TEMA Tend. Mat. Apl. Comput., **9**, No. 1 (2008), 105-114.

Sincronização do Sistema Caótico Unificado via Controle Ótimo Linear *Feedback* e Aplicação em Comunicação Segura

J.M.V. GRZYBOWSKI[1], M. RAFIKOV[2], Departamento de Física, Estatística e Matemática, DeFEM, UNIJUI, Cx.P. 560, 98700-000 Ijuí, RS, Brasil.

Resumo. O presente artigo estuda a sincronização do sistema caótico unificado via controle ótimo linear feedback e apresenta um esquema de comunicação segura baseado em sincronização de caos.

Palavras-chave. Sincronização, controle ótimo, caos, comunicação segura.

1. Introdução

A sincronização de caos aplicada à comunicação tem sido objeto de intenso estudo. A idéia de utilizar a sincronização de caos para transportar informações justifica-se por duas razões principais. Por um lado, porque sistemas caóticos possuem várias características desejáveis do ponto de vista criptográfico: ergodicidade, sensibilidade às condições iniciais, complexidade e dinâmica determinística. Isso significa que, além de transportar informações (como sinais periódicos fazem), o sinal caótico é potencialmente um método de criptografar. Por outro lado porque sistemas de comunicação sem fio baseiam-se em sincronização, e isso significa que há um grande campo para sua aplicação. Diversos trabalhos foram dedicados à proposta e análise de sistemas criptográficos baseados em sincronização de caos. Dentre os principais problemas encontrados nesses enfoques estão o nível insuficiente de segurança ([1], [2]) e o excessivo tempo necessário para sincronização ([4], [6]), o que os torna desinteressantes do ponto de vista prático. Lü et al. propuseram em [6] um sistema criptográfico particularmente interessante, baseado num sistema caótico que faz uma ponte entre o sistema de Lorenz e o sistema de Chen através da inclusão de um parâmetro $0 \leq \alpha \leq 1$, que foi utilizado como chave no sistema. Conforme mostrado em [6], através da construção de uma função de Lyapunov apropriada, é possível sincronizar os sistemas caóticos unificados através de acoplamento para $0 \leq \alpha \leq 1/29$. Logo, o espaço da chave fica restrito a esse subintervalo para o qual os sistemas podem ser sincronizados por acoplamento. Nesse contexto, propusemos em [3] a utilização do controle ótimo linear feedback, conforme metodologia proposta em [7], para sincronizar dois sistemas caóticos unificados para todo o intervalo

[1]zzmariovic@yahoo.com.br
[2]marat9119@yahoo.com.br

$0 \leq \alpha \leq 1$. Isso significa que é possível aumentar consideravelmente o espaço da chave e, como conseqüência, o nível de segurança do sistema.

O presente trabalho tem dois objetivos principais: em primeiro lugar estudar a sincronização do sistema caótico unificado aplicando o controle ótimo linear feedback em forma escalar (controlando apenas uma das equações do sistema) e a seguir em forma vetorial (controlando todas as equações); em segundo lugar, propor um sistema de encriptação baseado na sincronização de caos. Com base nos resultados obtidos em [3] e utilizando algumas idéias do sistema de encriptação caótica apresentado em [8], propomos um esquema de encriptação baseado no sistema caótico unificado apresentado em [6]. Na seção 2 é apresentada a metodologia de projeto do controle ótimo linear feedback para sistemas não-lineares. Na seção 3, apresentamos o sistema caótico unificado e simulações de sincronização do sistema através de controle escalar e vetorial. Na seção 4 apresentamos o esquema de encriptação baseado na sincronização de caos e resultados de simulações numéricas. A seção 5 apresenta conclusões.

2. Sincronização de Sistemas Não-lineares via Controle Ótimo Linear *Feedback*

Considere os sistemas mestre e escravo na forma

$$\dot{x} = Ax + g(x) \tag{2.1}$$

$$\dot{y} = Ay + g(y) + Bu \tag{2.2}$$

sujeitos a

$$x(0) = x_0 \tag{2.3}$$

$$y(0) = y_0 \tag{2.4}$$

onde $x, y \in R^n$ são vetores de estado; $A \in R^{nxn}$ é a matriz dos termos lineares do sistema; $g \in R^n$ é o vetor das funções não-lineares, $B \in R^{nxm}$ é uma matriz constante e $u \in R^m$ é um vetor de controle que estabiliza o sistema escravo na órbita desejada. Assim, definindo o vetor erro como

$$e = y - x, \tag{2.5}$$

obtemos o sistema em desvios

$$\dot{e} = Ae + g(y) - g(x) + Bu = Ae + g(x + e) - g(x) + Bu. \tag{2.6}$$

Introduzindo

$$h(x, e) = g(x, e) - g(x), \tag{2.7}$$

obtemos

$$\dot{e} = Ae + h(x, e) + Bu. \tag{2.8}$$

Teorema 2.1. *Se existem matrizes Q e R definidas positivas, sendo Q simétrica, de forma que a função*

$$l(x,e) = e^T Qe - h^T(x,e)Pe - e^T Ph(x,e) \tag{2.9}$$

é definida positiva, onde a matriz P é a solução da equação algébrica matricial de Ricatti

$$PA + A^T P - PBR^{-1}B^T P + Q = 0, \tag{2.10}$$

então o controle linear feedback

$$u = -R^{-1}B^T Pe \tag{2.11}$$

é ótimo no sentido de transferir o sistema em desvios (2.8) de qualquer estado inicial ao estado final

$$e(\infty) = 0 \tag{2.12}$$

minimizando o funcional

$$J = \int_0^\infty [l(x,e) + u^T Ru]dt. \tag{2.13}$$

Se a condição suficiente $l(x,e) \geq 0$, para qualquer $e \in R^n$ é satisfeita, então o sistema em desvios é globalmente assintoticamente estável e isso implica que o sistema mestre e o sistema escravo controlado estão sincronizados.

Demonstração. Considere o controle ótimo linear feedback (2.11) que transfere o sistema não-linear (2.8) de qualquer estado inicial para o estado final (2.12) minimizando o funcional (2.13), onde a função $l(x,e)$ precisa ser determinada.
De acordo com as regras da Programação Dinâmica, se o mínimo do funcional (2.13) existe, e se V é uma função suave das condições iniciais, então ela satisfaz a equação de Hamilton-Jacobi-Bellman

$$\min_u(\frac{dV}{dt} + e^T l(x,e)e + u^T Ru) = 0. \tag{2.14}$$

Considerando uma função de Lyapunov na forma

$$V = e^T, Pe, \tag{2.15}$$

onde P é uma matriz simétrica definida positiva e satisfaz a equação algébrica matricial de Ricatti (2.10), a derivada da função V, avaliada na trajetória ótima com controle (2.11) é

$$\dot{V} = \dot{e}^T Pe + e^T P\dot{e}. \tag{2.16}$$

Levando (2.8) em (2.16), obtemos

$$\dot{V} = e^T A^T Pe + h^T(x,e)Pe + e^T PAe + e^T Ph(x,e) - e^T PB(R^{-1})^T B^T Pe. \tag{2.17}$$

Substituindo $\dot{V}$ na equação de Hamilton-Jacobi-Bellman (2.14), obtemos

$$l(x,e) = e^T Qe - h^T(x,e)Pe - e^T Ph(x,e). \tag{2.18}$$

Observe que para uma função definida positiva $l(x,e)$ e uma matriz definida positiva R, a derivada da função (2.15), avaliada na trajetória ótima do sistema (2.8), é dada por

$$\dot{V} = -l(x,e) - u^T R u \tag{2.19}$$

e é definida negativa. Então a função (2.15) é uma função de Lyapunov e, de acordo com a teoria da estabilidade de Lyapunov, podemos concluir que o sistema em desvios (2.8) é globalmente assintoticamente estável se é satisfeita a condição suficiente $l(x,e) \geq 0$ para qualquer $e \in R^n$. Portanto, o sistema mestre e o sistema escravo controlado estão globalmente sincronizados.
De acordo com a teoria do controle ótimo de sistemas lineares com funcional quadrático, a solução da equação algébrica matricial de Ricatti (2.10) é uma matriz simétrica e definida positiva $P > 0$ para $Q > 0$ e $R > 0$ dados. Assim, a prova do teorema está completa. □

3. Sincronização do Sistema Caótico Unificado

3.1. O sistema caótico unificado

Lü et al. [6] propuseram um sistema caótico que unifica os sistemas de Lorenz e de Chen através da inclusão de um parâmetro $0 \leq \alpha \leq 1$. Para $\alpha = 0$, o sistema unificado se torna o sistema de Lorenz; para $\alpha = 1$, o sistema de Chen; e para $\alpha = 0,8$ surge um terceiro sistema, cujo atrator é topologicamente não-equivalente aos outros dois, chamado sistema de Lü. Para todo o intervalo de valores $0 \leq \alpha \leq 1$ o sistema apresenta comportamento caótico.

$$\begin{aligned} \dot{x_1} &= (25\alpha + 10)(x_2 - x_1) \\ \dot{x_2} &= (28 - 35\alpha)x_1 + (29\alpha - 1)x_2 - x_1 x_3 \\ \dot{x_3} &= x_1 x_2 - (\frac{\alpha + 8}{3})x_3. \end{aligned} \tag{3.1}$$

As equações do sistema caótico podem ser escritas na forma matricial como

$$\begin{pmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{pmatrix} = \begin{pmatrix} -25\alpha - 10 & 25\alpha + 10 & 0 \\ 28 - 35\alpha & 29\alpha - 1 & 0 \\ 0 & 0 & \frac{-\alpha - 8}{3} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{pmatrix}. \tag{3.2}$$

As figuras 1, 2 e 3 a seguir mostram os atratores do sistema caótico unificado para $\alpha = 0$ (atrator de Lorenz), para $\alpha = 0,8$ (atrator de Lü) e para $\alpha = 1$ (atrator de Chen).

As figuras 4 e 5 mostram o resultado de simulações numéricas da sincronização do sistema caótico unificado via controle ótimo linear feedback para $\alpha = 0,8$, primeiro usando controle escalar e em seguida controle vetorial.
Considerando o sistema mestre (3.2), o sistema escravo tem a forma

$$\begin{pmatrix} \dot{y_1} \\ \dot{y_2} \\ \dot{y_3} \end{pmatrix} = \begin{pmatrix} -25\alpha - 10 & 25\alpha + 10 & 0 \\ 28 - 35\alpha & 29\alpha - 1 & 0 \\ 0 & 0 & \frac{-\alpha - 8}{3} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} 0 \\ -y_1 y_3 \\ y_1 y_2 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}. \tag{3.3}$$

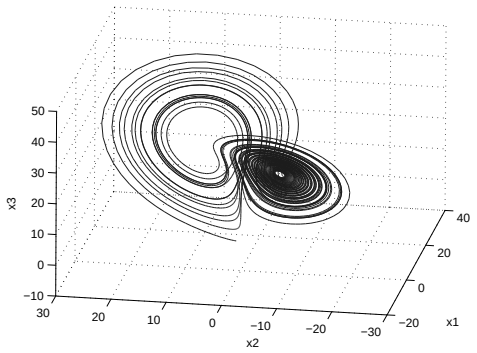


Figura 1: Atrator de Lorenz.

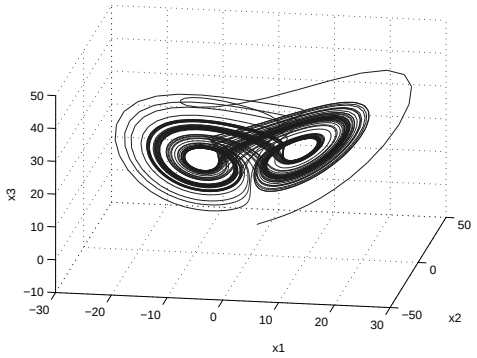


Figura 2: Atrator de Lü.

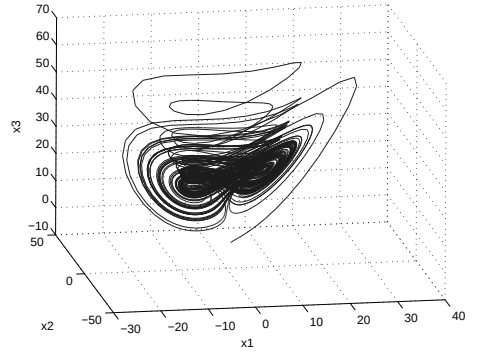


Figura 3: Atrator de Chen.

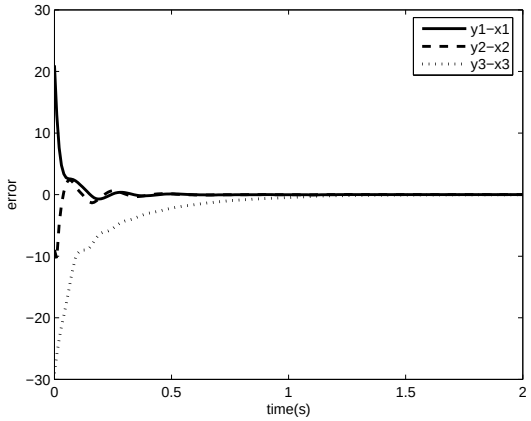


Figura 4: Erro de sincronização - controle escalar.

Para as simulações a seguir, utilizamos as condições iniciais $x(0) = \begin{pmatrix} -20 & 10 & 30 \end{pmatrix}^T$ e $y(0) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}^T$.

3.2. Simulações numéricas

Sincronização do sistema caótico unificado através de controle escalar

De (3.2) obtemos

$$A = \begin{pmatrix} -30 & 30 & 0 \\ 0 & 22,2 & 0 \\ 0 & 0 & -2,9333 \end{pmatrix}. \tag{3.4}$$

Escolhendo

$$Q = \begin{pmatrix} 8000 & 0 & 0 \\ 0 & 8000 & 0 \\ 0 & 0 & 8000 \end{pmatrix};\ B = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix};\ R = 1 \tag{3.5}$$

e resolvendo a equação algébrica matricial de Riccatti através da função LQR do software MATLAB®, obtemos o controle linear feedback em forma escalar

$$u_2 = -\begin{pmatrix} 27,664 & 122,960 & 0 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \tag{3.6}$$

A figura 4 mostra que o erro se aproxima rapidamente de zero e, dessa forma, os sistemas estão sincronizados.

Sincronização do sistema caótico unificado através de controle vetorial

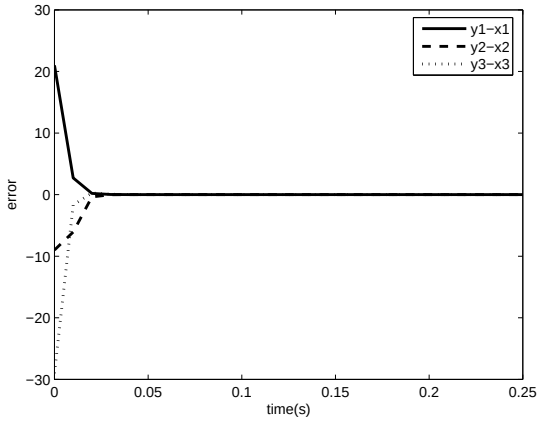


Figura 5: Erro de sincronização - controle vetorial.

Considerando-se (3.4) e escolhendo

$$Q = \begin{pmatrix} 8000 & 0 & 0 \\ 0 & 8000 & 0 \\ 0 & 0 & 8000 \end{pmatrix}; B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.7}$$

Resolvendo a equação algébrica matricial de Riccatti através da função LQR do software MATLAB®, obtemos o controle linear feedback em forma vetorial

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = -\begin{pmatrix} 63,793 & 10,144 & 0 \\ 10,144 & 117,061 & 0 \\ 0 & 0 & 86,558 \end{pmatrix} \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \\ y_3 - x_3 \end{pmatrix}. \tag{3.8}$$

A figura 5 mostra o comportamento das variáveis de estado dos sistemas mestre e escravo. O erro se aproxima rapidamente de zero, e os sistemas estão sincronizados após decorrido 0,27 segundo.

4. Aplicação em Comunicação Segura

Nesta seção apresentamos uma aplicação da sincronização de sistemas caóticos em comunicação. O sistema caótico unificado é utilizado como base do esquema e o processo consiste em duas etapas distintas: a sincronização e a encriptação, transmissão e decriptação da mensagem.

As equações do sistema transmissor e receptor são mostradas a seguir:

$$\begin{aligned} \dot{x_1} &= (25\alpha + 10)(x_2 - x_1) \\ \dot{x_2} &= (28 - 35\alpha)x_1 + (29\alpha - 1)x_2 - x_1x_3 + Cm \\ \dot{x_3} &= x_1x_2 - (\frac{\alpha + 8}{3})x_3 \end{aligned} \tag{4.1}$$

$$\begin{aligned} \dot{y_1} &= (25\alpha + 10)(y_2 - y_1) + u_1 \\ \dot{y_2} &= \dot{x_2} + u_2 \\ \dot{y_3} &= y_1 y_2 - (\frac{\alpha + 8}{3}) y_3 + u_3 \\ m &= \frac{1}{C}(\dot{x_2} - (28 - 35\alpha) y_1 - (29\alpha - 1) y_2 + y_1 y_3), \end{aligned} \tag{4.2}$$

onde m é a mensagem, C é uma constante que tem o objetivo de diminuir a amplitude da mensagem em relação ao sinal caótico transmitido $\dot{x_2}$.

Na primeira etapa, os sistemas transmissor e receptor são sincronizados na forma mestre/escravo, onde o sistema receptor é controlado e sua trajetória é levada à do sistema transmissor, de forma que o erro entre as trajetórias é levado a zero, ou seja, $\|e\| = 0$. Nesta etapa, $m = 0$.

Na segunda etapa, inicia-se em (4.1) o processo de encriptação e transmissão do sinal $\dot{x_2}$, que é recebido e decriptado na quarta equação de (4.2). Nesta etapa, $\|e\| = 0$ e, como conseqüência, $\|u\| = 0$.
No contexto da criptografia, o parâmetro α é a chave do sistema criptográfico. Dessa forma, o espaço da chave é o intervalo $[0, 1]$.

As simulações apresentadas contemplam a encriptação de uma imagem e um parágrafo de texto. Para a encriptação da imagem, as linhas da matriz de intensidade de brilho dos pixels que compõe a imagem são concatenadas e a matriz é transformada em um vetor; cada pixel é representado por um número inteiro que pertence ao intervalo $[0, 255]$. No caso do texto, os caracteres são convertidos em código ASCII, e passam a ser um número inteiro no intervalo $[0, 127]$. Assim o vetor m da mensagem é formado e, a seguir, cada elemento de m é adicionado à segunda equação do sistema transmissor em um passo de integração. Nas simulações, os sistemas são integrados através do método de Runge-Kutta de 4ª ordem, com passo de integração $p = 10^{-2}$ e $C = 10^{-6}$. Apresentamos o resultado da aplicação do algoritmo à notória "foto de Lenna"e a um parágrafo de texto nas figuras a 6 e 7.

5. Conclusões

Através da aplicação do controle ótimo linear feedback, obtivemos a sincronização do sistema caótico unificado através de controle escalar e vetorial. Em ambos os casos a sincronização ocorreu de maneira rápida e eficiente. As simulações numéricas do processo de encriptação revelaram que, tanto a imagem quanto o texto encriptados tornaram-se ininteligíveis após o processo, sendo recuperados com absoluta perfeição no receptor. Em trabalhos futuros pretendemos aumentar o nível de segurança do algoritmo através da utilização de parâmetro α variável.

Absctract. This paper studies the synchronization of the unified chaotic system via optimal linear feedback control and presents a secure communication scheme based on chaos synchronization.

Keywords. Synchronization, optimal control, chaos, secure communication.

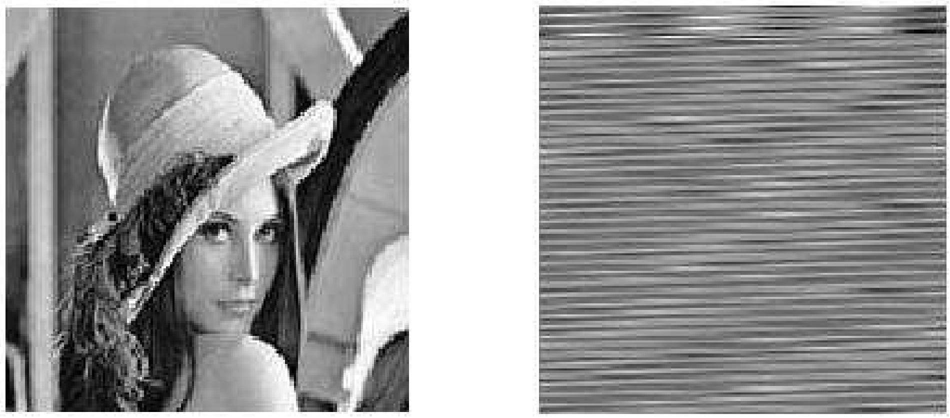
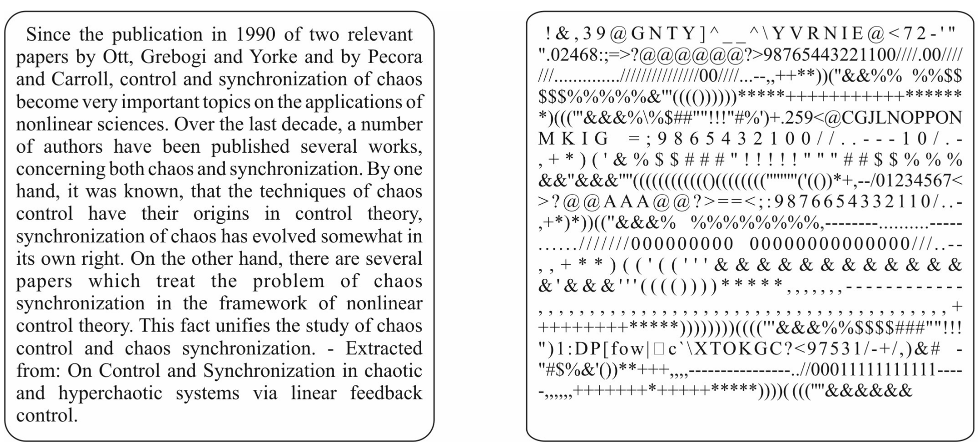


Figura 6: Imagem original e imagem encriptada.



Since the publication in 1990 of two relevant papers by Ott, Grebogi and Yorke and by Pecora and Carroll, control and synchronization of chaos become very important topics on the applications of nonlinear sciences. Over the last decade, a number of authors have been published several works, concerning both chaos and synchronization. By one hand, it was known, that the techniques of chaos control have their origins in control theory, synchronization of chaos has evolved somewhat in its own right. On the other hand, there are several papers which treat the problem of chaos synchronization in the framework of nonlinear control theory. This fact unifies the study of chaos control and chaos synchronization. - Extracted from: On Control and Synchronization in chaotic and hyperchaotic systems via linear feedback control.

!&,39@GNTY]^__^\YVRNIE@<72-'"
".02468:;=>?@@@@@@?>98765443221100////.00////
///............./////////////////00////...--,,++**))("&&%% %%$$
$$$%%%%%&'"((()))))*****++++++++++++******
*)((("'&&&%\%$##""!!!"#%')+.259<@CGJLNOPPON
MKIG =;98654321 00//..---10/.-
,+*)('&%$$###"!!!!!"""##$$%%%
&&"&&&'"(((((((((((()((((((((""""""('(())*+,--/01234567<
>?@@AAA@@?>==<;:98766543321 10/..-
,+*)*))(("&&&% %%%%%%%%,--------.........-----
....../////////000000000 000000000000000///..--
,,+**)(('(('''&&&&&&&&&&&&
&'&&&'''(((()))))*****,,,,,,,,------------
,,,+
+++++++++*****))))))))(((("'&&&%%$$$$###""!!!
")1:DP[fow|□c`\XTOKGC?<97531/-+/,)&# -
"#$%&'())**+++,,,,---------------..//0001111111111----
-,,,,,,++++++++*++++++*****))))(((("'&&&&&&

Figura 7: Texto original e texto encriptado.

Referências

[1] G. Alvarez, S. Li, Breaking network security based on synchronized chaos, *Computer Communications*, **17**, 1749-1756.

[2] G. Alvarez, F. Montoya, G. Pastor, M. Romera, Cryptanalyzing an improved security modulated chaotic encryption scheme using cyphertext absolute value, *Chaos, Solitons and Fractals* **23**, 1679-1681.

[3] J.M.V. Grzybowski, M. Rafikov, Synchronization of a unified chaotic system via optimal linear feedback control, in "Proceedings of the XI Brazilian Conference on Dynamics, Control and Their Applications", 2007.

[4] A.M. Harb, W.M. Ahmad, Chaotic systems synchronization in secure communication systems, in "Proceedings of the 2006 International Conference on Communication in Computing", CIC 2006, Las Vegas, Nevada, USA, June 26-29.

[5] G.P. Jiang, G. Chen, W.K.S. Tang, A new criterion for chaos synchronization using linear state feedback control, *International Journal of Bifurcation and Chaos*, **13** (2003).

[6] J. Lu, X. Wu, J. Lu, Synchronization of a unified chaotic system and application in secure communication, *Physics Letters A*, **305** (2002), 365-370.

[7] M. Rafikov, J.M. Balthazar, On control and synchronization in chaotic and hyperchaotic systems via linear feedback control, *Communications in Nonlinear Sciences and Numerical Simulation*, (2007), doi:10.1016/j.cnsns.2006.12.011.

[8] M. Sobhy, A. Shehata, Chaotic algorithms for data encryption, *IEEE International Conference on Acoustics, Speech and Signal Processing*, Proceedings (Cat. No.01CH37221). IEEE. Part vol.2, pp.997-1000.