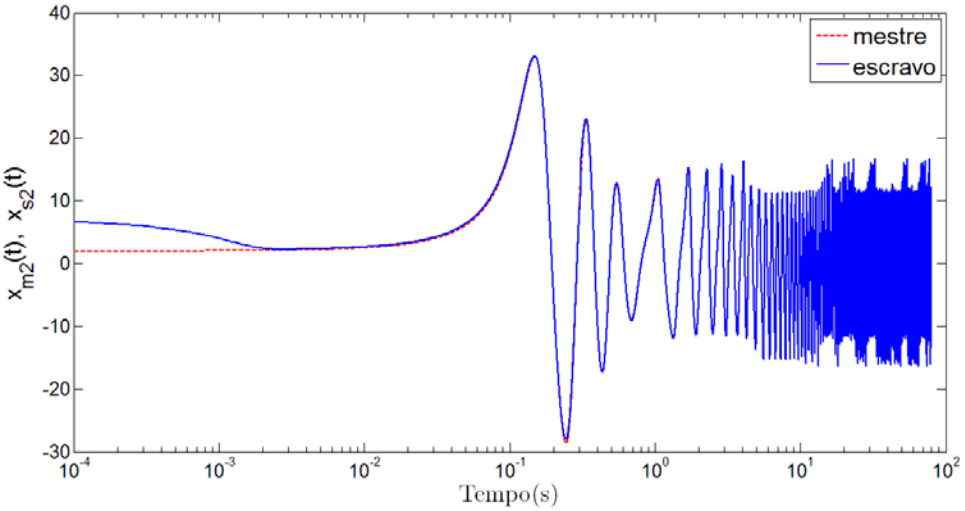


Figura 4.16. Desempenho da sincronização de x_{s2} (A-B) com distúrbios.

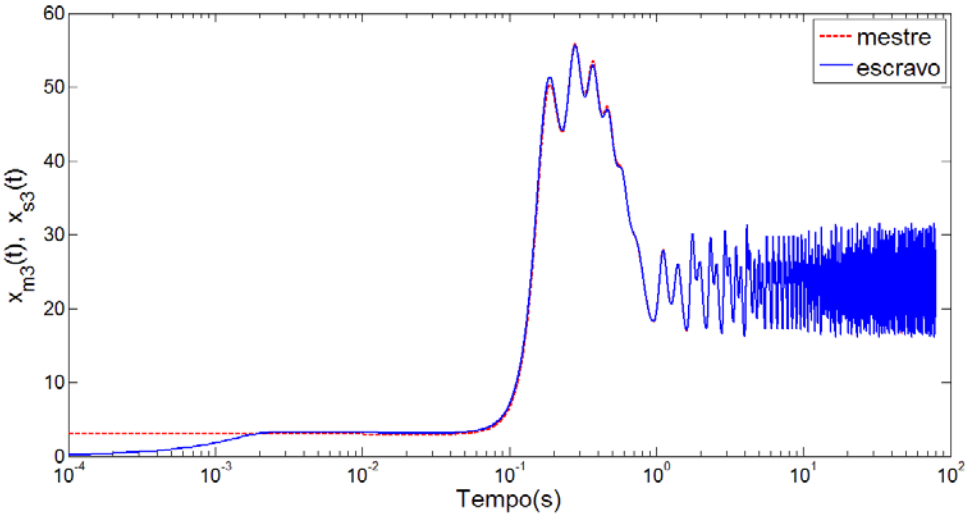


Figura 4.17. Desempenho da sincronização de x_{s3} (A-B) com distúrbios.

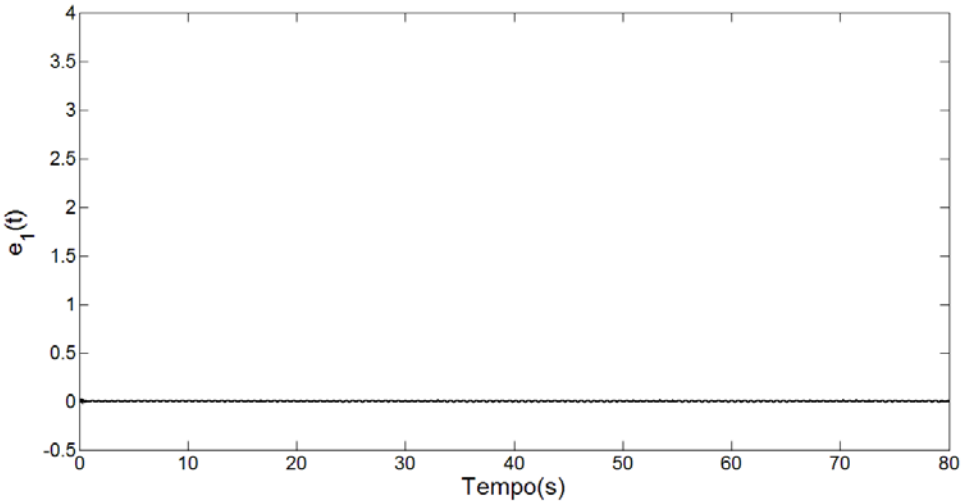


Figura 4.18. Erro de sincronização $(x_{m1} - x_{s1})$ de (A-B).

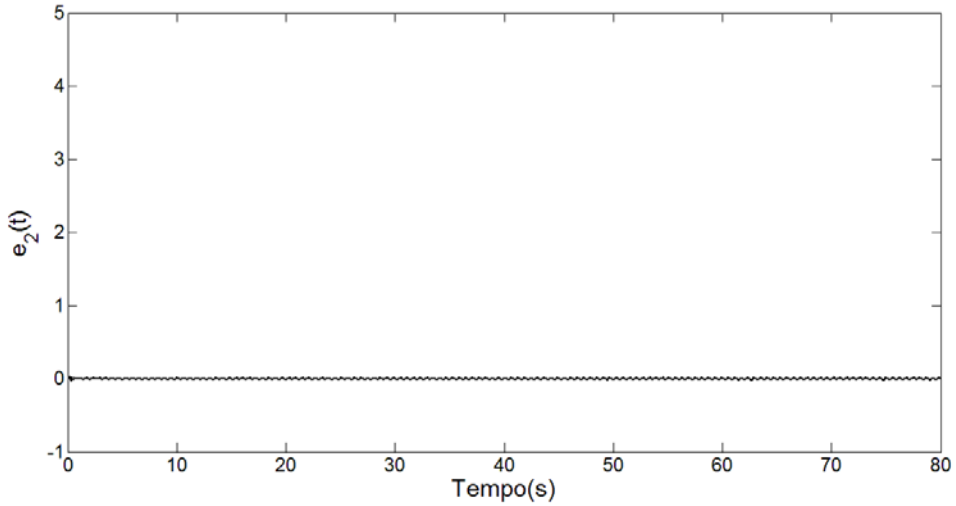


Figura 4.19. Erro de sincronização $(x_{m2} - x_{s2})$ de (A-B).

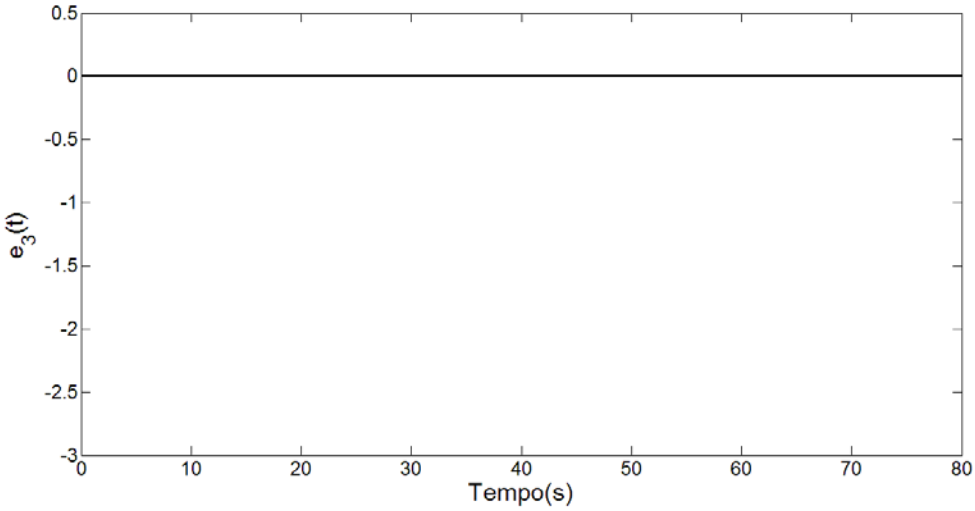


Figura 4.20. Erro de sincronização $(x_{m3} - x_{s3})$ de (A-B).

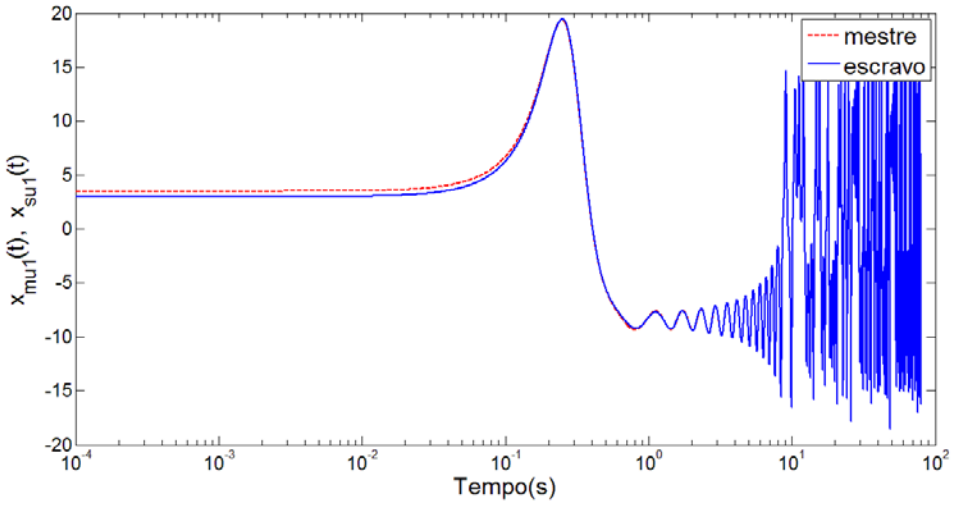


Figura 4.21. Desempenho da sincronização de x_{su1} (C-D) com distúrbios.

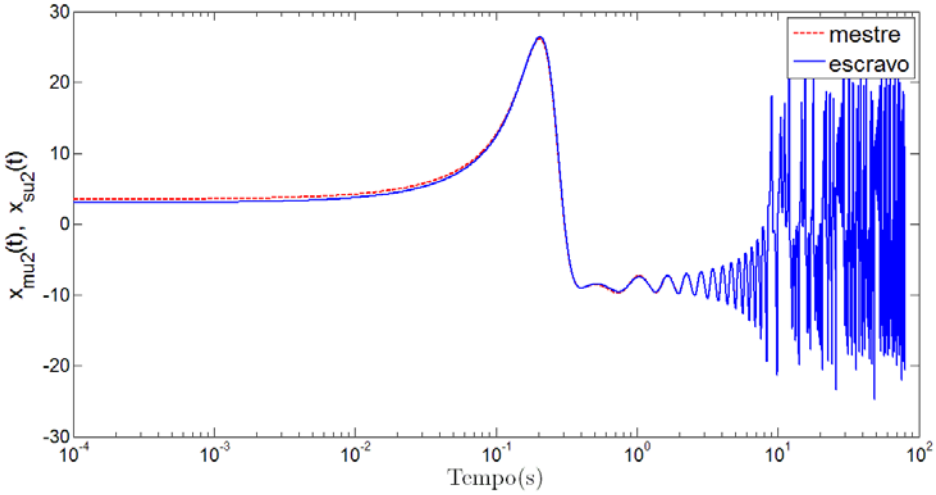


Figura 4.22. Desempenho da sincronização de x_{su2} (C-D) com distúrbios.

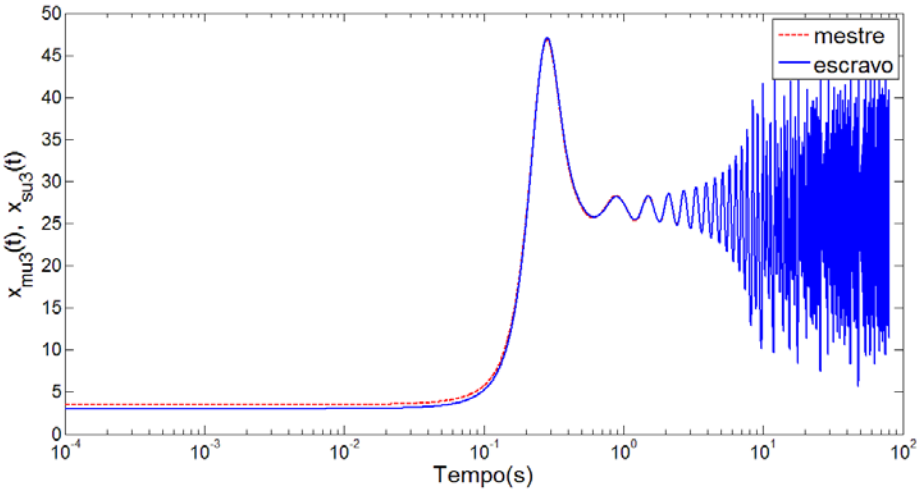


Figura 4.23. Desempenho da sincronização de x_{su3} (C-D) com distúrbios.

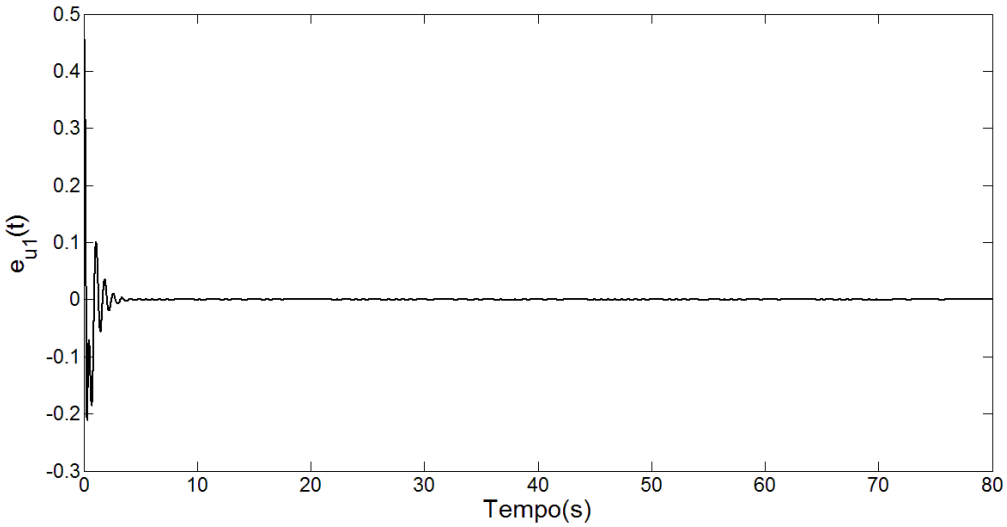


Figura 4.24. Erro de sincronização $(x_{mu1} - x_{su1})$ de (C-D).

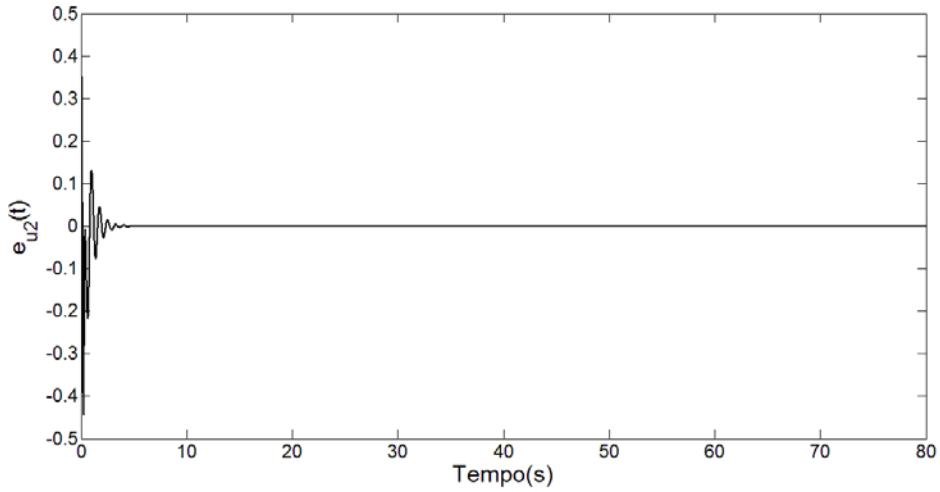


Figura 4.25. Erro de sincronização $(x_{mu2} - x_{su2})$ de (C-D).

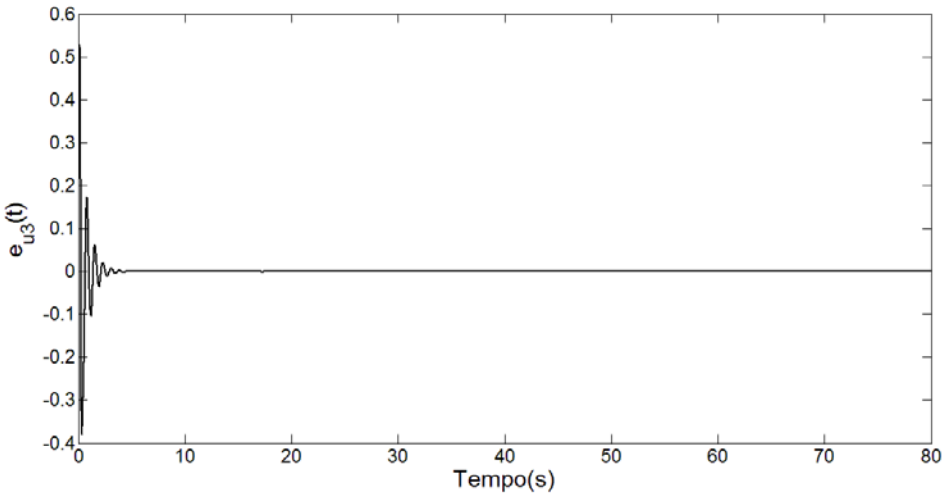


Figura 4.26. Erro de sincronização $(x_{mu3} - x_{su3})$ de (C-D).

Após comprovar a estabilidade dos algoritmos de sincronização dos sistemas principais e secundários na presença de distúrbios, na próxima seção será feito um estudo comparativo do esquema proposto com aqueles apresentados no capítulo 3.

4.5.2 Segundo experimento

Para confirmar a transmissão da mensagem e sua decriptação, inicialmente realizou-se a codificação da imagem digital Lena que possui 4096 pixels (64x64) em uma sequência binária de 32768 *bits*. A imagem codificada foi introduzida no sistema caótico (A) seguindo os métodos propostos na seção 4.3. Os quatro sistemas caóticos unificados foram considerados sujeitos a distúrbios da forma (4.42). Recuperou-se a imagem com a

utilização de um filtro. A imagem recuperada, já reconstruída, é reproduzida na figura 4.27.

Figura 4.27. Imagem digital Lena reconstruída (esquerda) ao lado da original.

Nota-se que a imagem digital Lena reconstruída é perfeitamente igual à enviada. Caso o sinal enviado pelo canal público fosse interceptado, a imagem recuperada (utilizando os mesmo artifícios que foram utilizados na reconstrução da imagem perfeita) seria irreconhecível, vide a Figura 4.28.

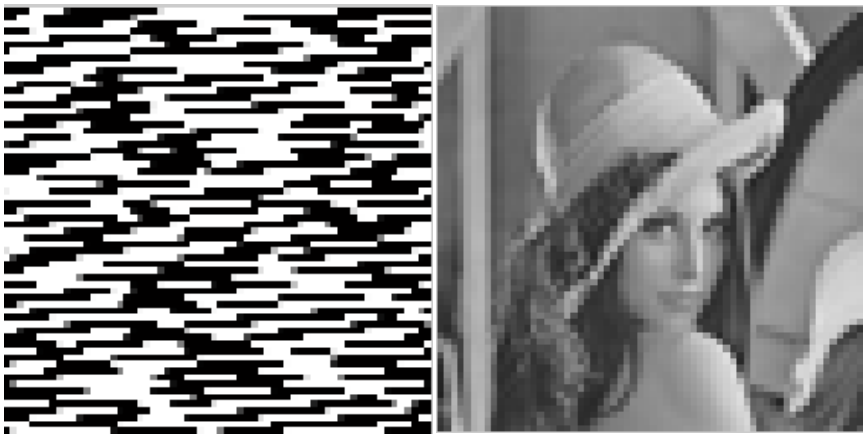


Figura 4.28. Imagem digital visualizada no canal público (esquerda) ao lado da original.

Como proposto pelo esquema de comunicação com segurança, dois dos sinais disponíveis no canal público são encriptados. As Figuras 4.29 e 4.30 representam os sinais de x_{e2} e x_{e3}. Em comparação com as figuras 4.16 e 4.17 devem ser notadas as diferenças entre os sinais originais x_{m2} e x_{m3} e suas encriptações.

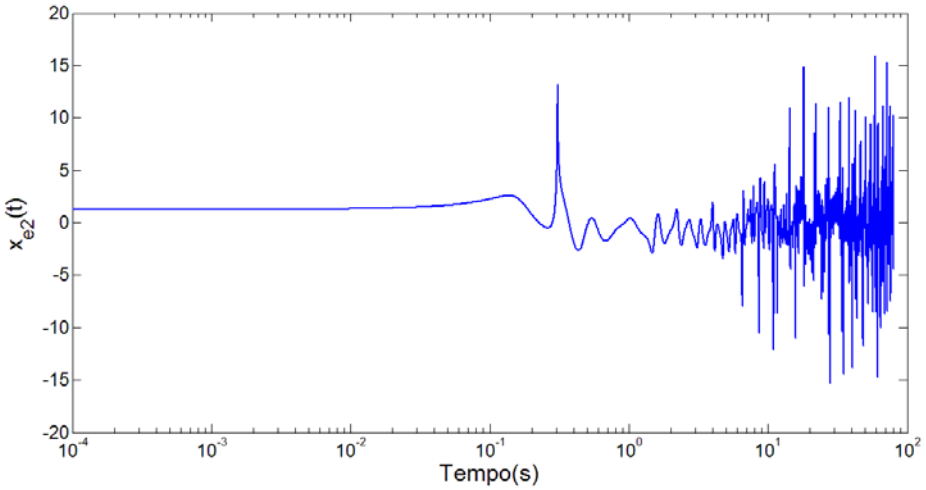


Figura 4.29. Sinal encriptado x_{e2} (x_{m2} encriptado).

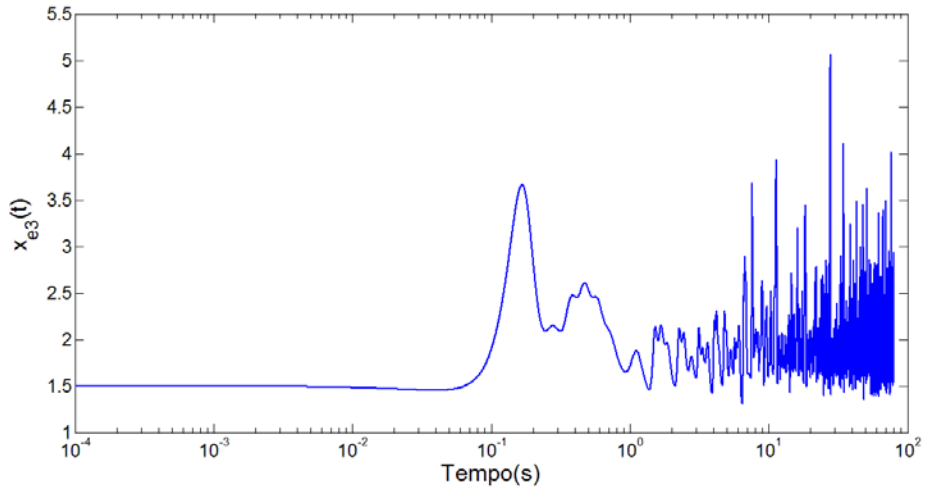


Figura 4.30. Sinal encriptado x_{e3} (x_{m3} encriptado).

A fim de se provar a segurança do esquema, simulou-se a obtenção da mensagem por alguém que teria conhecimento estrutural do esquema e seus sistemas, mas que não tivesse conhecimento integral das fórmulas expressas pelas equações (4.37), (4.40) e (4.41). Desta forma, foram obtidas duas imagens, vide Figuras 4.31 e 4.32. A primeira representa como seria a imagem recuperada quando há conhecimento integro de α_p mas desconhecimento parcial das fórmulas de decriptação, i.e., há o conhecimento da estrutura, mas não dos parâmetros. A segunda representa exatamente o contrário. Considerando a utilização de

$$x_{d2} = x_{e2}(|x_{mu2}| + 10) - 2x_{mu2} \tag{4.43}$$

$$x_{d3} = x_{e3}(|x_{mu3}| + 10) - 2x_{mu3} \tag{4.44}$$

como as fórmulas de decriptação, obtém-se como resultado a imagem exposta na Figura 4.31.

Figura 4.31. Imagem digital recuperada com conhecimento de α_p (esquerda) ao lado da original.

Considerando a utilização de

$$\alpha_p = \frac{|x_{m1}|+25}{27(|x_{m1}|+1)} \tag{4.45}$$

como a fórmula para reconstrução do α_p, obtém-se como resultado a imagem exposta na Figura 4.32.

Figura 4.32. Imagem digital recuperada com conhecimento das fórmulas de decriptação (esquerda) ao lado da original.

Nota-se que as imagens obtidas acima em nada remetem a imagem original, portanto pode-se dizer que, respeitando as considerações feitas neste capítulo, o esquema proposto é seguro e permite que a imagem seja reconstruída com perfeição apenas nos casos onde o receptor tem total conhecimento do esquema e dos sistemas que o compõe.

Apesar da presença de distúrbios e nos dois conjuntos de sistemas mestre-escravo e do desconhecimento de parâmetros nos sistemas (A-B), o sistema sincronizou mais rapidamente que nos dois esquemas de segurança estudados no capítulo 3. Deve-se

notar que como a mensagem é inserida no sistema (A), é a sincronização adaptativa a responsável por reproduzir este acréscimo no sistema (B). Considerando uma transferência de bits, a variação da amplitude da mensagem (múltiplos de 0 e 1) deverá ser igualada o mais rápido possível pelo sistema escravo. Logo, é a velocidade com que um sistema mestre-escravo sincroniza a responsável por permitir uma maior ou menor taxa de transferência de bits. Para exemplificar, consideraram-se os esquemas estudados no capítulo 3 sem a influência de distúrbios e utilizou-se a mesma sequência de bits utilizada no esquema aqui proposto. Assim, temos

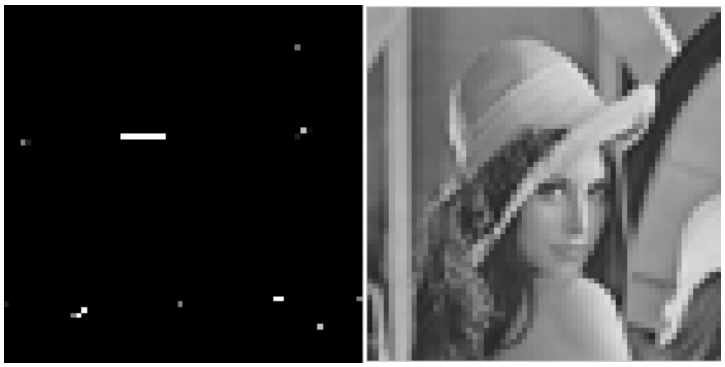


Figura 4.33. Imagem digital recuperada utilizando o esquema analisado na seção 3.2 (esquerda) ao lado da original.

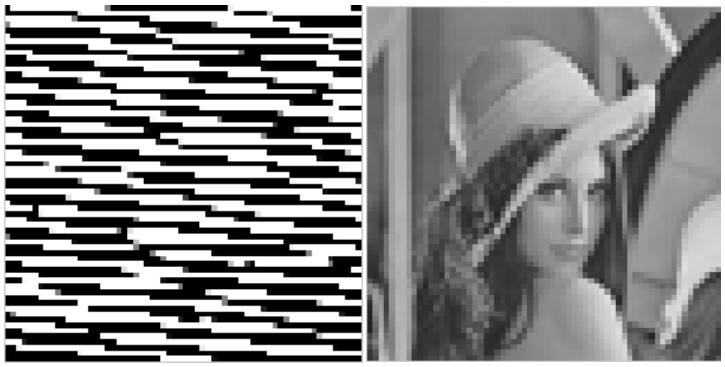


Figura 4.34. Imagem digital recuperada utilizando o esquema analisado na seção 3.3 (esquerda) ao lado da original.

Pela análise das figuras acima, evidenciam-se as falhas do esquema de comunicação analisados nas seções 3.2 e 3.3, quando a mensagem é binária e de alta frequência. Em contraponto, as simulações realizadas neste capítulo demonstram a segurança, estabilidade e robustez do esquema de segurança proposto.

4.6 CONCLUSÃO

Neste capítulo foi proposto um esquema para comunicação com segurança baseado em sincronização adaptativa de sistemas caóticos na presença de parâmetros incertos e distúrbios limitados. Com base na teoria de estabilidade de Lyapunov foi provado que o erro de sincronização converge assintoticamente para zero, mesmo na presença das incertezas mencionadas. Um exemplo de aplicação consistindo da transmissão de uma imagem foi implementado para mostrar a viabilidade do esquema proposto. Além disso, compararam-se os resultados obtidos com aqueles do capítulo 3, de forma a evidenciar os fatores positivos do esquema proposto.

CAPÍTULO 5

CONCLUSÃO

No presente trabalho, objetivando-se o controle de sistemas caóticos e a criação de um esquema de segurança eficiente, foi estudado um esquema de sincronização caótica adaptativa associada a um esquema de sincronização caótica por sinal comum.

Inicialmente, no capítulo 2, foram introduzidos conceitos e definições primordiais para o estudo de sistemas caóticos, sua sincronização e esquemas de comunicação com segurança.

Na sequência, no capítulo 3, os conceitos apresentados foram utilizados para analisar o comportamento dinâmico do sistema caótico unificado quando seu parâmetro principal é alterado. Para melhor compreensão de suas propriedades, foram realizadas simulações de modo a obter seus atratores. A escolha deste sistema se deve a sua relevância para a literatura, já que este com o alterar de um parâmetro pode se comportar como os sistemas Lorenz, Lü ou Chen. Em seguida foram analisados e simulados dois esquemas de comunicação com segurança baseados em sincronização caótica.

No capítulo 4, propôs-se um esquema de comunicação com segurança que considera a presença de distúrbios e a incerteza de parâmetro. O esquema foi comparado aos estudados no capítulo 3 de forma a se evidenciar a sincronização mais rápida e aumento de segurança na transferência da mensagem. Utilizou-se nesse esquema um algoritmo adaptativo projetado no contexto da teoria de estabilidade de Lyapunov. Para evidenciar as características de segurança, codificou-se uma imagem digital de 64x64 *pixels* em uma sequência de *bits* e esta foi transmitida via sinal analógico (degrau).

O presente trabalho contribuiu com a apresentação de um esquema de segurança que, mesmo afetado por incerteza de parâmetro e distúrbios limitados, consegue mascarar, transmitir e recuperar uma imagem transmitida por uma sequencia de bits. A abordagem de considerar incertezas e distúrbios torna o esquema mais realista, uma vez que estes são inerentes na construção de circuitos. Tal contribuição pode ser relevante para criptografar sinais em sistemas de telecomunicação. Para embasar o estudo, simulações

exaustivas foram implementadas para comprovar a transferência correta da imagem, a sincronização dos sistemas e comparar o estudo proposto com os estudos analisados.

Como sugestão para trabalhos futuros menciona-se as seguintes:

Sugestão 5.1: Foi assumido neste trabalho o conhecimento do limitante superior dos distúrbios. Um estudo mais realista poderia considerar desconhecido este limitante.

Sugestão 5.2: Em trabalhos futuros devem-se usar métodos mais avançados de criptografia associada à sincronização tendo em vista que novos algoritmos de quebra de segurança estão sempre em desenvolvimento.

Sugestão 5.3: O envio dos três sinais durante toda a sincronização, estados do sistema caótico generalizado, pode ocupar uma larga banda de transmissão. Sugere-se o estudo de modo de sincronização por impulsos, pois este poderia diminuir a banda de transmissão dos sinais para sincronização. Para maiores detalhes vide [40].

REFERÊNCIAS BIBLIOGRÁFICAS

[1] STROGATZ, S. H. **Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry and Engineering.** 1ª Edição. Ed. Westview Press, 2001.

[2] OTT, E., GREBOGI, C. e YORKE, J. A. Controlling Chaos. **Physical Review Letters:** v.64, n.11 p.1196-1199, 1990.

[3] PECORA, L. M. e CARROLL, T. L. Synchronization in Chaotic Systems. **Physical Review Letters:** v.64, n.8, p821-825 1990.

[4] CUOMO, K. M. e OPPENHEIM, A. V. E STROGATZ, S. H. Synchronization of Lorenz-based chaotic circuits with applications to communication. **IEEE Transactions On Circuits and Systems – II: Analog and Digital Signal Processing:** v.40, n.10, p.626-632,1993.

[5] DEDIEU, H., KENNEDY, M. P. e HASLER, M. Chaos Shift Keying: modulation and demodulation of chaotic carrier using self-synchronizing Chua's circuits. **IEEE Transactions On Circuits and Systems – II: Analog and Digital Signal Processing:** v.40, n.10, p.634-642,1993.

[6] CHUA, L. O. e YANG, T. Secure Communication via Chaotic Parameter Modulation. **IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications:** v.43, n.9, p.817-819, 1996.

[7] CHUA, L. O. e WU, C. W. A Simple Way to Synchronize Chaotic Systems With Applications to Secure Communications Systems. **International Journal of bifurcation and Chaos:** v.3, n.6, p.1619-1627, 1993.

[8] CHUA, L. O., YANG, T. e WU, C. W. A. Cryptography Based on Chaotic Systems. **IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications:** v.44, n.5, p.469-472, 1997.

[9] HOU, Y., LIAU, B. e CHEN, H. Synchronization of Unified Chaotic Systems Using Sliding Mode Controller. **Mathematical Problems in Engineering** v.2012, p.10-17, 2012.

[10] SMAOUI N., KAROUMA, A e ZRIBI, M. Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems. **Communications in Nonlinear Science and Numerical Simulation:** n.16, p.3279-3293, 2011.

[11] WANG, M., WANG, X. e PEI, B. A new digital communication scheme based on chaotic modulation. **Nonlinear Dynamics:** n.67, p.1097-1104, 2012.

[12] LI, K., ZHAO, M. e FU, X. Projective Synchronization of Driving-Response Systems and Its Application to Secure Communications. **IEEE Transactions on Circuits and Systems – I: Regular Papers:** v.56, n.10, p.2280-2291, 2009.

[13] KHALIL, H. **Nonlinear Systems.** 3ª Edição. New Jersey: Ed. Prentice-Hall, Inc, 2001.

[14] SLOTINE, J. J. E. e LI, W. **Applied Nonlinear Control.** 1ª Edição. New Jersey, Ed. Prentice-Hall, Inc, 1991.

[15] LI, T. e YORKE, J. A. Period Three Implies Chaos. **The American Mathematical Monthly:** v.82, n.10, p.985-992, 1975.

[16] GLEICK, J. **Chaos: Making New Science**. New York, NY. Ed. Penguin Books, 1987.

[17] MARTELLI, M., DANG, M. e SEPH, T. Defining Chaos. **Mathematics Magazine:** v.71, n.2, p.112-122, 1998.

[18] KINZEL, W., ENGLERT, A. e KANTER, I. On Chaos Synchronization and Secure Communication. **Philosophical Transactions of The Royal Society:** n.368, p.379-389, 2010.

[19] CUOMO, K. M. e OPPENHEIM, A. V. Circuit Implementation of Synchronized Chaos with Applications to Communications. **Physical Review Letters:** v.71, n.1, p.65-68, 1993.

[20] OGORZALEK, M. J. Taming Chaos – Part I: Synchronization. **IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications:** v.40, n.10, p.693-699,1993.

[21] RULKOV, N. F., SUSHCHIK, M. M. e TSIMRING, L. S. Generalized synchronization of chaos in directionally coupled chaotic systems. **Physical Review Letters:** v.51, n.2, p.980-994,1995.

[22] PIKOVSKY, M. ROSENBLUM, M. e KURTHS, J. **Synchronization: A universal concept in non-linear sciences.** Cambridge Nonlinear Science Series, Cambridge University Press, Cambridge, 2003.

[23] KOCAREV, L. e PARLITZ, U. Generalized Synchronization, Predictability, and Equivalence of Unidirectionally Coupled Dynamical Systems. **Physical Review Letters:** v.76, n.11, p.1816-1819, 1996.

[24] PIKOVSKY, M. ROSENBLUM, M. e KURTHS, J. Phase Synchronization of Chaotic Oscillators. **Physical Review Letters:** v.76, n.11, p.1804-1807, 1996.

[25] OSIPOV, G. V., PIKOVSKY, A. S., ROSENBLUM, M. G. e KURTHS, J. Phase synchronization effects in a lattice on nonidentical Rössler oscillators. **Physical Review Letters:** v.55, n.3, p.2353-2361, 1997.

[26] PECORA, L. M., CARROLL, T. L. e HEAGY, J. F. Statistics for mathematical properties of maps between time series embeddings. **Physical Review Letters:** v.52, n.4, p.3420-3439, 1995.

[27] PAZÓ, D., ZAKS, M. A. e KURTHS, J. Role of unstable periodic orbits in phase and lag synchronization between coupled chaotic oscillators. **Chaos – An Interdisciplinary Journal of Nonlinear Science:** v.13, n.309, p.309-318, 2003.

[28] Li, X., LEUNG, A. C., LIU, X., HAN, X. e CHU, Y. Adaptive synchronization of identical chaotic and hyper-chaotic systems with uncertain parameters. **Nonlinear Analysis: Real World Applications:** v.11, p.2215-2223, 2010.

[29] LORENZ, E. N. Deterministic Nonperiodic Flow. **Journal of the Atmospheric Sciences:** v.20, p.130-141, 1963.

[30] CHEN, G. e UETA, T. Yet Another Chaotic Attractor. **International Journal of Bifurcation and Chaos:** v.9, n.7, p.1465-1466, 1999.

[31] LÜ, J. e CHEN, G. A new chaotic attractor coined. **International Journal of Bifurcation and Chaos:** v.12, n.3, p.659-661, 2002.

[32] LÜ, J., CHEN, G., CHENG, D. e CELIKOVSKY, S. Bridge the gap between the Lorenz system and the chen system. **International Journal of Bifurcation and Chaos:** v.12, n.12, p.2917-2926, 2002.

[33] KANSO, A. e GHEBLEH, M. A novel image encryption algorithm base on a 3D chaotic map. **Communications in Nonlinear Sciences and numerical Simulation:** n.17, p.2943-2959, 2012.

[34] MATA-MACHUCA, J. L., MARTINEZ-GUERRA, R., AGUILAR-LOPEZ, R. e AGUILAR-IBANEZ, C. A chaotic system in synchronization and secure communications. **Communications in Nonlinear Science and Numerical Simulation:** n.17, p.1706-1713, 2011.

[35] QUN DING, J. e DU, B. A new improved scheme of chaotic masking secure communication based on Lorenz system. **International Journal of Bifurctaion and Chaos:** v.22, v.5., p.347-357, 2012.

[36] XIAOHONG, H. e XIAOMING, C. A chaotic digital secure communication based on a modified gravitational search algorithm filter. **Information Sciences:** n.208, p.14-27, 2012.

[37] WANG, X. e ZHU, L. Adaptive Full State Hybrid Projective Synchronization of Unified Chaotic Systems with Unknown Parameteres. **International Journal of Modern Physics B: Condensed Matter Physics; Statistical Physics; Applied Physics:** v.25, n.32, p4661-4666, 2011.

[38] CHENG, C. e CHENG, C. An asymmetric image cryptosystem based on the adaptive synchronization of na uncertain unified chaotic system and a cellular neural network. **Communications in Nonlinear Science and Numerical Simulation:** v.18, n.10. p.2825-2837, 2013.

[39] LIANG, H., WANG, Z e YUE, Z. Generalized synchronization and control for incommensurate fractional unified chaotic system and applications in secure communication. **Kybernetika:** v.48, n.2, p.190-205, 2012.

[40] YANG, T. **Impulsive Control Theory**. Berlin: Spinger-Verlag, 2001.

ANEXOS

Anexo 1 – Código fonte para a obtenção das Figuras 3.1-3.4.

Anexo 2 – Código fonte do controlador proposto em [7].

Anexo 3 – Código fonte do controlador proposto em [9].

Anexo 4 – Código fonte para obtenção das Figuras 3.6-3.12, 3.14-3.20.

Anexo 5 – Código fonte do controlador proposto neste trabalho.

Anexo 6 – Código fonte para obtenção das Figuras 4.3-4.26 e 4.29-4.30.

Anexo 7 – Funções utilizadas na obtenção das Figuras 4.27-4.28 e 4.31-4.34.

Anexo 8 – Código fonte para obtenção das Figuras 4.27-4.28 e 4.31-4.34.

```
function Mapeador = Mapeador ()
    lor_system = inline('[((25*1.5)+10)*(x(2)-x(1));(28-35*1.5)*x(1)-
x(1)*x(3)+(29*1.5-1)*x(2); x(1)*x(2)-((1.5+8)/3)*x(3)]', 't', 'x');
    options = odeset('RelTol', 1e-4, 'AbsTol', 1e-4);
    [t, xa]  = ode45(lor_system, [0,500],[15,10,10],options);
    plot3(xa(:,3),xa(:,1),xa(:,2))

    fsize=15;
    title('Atrator Com alfa = 5', 'Fontsize', fsize)
    zlabel('z(t)','Fontsize',fsize);
    xlabel('x(t)','Fontsize',fsize);
    ylabel('y(t)','Fontsize',fsize);
```

```
function [sys,x0,str,ts] = chuacap3(t,x,u,flag)

switch flag,

   %%%%%%%%%%%%%%%%%
   % Initializacao %
   %%%%%%%%%%%%%%%%%
case 0,
    sizes = simsizes;
    sizes.NumContStates  = 6;
    sizes.NumDiscStates  = 0;
    sizes.NumOutputs     = 10;
    sizes.NumInputs      = 0;
    sizes.DirFeedthrough = 0;
    sizes.NumSampleTimes = 1;
    sys = simsizes(sizes);
    x0 = [1; 2; 3; 5; 7; 0];       %verificar condições iniciais
    str=[];
    ts=[0 0];
   %%%%%%%%%%%%
   % Derivadas%
   %%%%%%%%%%%%
case 1,
    sys = [((25*alfa(t,x,u))+10)*(x(2)-x(1));
            28*(x(1)+D(t,x,u))-35*alfa(t,x,u)*x(1)-
(x(1)+D(t,x,u))*x(3)+(29*alfa(t,x,u)-1)*x(2);
            (x(1)+D(t,x,u))*x(2)-((alfa(t,x,u)+8)/3)*x(3);
            ((25*alfa(t,x,u))+10)*(x(5)-x(4));
            28*(x(1)+D(t,x,u))-35*alfa(t,x,u)*x(4)-
(x(1)+D(t,x,u))*x(6)+(29*alfa(t,x,u)-1)*x(5);
            (x(1)+D(t,x,u))*x(5)-((alfa(t,x,u)+8)/3)*x(6)];

   %%%%%%%%%%
   % Saidas %
   %%%%%%%%%%
case 3,
   sys = [x(1);x(2);x(3);x(4);x(5);x(6);x(4)-x(1);x(5)-x(2);x(6)-x(3);
D(t,x,u)+x(1)-x(4)];

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

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

    %%%%%%%% Alfa %%%%%%%%%%
function alfa = alfa(t,x,u)
    alfa = 0.02;

function D = D(t,x,u)

%%% Mensagem utilizada no capitulo 3 %%%
    D=0.01*sin(3.1415*t);
```

```
%%% Mensagem utilizada para obter imagem Lena%%%
    global recebe;

    g=0.002;
    h=10;
    i=bit(t,x,u);

    if (t<h);
        D = 0;
    elseif (t>=(h+bit(t,x,u)*g)) && (t<(h+(bit(t,x,u)+1)*g)) &&
(t<75.536);
        D = 0.5*recebe(i+1);
    else (t>(h+32768*g));
        D = 0;
    end

function bit=bit(t,x,u)
    bit = floor((t-10)*500);
```

```
function [sys,x0,str,ts] = deslizante(t,x,u,flag)
        B=2;
        n=2;
        k=5;
        a=0.001;

switch flag,

   %%%%%%%%%%%%%%%%%
   % Initializacao %
   %%%%%%%%%%%%%%%%%
case 0,
    sizes = simsizes;
    sizes.NumContStates  = 7;
    sizes.NumDiscStates  = 0;
    sizes.NumOutputs     = 10;
    sizes.NumInputs      = 0;
    sizes.DirFeedthrough = 0;
    sizes.NumSampleTimes = 1;
    sys = simsizes(sizes);
    x0 = [1; 2; 3; 5; 7; 0; -2];       %verificar condições iniciais
    str=[];
    ts=[0 0];
   %%%%%%%%%%%%%
   % Derivadas %
   %%%%%%%%%%%%%
case 1,
    sys = [((25*alfa(t,x,u))+10)*(x(2)-x(1));
           (28-35*alfa(t,x,u))*x(1)-x(1)*x(3)+(29*alfa(t,x,u)-
1)*x(2)+D(t,x,u);
           x(1)*x(2)-((alfa(t,x,u)+8)/3)*x(3);
           ((25*alfa(t,x,u))+10)*(x(5)-x(4));
           (28-35*alfa(t,x,u))*x(4)-x(1)*x(6)+(29*alfa(t,x,u)-
1)*x(5)+controlador(t,x,u);
           x(1)*x(5)-((alfa(t,x,u)+8)/3)*x(6);
           D(t,x,u)-n*k*(x(7)/(abs(x(7))+a))];
   %%%%%%%%%%
   % Saidas %
   %%%%%%%%%%
case 3,
   sys = [x(1);x(2);x(3);x(4);x(5);x(6);x(1)-x(4);x(2)-x(5);x(3)-x(6);
controlador(t,x,u)];

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

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

    %%%%%%%% Alfa %%%%%%%%%%

function alfa = alfa(t,x,u)

 alfa = 0;
```

```
function D = D(t,x,u)

    %%% Mensagem utilizada na simulaçao do capitulo 3 %%%
    D=0.5*sin(5*t);

    %%% Mensagem para obtenção da Lena %%%
    global recebe;

    g=0.002;
    h=10;
    i=bit(t,x,u);

    if (t<h);
        D = 0;
    elseif (t>=(h+bit(t,x,u)*g)) && (t<(h+(bit(t,x,u)+1)*g)) &&
(t<75.536);
        D = 0.5*recebe(i+1);
    else (t>(h+32768*g));
        D = 0;
    end

function bit=bit(t,x,u)
    bit = floor((t-10)*500);

    function controlador = controlador (t,x,u)
        B=2;
        n=2;
        k=5;
        a=0.001;
        controlador = (38+10*alfa(t,x,u))*(x(1)-x(4))+(29*alfa(t,x,u)-
1+B)*(x(2)-x(5))+n*k*(x(7)/(abs(x(7))+a));
```

```
fsize=22;
set(0,'DefaultAxesColorOrder',[0 0 0]);

figure;
plot(tout, yout(:,7) , 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('e_{1}(t)','Fontsize',fsize);

figure;
plot(tout, yout(:,8), 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('e_{2}(t)','Fontsize',fsize);

figure;
plot(tout, yout(:,9), 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('e_{3}(t)','Fontsize',fsize);

figure;
plot(tout, yout(:,10), 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('sinal de mensagem recuperado','Fontsize',fsize);

figure;
semilogx(tout, yout(:,1), '--r',tout, yout(:,4), 'b','LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','interpreter','latex','Fontsize',fsize);
ylabel('x_{m1}(t),  x_{s1}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,2), '--r',tout, yout(:,5), 'b','LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{m2}(t),  x_{s2}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,3), '--r',tout, yout(:,6), 'b','LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{m3}(t),  x_{s3}(t)','Fontsize',fsize);
```

```
function [sys,x0,str,ts] = Principal2(t,x,u,flag)
    A = [-25 25 0; -35 29 0; 0  0 -1/3];
    B = [-10 10 0; 28 -1 0; 0 0 -8/3];
    P = [0.0001 0 0; 0 10 0; 0 0 5];
    K=P+P';
    y2=20;
    yb=0.05;

switch flag,
   %%%%%%%%%%%%%%%%%
   % Initializacao %
   %%%%%%%%%%%%%%%%%
case 0,
    sizes = simsizes;
    sizes.NumContStates  = 13;
    sizes.NumDiscStates  = 0;
    sizes.NumOutputs     = 26;
    sizes.NumInputs      = 0;
    sizes.DirFeedthrough = 0;
    sizes.NumSampleTimes = 1;
    sys = simsizes(sizes);
    x0 = [1; 2; 3; 5; 7; 0; 0.8; 3; 3; 3; 3.5; 3.5; 3.5];
%verificar condições iniciais
    str=[];
    ts=[0 0];
   %%%%%%%%%%%%%
   % Derivadas %
   %%%%%%%%%%%%%
case 1,
    sys = [Fm(t,x,u) + (alfa(t,x,u)*A+B)*Gm(t,x,u) + delta_f(t,x,u);
           Fs(t,x,u) + (x(7)*A+B)*Gs(t,x,u) + controlador(t,x,u);
           -
yb*(y2*norm(erro(t,x,u))*(x(7)))+(erro1(t,x,u))*(0.0001*K*A*[x(1);
yd1(t,x,u); zd1(t,x,u)]);
           ((25*alfa2(t,x,u))+10)*(x(9)-x(8)-0.01*x(8));
            (28-35*alfa2(t,x,u))*x(8)-x(8)*x(10)+(29*alfa2(t,x,u)-
1)*x(9)+0.01*x(9);
            x(8)*x(9)-((alfa2(t,x,u)+8)/3)*x(10)-0.01*x(10);
            ((25*alfa3(t,x,u))+10)*(x(12)-x(11));
            (28-35*alfa3(t,x,u))*x(8)-x(8)*x(13)+(29*alfa2(t,x,u)-
1)*x(12);
            x(8)*x(12)-((alfa3(t,x,u)+8)/3)*x(13)];
   %%%%%%%%%%
   % Saidas %
   %%%%%%%%%%
case 3,
   sys = [x(1);x(2);x(3);x(4);x(5);x(6);x(4)-x(1); x(5)-x(2);x(6)-
x(3);x(7); alfa(t,x,u); D(t,x,u); x(5)-yd1(t,x,u); x(6)-zd1(t,x,u);
xe1(t,x,u); ye1(t,x,u); ze1(t,x,u); x(11)-x(8); x(12)-x(9); x(13)-x(10);
x(8); x(9); x(10); x(11); x(12); x(13)];
   %%%%%%%%%%
   % Encerra %
   %%%%%%%%%%
case {2,4,9},
    sys = [];

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

```
function alfa = alfa(t,x,u)
    alfa = 1;

function alfa2 = alfa2(t,x,u)
    alfa2 = abs(x(1))/(29*((abs(x(1))+1)));

function alfa3 = alfa3(t,x,u)
    %%% Se houver conhecimento da fórmula %%%
    alfa3 = abs(x(1))/(29*((abs(x(1))+1)));

    %%% Se não houver conhecimento da fórmula %%%
    alfa3 = abs(x(1))+25/(27*((abs(x(1))+1)));

function Fm = Fm(t,x,u)
    Fm = [0; -x(1)*x(3); x(1)*x(2)];

function Gm = Gm(t,x,u)
    Gm = [x(1); x(2); x(3)];

function Fs = Fs(t,x,u)
    Fs = [0; -x(4)*x(6); x(4)*x(5)];

function Gs = Gs(t,x,u)
    Gs = [x(4); x(5); x(6)];

function delta_f = delta_f(t,x,u)%Distúrbio utilizado%
    delta_f = [0.3*x(1); 0.1*x(2); (0.1*x(1))];

    function D = D(t,x,u) %Função para transmitir o bits da imagem Lena%

    global recebe;

    g=0.002;
    h=10;
    i=bit(t,x,u);

    if (t<h);
        D = 0;
    elseif (t>=(h+bit(t,x,u)*g)) && (t<(h+(bit(t,x,u)+1)*g)) &&
(t<75.536);
        D = 0.5*recebe(i+1);
    else (t>(h+32768*g));
        D = 0;
    end

function bit=bit(t,x,u)
    bit = floor((t-10)*500);

function controlador = controlador(t,x,u) % Controle adaptativo%
    k=0.0001;

    lambda0 = 0.01;
    y1 = 1;
    P = 0.0001*[0.0001 0 0 ;0 0.1 0; 0 0 0.05];
    L=[0.1 0 0;
       0 100 0;
       0 0 5];
    K=P+P';
```

```
A = [-25 25 0;
          -35 29 0;
          0  0 -1/3];
    B = [-10 10 0;
          28 -1 0;
          0 0 -8/3];
    lambdaMin = min(eig(K));
    ur = k*erro(t,x,u)/(lambdaMin*(norm(erro(t,x,u))+y1*(exp(-
lambda0*t)+0.2)));
    controlador = -(Fs(t,x,u)-Fm(t,x,u))-B*(erro(t,x,u))-ur-
L*erro(t,x,u)-A*erro(t,x,u)*x(7);

 function erro = erro(t,x,u)
    erro= [x(4)-x(1); x(5)-yd1(t,x,u); x(6)-zd1(t,x,u)];

 function erro1 = erro1(t,x,u)
    erro1= [x(4)-x(1) x(5)-yd1(t,x,u) x(6)-zd1(t,x,u)];

%%%%%%% encriptacao dos sinais transmitidos %%%%%%%%%
function ye1 = ye1(t,x,u)
    ye1 = (x(2)+x(9))/((abs(x(9))+1));

function ze1 = ze1(t,x,u)
    ze1 = ((x(3)+x(10))/((abs(x(10))+1)));

%%%%% Sem encriptaçao %%%%%%
function ye1 = ye1(t,x,u)
    ye1 = x(2);

function ze1 = ze1(t,x,u)
    ze1 = x(3);

%%%%%%% decriptacao dos sinais transmitidos %%%%%%%%%
function yd1 = yd1(t,x,u)
    yd1 = ye1(t,x,u)*(abs(x(12))+1)-x(12);

function zd1 = zd1(t,x,u)
    zd1 = (ze1(t,x,u))*(abs(x(13))+1)-x(13);

%%%%%%%  sem decriptacao %%%%%%%%%
function yd1 = yd1(t,x,u)
    yd1 = ye1(t,x,u);

function zd1 = zd1(t,x,u)
    zd1 = ze1(t,x,u);

%%%% Decriptaçao quando não se tem total conhecimento de sua formula %%%%

function yd1 = yd1(t,x,u)
    yd1 = ye1(t,x,u)*(abs(x(12))+10)-2*x(12);

function zd1 = zd1(t,x,u)
    zd1 = (ze1(t,x,u))*(abs(x(13))+10)-2*x(13);
```

```
fsize=22;
set(0,'DefaultAxesColorOrder',[0 0 0]);

figure;
semilogx(tout, yout(:,16), 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{e2}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,17), 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{e3}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,1), '--r',tout, yout(:,4),'-b', 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{m1}(t),  x_{s1}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,2), '--r',tout, yout(:,5),'-b', 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','interpreter','latex','Fontsize',fsize);
ylabel('x_{m2}(t),  x_{s2}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,3), '--r',tout, yout(:,6),'-b', 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{m3}(t),  x_{s3}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,24), '--r',tout, yout(:,21),'-b', 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{mu1}(t),  x_{su1}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,25), '--r',tout, yout(:,22),'-b', 'LineWidth', 2 );
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','interpreter','latex','Fontsize',fsize);
ylabel('x_{mu2}(t),  x_{su2}(t)','Fontsize',fsize);

figure;
semilogx(tout, yout(:,26), '--r',tout, yout(:,23),'-b', 'LineWidth', 2 );
```

```
set(0,'DefaultAxesFontSize', 17);
h=legend('mestre','escravo');
set(h,'FontSize',fsize);
xlabel('Tempo(s)','Fontsize',fsize);
ylabel('x_{mu3}(t),  x_{su3}(t)','Fontsize',fsize);
```

```
function [A] = jogadecimal(c)    %Função para pegar sequencias de 8 bits%
                                  %transmitidas e colocar na forma de uma%
cont = 1;                        %matriz 64x64 %
cont2 = 1;

for i=1:8:32761
    a = c(i:(i+7));
    b = bi2de(a);
    A(cont2, cont) = b;
    cont = cont+1;
    if cont == 65
        cont =1;
        cont2 = cont2 +1;
    end
end

function [c] = pegabits(A)              %Transforma uma matriz 64x64 com%
                                     %elementos de 8 bits em uma sequencia%
c=[];                                %de 32768 bits %
X=64; %tamanho de um eixo da foto

for i=1:X
    for j=1:X
        a = A(i,j);
        b = de2bi(a,8);
        c = horzcat(c,b);
    end
end

function [b,c]= capta(yo)    %reconstrói a sequencia de bits transmitida%

flag1 = 0;
cont1=0;
cont0=0;
x = 0.00004;
b=zeros(1,3000001);
c=zeros(1,132100);
i=0;

for tempo = 100001:20:799996
    i = i+1;
    presente = yo(tempo+5,15);
    passado = yo((tempo),15);
    if ((passado-presente)>x)
        b(tempo:tempo+19) = [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1];
        c(i)=1;
        flag1=1;
        cont0=0;
    elseif (flag1==1) && ((presente-passado)<x)
        b(tempo:tempo+19) = [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1];
        c(i)=1;
        cont1 = cont1+1;

    elseif ((presente-passado)>x)
        b(tempo:tempo+19) = [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
        c(i)=0;
        flag1=0;
        cont1=0;
```

```
else b(tempo:tempo+19) = [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
        c(i)=0;
        cont0 = cont0+1;
    end
end
```

```
b = imread('lena_rgb_p3.ppm');  %Código a ser digitado na tela principal%
a = rgb2gray(b);                %do matlab onde Lena_rgb.ppm é a figura%
c=imresize(a,0.125);            %original, depois faz-se sua conversão%
global recebe                   %para escala de cinza e 64x64 pixels%
recebe = pegabits (c);          %e então utilizam-se as funções já%
recebe = double(recebe);        %descritas.%
[e f] = capta(yout);
h = uint8 (g);
figure
imshow(h)
```