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

JOSÉ A. R. VARGAS[1], FÁBIO T. VITAL[2]

[1,2]*Universidade de Brasília*
Departamento de Engenharia Elétrica, Caixa postal 4386
70910-900 Campus Universitário Darcy Ribeiro, Brasília, DF, Brasil
E-mails: vargas@unb.br, ft.vital@yahoo.com.br

Abstract— This paper proposes a scheme for secure communication based on adaptive synchronization of unified chaotic systems. The synchronization scheme is based on Lyapunov stability theory to guarantee asymptotic convergence of the synchronization error to zero, even in the presence of bounded disturbances and uncertain parameters. A simulation example is presented to show the application of the proposed scheme.

Keywords— Chaotic systems, synchronization, Lyapunov methods.

Resumo— Neste trabalho é proposto um esquema para comunicação com segurança baseado em sincronização adaptativa de sistemas caóticos unificados. O esquema de sincronização é baseado na teoria de estabilidade de Lyapunov, objetivando-se garantir a 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.

Palavras-chave— Sistemas caóticos, sincronização, métodos de Lyapunov.

1 Introdução

Recentemente vários esquemas para comunicação com segurança baseados em sincronização de sistemas caóticos têm sido propostos na literatura (Kanso and and Ghebleh, 2012, Mata-Machuca, et al, 2011, Qun and Du, 2011, Smaoui, et al, 2011, XiaoHong and XiaoMing, 2012). Nestes esquemas o objetivo básico é mascarar a informação transmitida, de forma que 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 assegura-se a confidencialidade da informação transmitida. Os canais de transmissão típicos incluem, por exemplo, internet, telefonia celular e comunicação por satélite.

Embora, conforme mencionado, existam vários esquemas para a comunicação com segurança na literatura (vide, por exemplo, Mata-Machuca, et al, 2011, Smaoui, et al, 2011, e as referencias neles), a maioria destes esquemas 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, além do ruído associado ao canal de transmissão, são inevitáveis.

Motivado pelos fatos anteriores, neste artigo é proposto 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 cifrado, na ausência de ruído de canal, e a possibilidade de uso de injeção de ruído no sistema mestre como uma chave adicional de segurança, pois este procedimento dificulta a decifração. Para prova de estabilidade e convergência é usada uma análise tipo Lyapunov-like e os resultados são validados através de um estúdio computacional.

2 Formulação do Problema

Considere o sistema caótico unificado descrito pela seguinte equação diferencial

$$\dot{x}_m = (\alpha A + B)x_m + f_m(x_m) + cH(t) \qquad (1)$$

onde $x_m \in \Re^3$ é o estado do sistema mestre, $f_m(.)$ é um mapeamento conhecido, c é uma constante positiva conhecida, $H(t)$ é a mensagem a ser enviada, α é um parâmetro conhecido,

$$A = \begin{bmatrix} -25 & 25 & 0 \\ -35 & 29 & 0 \\ 0 & 0 & -\frac{1}{3} \end{bmatrix} \qquad (2)$$

$$B = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -\frac{8}{3} \end{bmatrix} \quad (3)$$

e

$$f_m(x_m) = \begin{bmatrix} 0 \\ -x_{m1}x_{m3} \\ x_{m1}x_{m2} \end{bmatrix}. \quad (4)$$

Assume-se que o seguinte possa ser estabelecido.

Hipótese 1: Na região $[0, \infty)$

$$\|H(t)\| \leq h_0 \quad (5)$$

onde h_0 é uma constante positiva, tal que $h_0 \leq \bar{h}_0$ e $\bar{h}_0$ é uma constante conhecida.

Hipótese 2: O parâmetro α é limitado superiormente por uma constante positiva conhecida $\bar{\alpha}$, tal que $\bar{\alpha} \geq \alpha$.

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

Comentário 2: No caso em que $\alpha = 0$, $\alpha = 0.8$ e $\alpha = 1$, o sistema (1) torna-se os sistemas Lorenz, Lü e Chen respectivamente quando $H(t) = 0$.

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

$$\dot{x}_s = (\hat{\alpha}A + B)x_s + f_s(x_s) + d(x_s, t) + u \quad (6)$$

onde $x_s \in \Re^3$ é o estado do sistema escravo, $u \in \Re^3$ é a entrada do controlador, $f_s(.)$ é uma função de mapeamento conhecida, $d(x_s, t)$ é um distúrbio desconhecido e $\hat{\alpha}$ é a estimação do parâmetro α do sistema mestre que se assume desconhecido para o sistema escravo,

$$f_s(x_s) = \begin{bmatrix} 0 \\ -x_{s1}x_{s3} \\ x_{s1}x_{s2} \end{bmatrix}. \quad (7)$$

Assume-se que o seguinte possa ser estabelecido.

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

$$\|d(x_s, t)\| \leq d_{s0} \quad (8)$$

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

Comentário 3: A hipótese 1 é natural uma vez que sistemas caóticos unificados são limitados por definição.

Portanto, nosso objetivo é projetar um controlador por realimentação u, tal que o estado x_s do sistema caótico escravo (6) sincronize com o estado x_m do sistema mestre (1), isto é, $\lim_{t\to\infty}[x_s(t) - x_m(t)] = 0$.

Defina o erro de sincronização como $e = x_s - x_m$. Então, de (1) e (6), obtém-se a equação de erro de sincronização

$$\dot{e} = \hat{\alpha}Ae + \tilde{\alpha}Ax_m + Be + f_s(x_s) - f_m(x_m) + D(t) + u \quad (9)$$

onde $D(t) = d(t) - cH(t)$ e $\tilde{\alpha} = \hat{\alpha} - \alpha$. (10)

Comentário 4: Note que nesta formulação, por simplicidade, foi considerado que $f_m(.) = f_s(.)$. Entretanto, esses mapeamentos não lineares podem não estar relacionados entre si, por exemplo, para incluir o conhecimento prévio de distúrbios.

3 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, almejamos 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. Adicionalmente, é apresentado um esquema para comunicação com segurança através de um canal público.

3.1 Esquema de sincronização

Nesta seção é provado, usando-se uma análise do tipo *Lyapunov-like*, que o erro de sincronização converge assintoticamente para zero.

Teorema 1: Considere os sistemas escravo (6) e mestre (1), que satisfazem as hipóteses 1-3, a lei de controle

$$u = -(\hat{\alpha}Ae + \tilde{\alpha}Ax_m + Be + f_s(x_s) - f_m(x_m)) - Le - u_r \quad (11)$$

com

$$u_r = \frac{le}{\lambda_{min}(K)[\|e\| + \gamma_1 \exp(-\gamma_0 t)]} \quad (12)$$

$$\dot{\hat{\alpha}} = -\gamma_\alpha[\gamma_2\|e\|\hat{\alpha} + e^T KAx_m] \quad (13)$$

onde

$$Q = L^T P + PL, P = P^T > 0, Q > 0, K = P + P^T$$

$$\gamma_3 = \lambda_{mín}(Q), \gamma_2 > 0, \gamma_1 > 0, \gamma_0 \geq 0, \gamma_\alpha > 0$$

$$\|\alpha\| \leq \bar{\alpha}, \|D(t)\| \leq D_0, \ \forall t \geq 0. \quad (14)$$

$\frac{l}{2} = \|K\|_F D_0 + \frac{\gamma_2}{2}\bar{\alpha}^2$, 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

$$V = e^T P e + \frac{\gamma_\alpha^{-1}\tilde{\alpha}^2}{2} \quad . \tag{15}$$

Derivando (14) em relação ao tempo resulta

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + \gamma_\alpha^{-1}\tilde{\alpha}\dot{\tilde{\alpha}} \, . \tag{16}$$

Utilizando (15), o erro de sincronização em malha fechada pode ser escrito como

$$\dot{e} = -Le + \tilde{\alpha}Ax_m + D(t) - u_r \quad . \tag{17}$$

Avaliando (16) ao longo da trajetória de (17), obtém-se

$$\begin{aligned}\dot{V} = {} & -e^T(L^T P + PL)e + e^T(P + P^T)\tilde{\alpha}Ax_m \\ & + e^T(P + P^T)(D(t) - u_r) + \gamma_\alpha^{-1}\tilde{\alpha}\dot{\tilde{\alpha}} \, .\end{aligned} \tag{18}$$

Usando agora (13) e (14), resulta

$$\dot{V} = -e^T Q e + e^T K D(t) - e^T K u_r - \gamma_2\tilde{\alpha}\hat{\alpha}\|e\| \, . \tag{19}$$

Adicionalmente, pode-se estabelecer que

$$\tilde{\alpha}\hat{\alpha} = \frac{1}{2}\tilde{\alpha}^2 + \frac{1}{2}\hat{\alpha}^2 - \frac{1}{2}\alpha^2 \, . \tag{20}$$

$$\lambda_{\text{mín}}(\text{Q})\|e\|^2 \le e^T Q e \le \lambda_{\text{máx}}(\text{Q})\|e\|^2 \tag{21}$$

Deste modo, empregando as hipóteses 1-3, (14), (20)-(21), (19) implica

$$\begin{aligned}\dot{V} \le {} & -\gamma_3\|e\|^2 + \|K\|_F D_0\|e\| - e^T K u_r + \frac{\gamma_2}{2}\alpha^2\|e\| \\ & - \frac{\gamma_2}{2}\tilde{\alpha}^2\|e\| \quad .\end{aligned} \tag{22}$$

A substituição de (12) em (22) resulta

$$\begin{aligned}\dot{V} \le {} & -\gamma_3\|e\|^2 + \left(\|K\|_F D_0 + \frac{\gamma_2}{2}\bar{\alpha}^2\right)\|e\| \\ & - \frac{l\|e\|^2}{[\|e\| + \gamma_1\exp(-\gamma_0 t)]} \\ & - \frac{\gamma_2}{2}\tilde{\alpha}^2\|e\| \quad .\end{aligned} \tag{23}$$

Utilizando-se (14) em (23), tem-se

$$\begin{aligned}\dot{V} \le {} & -\gamma_3\|e\|^2 - \frac{\frac{l}{2}\|e\|[\|e\| - \gamma_1\exp(-\gamma_0 t)]}{[\|e\| + \gamma_1\exp(-\gamma_0 t)]} \\ & - \frac{\gamma_2}{2}\tilde{\alpha}^2\|e\| \quad .\end{aligned} \tag{24}$$

Note que a expressão anterior implica

$$\dot{V} \le -\|e\|(\gamma_3\|e\| - \frac{l}{2} + \frac{\gamma_2}{2}\tilde{\alpha}^2) \tag{25}$$

Portanto $\dot{V} \le 0$ sempre que:

$$\|e\| \ge \frac{l}{2\gamma_3} = \alpha_1 \quad \text{ou} \quad |\tilde{\alpha}| \ge \sqrt{\frac{l}{\gamma_2}} = \alpha_2$$

Então, uma vez que α_1 e α_2 são constantes, empregando-se os argumentos usuais de Lyapunov (Slotine and Li, 1991), conclui-se que $e(t)$ e $\tilde{\alpha}(t)$ são uniformemente limitadas.

Por outro lado, a desigualdade (24) implica

$$\dot{V} \le -\gamma_3\|e\|^2 - \frac{\frac{l}{2}\|e\|[\|e\| - \gamma_1\exp(-\gamma_0 t)]}{[\|e\| + \gamma_1\exp(-\gamma_0 t)]} \tag{26}$$

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

$$\Omega = \{e(t) \mid \|e\| \le \gamma_1\exp(-\gamma_0 t), t \ge 0\} \tag{27}$$

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

$$\dot{V} \le -\gamma_3\|e\|^2 \tag{28}$$

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

$$\lim_{t\to\infty}\int_0^t \|e(\tau)\|^2 \, d\tau \le \frac{V(0) - V_\infty}{\gamma_3} < \infty \tag{29}$$

onde $\lim_{t\to\infty} V(t) = V_\infty < \infty$. Note que, baseado em (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 (Slotine and Li, 1991), conclui-se que $\lim_{t\to\infty} e(t) = 0$ para todo e.

3.2 Esquema de Comunicação Proposto

Baseado no teorema 1, a arquitetura do esquema de comunicação com segurança proposto é estabelecida por dois sistemas unificados caóticos diferentes e sujeitos a distúrbios como mostrado na figura 1.

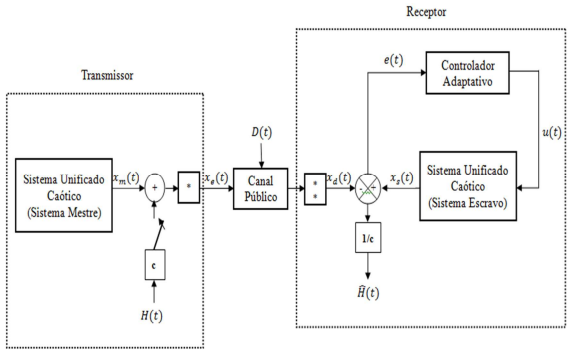

Figura 1. Esquema de comunicação com segurança proposto

No transmissor têm-se o sistema (1) com parâmetro α, enquanto no receptor têm-se o sistema (6) que utiliza uma estimativa do valor de α definida por (13) e um controlador adaptativo definido por (11). No transmissor, a mensagem original $H(t)$ é multiplicada por um fator c e somada ao sistema (1). Este fator deve ser escolhido de modo a reduzi-lo a ponto de ser mascarado com sucesso pelo sistema caótico. O sinal resultante é então encriptado (*) e enviado via canal publico como $x_e(t)$ com um distúrbio $D(t)$. O receptor recebe o sinal decriptado (**) $x_d(t)$ e, por intermédio do controlador adaptativo (11) e a estimação de parâmetro (13), atinge a sincronização após um tempo T_s. Em um instante arbitrário T_i ,onde $T_i > T_s$, o receptor começa a recuperar a mensagem $H(t)$. Durante a comunicação, o transmissor pode utilizar como chave de segurança $K_e = \{x_{m1}(0), x_{m2}(0), x_{m3}(0), \alpha, T_i\}$ e o receptor, $K_d = \{x_{s1}(0), x_{s2}(0), x_{s3}(0), \hat{\alpha}(0), T_i\}$. O sinal encriptado é enviado através de um canal aberto a invasores, porém o desconhecimento dos valores utilizados na chave de decriptação deixa a recuperação do sinal extremamente difícil. Além disso, é importante notar que mesmo a menor das diferenças na chave de decriptação altera completamente o sinal obtido.

4 Simulações

Nesta seção, avaliamos a viabilidade do sistema de comunicação proposto. O primeiro experimento serve para confirma o esquema de sincronização adaptativa proposto em 3.1 e o segundo experimento é para confirmar a transmissão da mensagem e sua decriptação. Foi utilizada uma imagem digital Lena 128x128. 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.

Foi considerado que $x_m(0) = [1.5\ 2\ 5]$ e $x_s(0)$ =[4 8 3]. Para obter a sincronização do sistema escravo (6) e o sistema mestre (1), foram utilizadas as leis de controle (11)-(12) e a lei de adaptação (13).

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 $P = diag(0.0001, 0.1, 0.05, 0.01)$.

As chaves de encriptação e decriptação foram consideradas respectivamente como

$$\begin{cases} K_e = \{x_{m1}(0), x_{m2}(0), x_{m3}(0), \alpha, T_i\} \\ K_d = \{x_{s1}(0), x_{s2}(0), x_{s3}(0), \hat{\alpha}(0), T_i\} \end{cases} \quad (30)$$

A mensagem transmitida é uma sequência de bits que compõe a imagem escolhida em escala de cinza (8 bits por pixel). Vide figura 11 para maiores detalhes.

As Figuras 2-4 mostram os desempenhos de sincronização obtidos com o esquema proposto. Nelas deve ser notada a rápida sincronização entre os sistemas mestre e escravo. Isso mostra que o controlador adaptativo proposto consegue atingir a sincronização em aproximadamente 1 ms. Já as figuras 8-10 mostram os estados encriptados que estão disponíveis no canal público. Se compararmos estes sinais com os sinais originais presentes nas figuras 2-4 vê-se uma grande diferença.

A imagem digital Lena reconstruída, figura 11, é perfeitamente igual à enviada. Quando a imagem é visualizada no canal público ela se torna irreconhecível, figura 12. Na tentativa de obter a imagem com uma chave quase idêntica obtivemos a figura 13, que comprova a dificuldade na quebra de sigilo da mensagem. Desta forma mostramos que o esquema de envio de informação proposto é seguro.

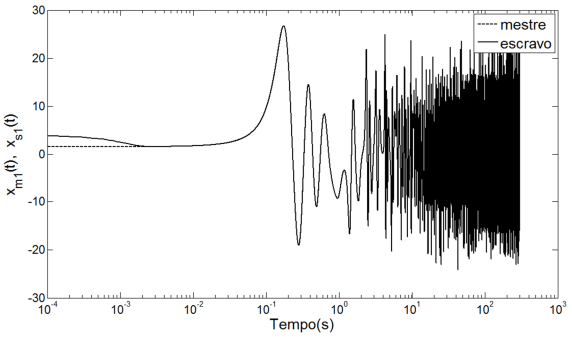

Figura 2. Desempenho da sincronização de $x_{s1}(t)$.

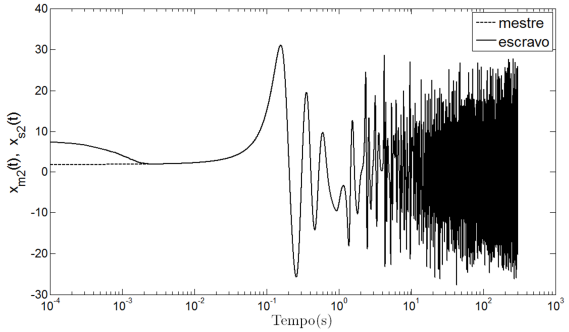

Figura 3. Desempenho da sincronização de $x_{s2}(t)$.

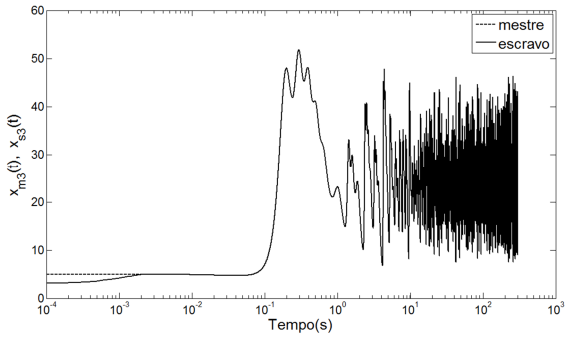

Figura 4. Desempenho da sincronização de $x_{s3}(t)$.

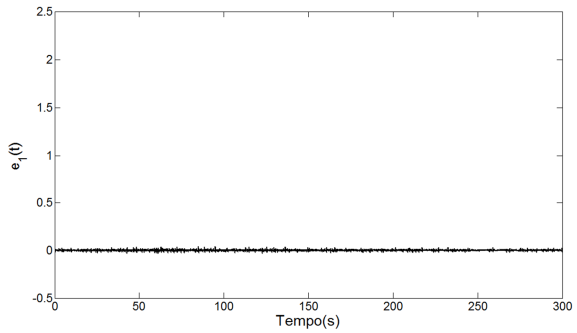

Figura 5. Erro de sincronização $e_1(t)$.

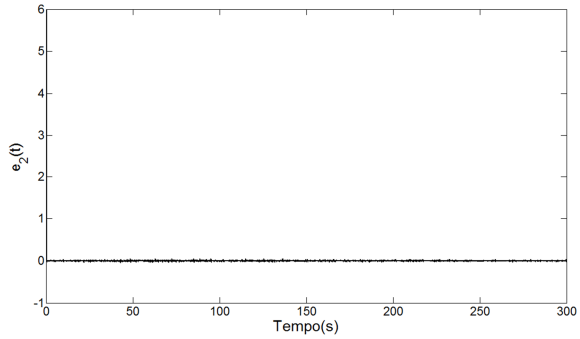

Figura 6. Erro de sincronização $e_2(t)$.

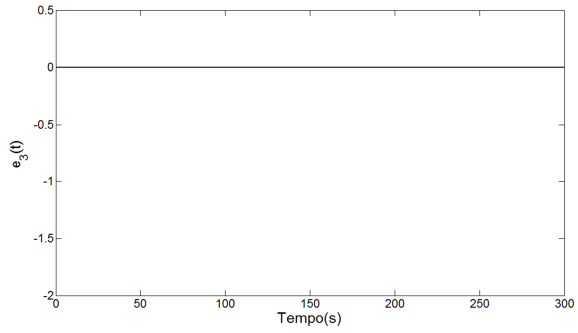

Figura 7. Erro de sincronização $e_3(t)$.

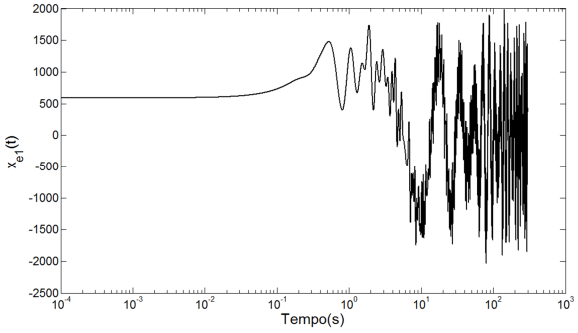

Figura 8. Sinal $x_{e1}(t)$, i.e., $x_{m1}(t)$ encriptado.

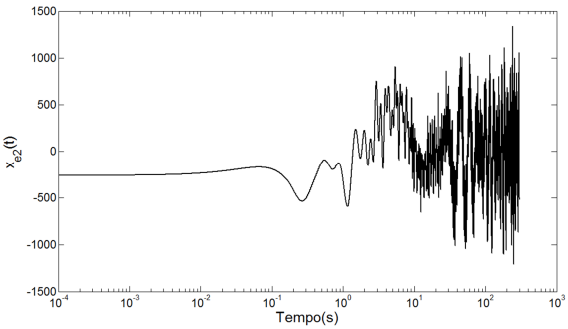

Figura 9. Sinal $x_{e2}(t)$, i.e., $x_{m2}(t)$ encriptado.

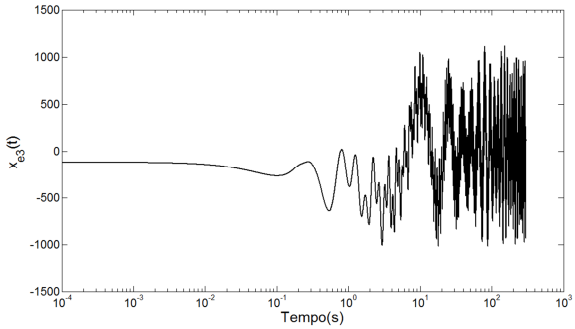

Figura 10. Sinal $x_{e3}(t)$, i.e., $x_{m3}(t)$ encriptado.

Figura 11. Imagem digital Lena 128x128 em escala cinza.

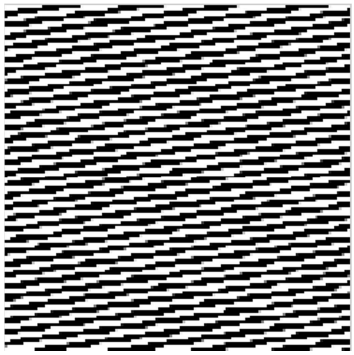

Figura 12. Imagem digital visualizável no canal público.

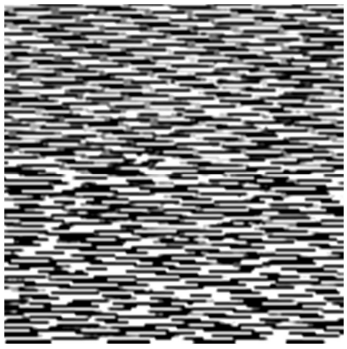

Figura 13. Imagem digital obtida com a utilização de uma chave de decriptação errada.

5 Conclusões

Neste artigo 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.

6 Referências

Kanso, A. and Ghebleh, M. (2012). A novel image encryption algorithm base on a 3D chaotic map. Communications in Nonlinear Sciences and numerical Simulation. No 17, pp. 2943-2959.

Mata-Machuca, J. L., Martinez-Guerra, R., Aguilar-Lopez, R. and Aguilar-Ibanez, C. (2011). A chaotic system in synchronization and secure communications, Communications in Nonlinear Science and Numerical Simulation, No. 17, pp. 1706-1713.

Qun Ding, J. and Du, B. (2011). A new improved scheme of chaotic masking secure communication based on Lorenz system. International Journal of Bifurctaion and Chaos, Vol. 22, No. 5.

Slotine, J.J. and Li, W. (1991). Applied nonlinear control, Prentice-Hall, Inc., Englewood Cliffs, New Jersey.

Smaoui, N.; Karouma, A. and Zribi, M. (2011). Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systms, Commun Nonlinear Sci Numer Simulat, No 16, pp. 3279-3293.

XiaoHong, H. and XiaoMing, C. (2012). A chaotic digital secure communication based on a modified gravitational search algorithm filter. Information Sciences, No 208, pp. 14-27.