• SINCRONIZAÇÃO DE SISTEMA CAÓTICO

Leiliane Borges Cunha– leilianebc@hotmail.com
Universidade Federal do Pará-UFPA, Faculdade de Engenharia Elétrica - FEE
Rua Augusto Corrêa, 01, Guamá
66075-110, Belém - Pará

Bruno Igor Dias de Sousa – igordias15@hotmail.com

José Augusto Lima BarreiroS – barreiro@ufpa.br

Resumo*: A construção deste trabalho objetiva analisar técnicas de projeto de controladores com domínios no espaço de estado coincidentes com os de atratores caóticos, e técnicas de modo a forçá-los a entrarem em comportamento pré-especificado. O controle do caos pode ser compreendido como a utilização de pequenas perturbações para a estabilização de orbitas periódicas instáveis, imersas em um atrator caótico. Tendo em vista que o caos pode ocorrer em vários processos naturais, a idéia de o comportamento caótico ser controlado através de pequenas perturbações de certos parâmetros físicos, permite que este tipo de comportamento seja desejável em diversas aplicações. Com base nessa literatura, fez-se um estudo do sincronismo de um sistema caótico unificado, através de dois sistemas (mestre-escravo), que com o auxilio do software MATLAB, foi possível simulá-los e obter respostas temporais e o espaço de fases das variáveis que regem cada equação. Com isso, verificou-se que, com a variação dos parâmetros de controle escolhidos para o sistema, o mesmo adquire comportamentos diferentes para cada valor fornecido, ou seja, para uns valores, o sistema apresenta comportamento caótico, caracterizando a não linearidade do sistema e para outros, periodicidade.*

Palavras-chave*: Sistemas Não-Lineares, Caos, Sincronização, criptografia.*

1. INTRODUÇÃO

A existência de sistemas dinâmicos, intrinsecamente determinísticos com comportamento caótico já havia sido observada no início do século passado por Henri Poincaré, que abandonou o assunto por considerá-lo apenas uma curiosidade matemática. A teoria do caos, assim batizada, começou formalmente no ano de 1955, quando um cientista do departamento de meteorologia do Boston Tech, atualmente conhecido como M.I.T. (Instituto de Tecnologia de Massachusetts), chamado Eduard Norton Lorenz, herdou a direção de um projeto de pesquisa cujo estudo se concentrava na previsão estatística do tempo. O trabalho do meteorologista se limitava a determinar os valores destas constantes a, b, c e os preditores – elementos climáticos que multiplicam as constantes. Lorenz, não satisfeito com os resultados de previsões sinópticas e numéricas obtidos com equações de caráter linear, propôs utilizar

previsões a partir de sistemas de equações não lineares, isto é bem razoável pelo fato que a linearidade perfeita faz com que cada variável sempre assuma os mesmos valores apresentados no ciclo anterior. Tal modelo tinha como objetivo reproduzir o movimento das correntes de ar na atmosfera.

Ao repetir alguns cálculos em seu modelo, Lorenz percebeu que os novos resultados de sua simulação não se pareciam com os obtidos anteriormente, sendo inicialmente iguais e diferindo após algum tempo. Fisicamente, este resultado poderia ser interpretado como sendo as condições climáticas que, primeiramente, comportavam-se de forma semelhante à simulação anterior, dias após surgiam pequenas diferenças, depois diferenças cada vez maiores até que, semanas depois, as características climáticas eram totalmente diferentes das características da simulação anterior. Entretanto, a conclusão de Lorenz foi que os números usados não eram exatamente os mesmos, pois estavam arredondados, e a esta pequena diferença, causada pela aproximação, embora irrisória no início, foi de maneira tão incisiva se avolumando até que mudasse totalmente o resultado final. Tal fenômeno foi denominado de caos.

Com a proliferação de artigos envolvendo o controle, sincronização e a criptografia de diversos sistemas caóticos, começou-se a vislumbrar diversas aplicações práticas para este interessante campo de pesquisa, hoje conhecido como controle de caos.

Na engenharia, suas aplicações são inúmeras, envolvendo a engenharia eletrônica de osciladores, a engenharia de controle de motores usando técnicas não-lineares, a engenharia de telecomunicações, envolvendo técnicas de criptografia de sinais e imagens, técnicas de modulação e demodulação de sinais, equalização de canais, etc. também há aplicações em outras áreas da engenharia, e mesmo em outras áreas da ciência, como a biologia, onde abundam análise de sinais não-lineares provenientes dos seres vivos (relógios ou osciladores biológicos), quer sejam de origem endógena, ou por resposta a estímulos.

Nesse sentido, busca-se realizações, por simulações, da modelagem matemática de sistemas caóticos, bem como no processo de criptografia na transmissão digital de sinais.

1. CARACTERIZAÇÃO DA DINÂMICA CAÓTICA

A dinâmica caótica apresenta conceitos relativos a sistemas dinâmicos não lineares, mais precisamente sobre caos, tais como dependência sensível às condições iniciais, conjugação de mapas, aleatoriedade e atratores estranhos.

1.1. Dependência sensível às condições iniciais

Um sistema dinâmico apresenta dependência sensível às condições iniciais quando o sinal gerado pelo sistema com condições iniciais ligeiramente diferentes apresenta valores completamente distintos do sinal anterior, após algumas iterações, e sua resposta tende a apresentar um comportamento totalmente aleatório e órbitas caóticas, ou seja, se torna totalmente aperiódico e imprevisível.

1.2. Sinais caóticos

Informalmente, um sinal caótico é determinístico, aperiódico e apresenta dependência sensível a condições iniciais. Orbitas com dependência sensível a condições iniciais possuem imprevisibilidade na evolução temporal, portanto, é impossível determinar com exatidão a trajetória de uma condição inicial próxima a uma órbita com dependência sensível a

condições iniciais, mesmo realizando tal análise logo após algumas iterações. É difícil determinar com exatidão a condição inicial de uma órbita, por isso, quando se trabalha com sinais caóticos deve-se considerar esta incerteza.

1.3. Atratores estranhos

Um dos conceitos mais fundamentais no estudo da teoria do caos é o atrator. Um atrator é um conjunto de sistemas dinâmicos de condição estável. Alguns atratores são simples ponto, outros são objetos de geometria complexa. Os atratores podem ser divididos em dois grupos: não caóticos ou caóticos. Os atratores não caóticos são previsíveis e de trajetória regular. Os atratores caóticos ou atratores estranhos aparecem apenas após o começo do caos. Em relação aos efeitos que produzem, estes atratores revelam-se extremamente sensíveis às mais ligeiras variações verificadas nas condições iniciais do seu desenvolvimento, à medida que as iterações vão ocorrendo ao longo do tempo, assim se vai desenvolvendo certo padrão de desordem.

2. CRIPTOGRAFIA E SINCRONIZAÇÃO DO SISTEMA CAÓTICO UNIFICADO

Um dos assuntos bastante abordado na atualidade é o sincronismo e a criptografia de sistemas caóticos, pois esses dois processos estão sendo aplicado em grande escala em processos de comunicações, principalmente, quando se detecta presença de ruído.

2.1. Criptografia

A criptografia é arte de codificar mensagens garantindo o sigilo das informações. Além do uso militar, a criptografia desempenha um importante papel na tecnologia moderna, garantindo a segurança das transações comerciais na internet e a privacidade dos dados dos computadores modernos. Atualmente os principais algoritmos de criptografia se baseiam em algoritmos simétricos, nos quais a várias operações bit a bit e permutações entre os elementos vizinhos de um texto e a palavra chave codificam as mensagens e algoritmos assimétricos, que tem como base a teoria dos números. Um problema destes algoritmos é a facilidade para quebrar suas cifras. Como uma alternativa para sofisticar os algoritmos de criptografia e aumentar sua segurança é a exploração de métodos baseados em sistemas caóticos. A teoria do caos para a física e a matemática é a hipótese que explica o funcionamento de sistemas complexos e dinâmicos, os quais apresentam grande instabilidade nas condições iniciais, produzindo resultados para cada configuração inicial. Este trabalho apresenta um algoritmo de criptografia de dados baseado no sistema caótico do Atrator de Lorenz.

A criptografia embaralha letras, números e símbolos para codificar textos e somente pessoas autorizadas podem decodificar e recuperar o texto original. Tradicionalmente, a criptografia utiliza operações lógicas ou aritméticas simples para o embaralhamento. No entanto, hoje em dia boa parte dos algoritmos aplicados na criptografia já foram quebrados e esse duelo entre códigos estabelecidos e os que tentam quebrá-los dura mais de dois mil anos, tanto que a criptografia foi amplamente usada em operações militares, muitas batalhas e mesmo guerras, foram vencidas ou perdidas pelo sucesso ou fracasso da criptografia.

Pesquisas envolvendo a criptografia em sistemas caóticos já foram objeto de estudos e, nas últimas décadas, algoritmos de criptografia baseados na teoria do caos foram criados. Entretanto, esses algoritmos apresentavam severas limitações, tornando-os inseguros e demasiadamente lentos para aplicações comerciais. Mas, a combinação feita entre a

criptografia tradicional e sistemas caóticos permitiu melhorias na segurança e maior velocidade.

A teoria do caos explica o comportamento aparentemente errático e imprevisível de determinados sistemas naturais. Esses sistemas são não-lineares e seu comportamento depende fortemente de como são inicializados.

Nos sistemas caóticos, pequenas diferenças são fortemente amplificadas. Isto é bem ilustrado pelas correntes de ar atmosféricas, onde o bater de asas de uma borboleta em São Paulo pode produzir uma nevasca em moscou - o chamado efeito borboleta.

2.2. Criptografia caótica

O sistema caótico produz uma seqüência de números pseudo-aleatórios, e se os parâmetros iniciais do sistema caótico forem exatamente os mesmos, a seqüência será sempre a mesma. Na criptografia caótica, utilizada por muitos pesquisadores brasileiros, estas seqüências são utilizadas para embaralhar as mensagens.

As técnicas de criptografia consistem em transformar um arquivo ou documento em um formato que embora preserve a informação, seja inteligível (criptografada). Na transformação inversa, o arquivo ou documento retornar a sua forma original e para garantir que a transformação inversa seja realizada somente por alguém autorizado, é utilizada chaves e senhas nas transformações.

A teoria do caos para a física e a matemática é a hipótese que explica o funcionamento de sistemas complexos e dinâmicos. Em sistemas dinâmicos complexos, determinados resultados podem ser "instáveis" no que diz respeito à evolução temporal como função de seus parâmetros e variáveis. Estes sistemas existem com relativa abundância em problemas físicos e químicos, e são governados por equações relativamente simples (de fácil implementação computacional). Pela instabilidade que o sistema possui, onde uma mínima variação nas condições iniciais produz resultados completamente diferentes (resultando numa imprevisibilidade do sistema) torna-se interessante.

2.3. Sincronização do sistema caótico unificado

A sincronização de caos aplicada à comunicação tem sido objeto de intenso estudo em diversos países. 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: periodicidade, sensibilidade à 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.

Com base nisso, foi proposto um sistema criptográfico particularmente interessante, baseado num sistema caótico unificado, que estuda a previsão do tempo através do comportamento da atmosfera, que faz uma ponte entre o sistema de Lorenz, o sistema de Lu e o sistema de Chen, através da inclusão de um parâmetro α que varia de $0<\alpha<1$, que foi utilizado como a chave do sistema criptográfico. Em geral, para qualquer valor de α neste intervalo, o sistema unificado apresenta comportamento caótico.

Logo, as equações do sistema caótico unificado da Equação (1) são mostradas abaixo, onde x, y e z representam, respectivamente, o fluxo convectivo, a distribuição de temperatura horizontal e a distribuição de temperatura vertical e s, r e b, que representam os parâmetros

que intervêm nas equações, são, respectivamente, a relação entre a viscosidade e a condutividade térmica, a diferença de temperaturas entre o lado inferior e superior e a relação entre a altura e a largura do retângulo. Lembrando que, para esse tipo de sistema unificado, os parâmetros citados foram mantidos constantes, variando-se somente o parâmetro α, que é o parâmetro que caracteriza o sistema unificado (Lorenz, Lu e Chen).

$$\begin{cases} \dot{x} = (25 \propto +S)(y - x) \\ \dot{y} = -xz + (r - 35 \propto)x + (29 \propto -1)y \\ \dot{z} = xy - \frac{(\propto+b)}{3} z \end{cases} \quad (1)$$

2.3.1. Verificação do sincronismo

O sistema caótico usado para a verificação de sincronismo foi o Sistema de Lorenz, ou seja, considerou-se α=0. Em seguida, variaram-se somente as condições iniciais, criando, assim, outro sistema idêntico. A este dois sistema chamou-se de sistema MESTRE/ESCRAVO, que são as Equação (2) e Equação (3), respectivamente, como mostra as equações abaixo:

$$\begin{cases} \dot{x_1} = (25 \propto +S)(x_2 - x_1) \\ \dot{x_2} = -x_1 x_3 + (r - 35 \propto)x_1 + (29 \propto -1)x_2 \\ \dot{x_3} = x_1 x_2 - \frac{(\propto+b)}{3} x_3 \end{cases} \quad (2)$$

$$\begin{cases} \dot{y_1} = (25 \propto +S)(y_2 - y_1) + U1 \\ \dot{y_2} = -y_1 y_3 + (r - 35 \propto)y_1 + (29 \propto -1)y_2 + U2 \\ \dot{y_3} = y_1 y_2 - \frac{(\propto+b)}{3} z + U3 \end{cases} \quad (3)$$

2.3.2. Simulação

Tabela 1- Parâmetros de simulação do sistema unificado

r=28	b=8/3	s=10	α=0	U1=0	U2=0	U3=0

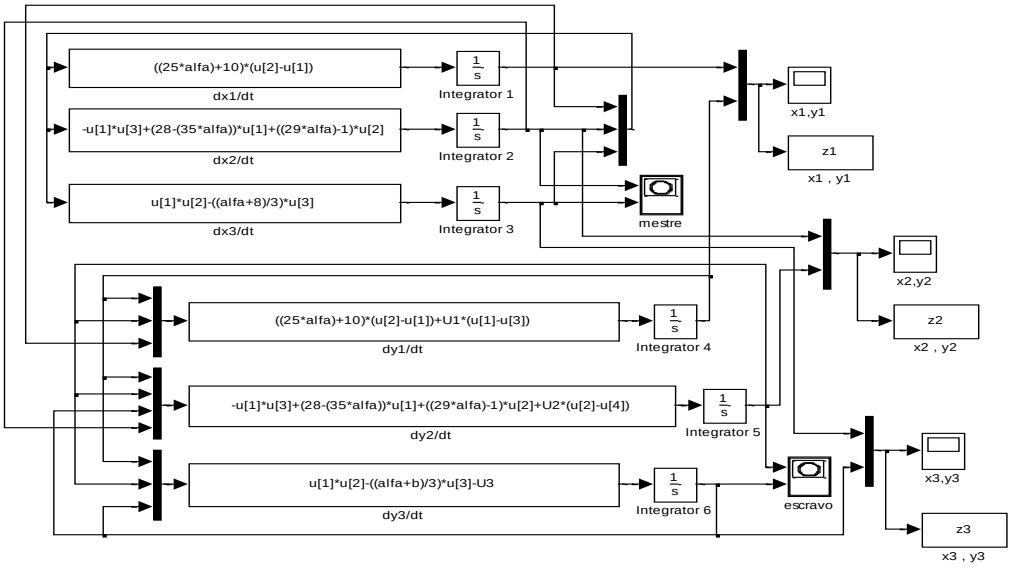

Figura 1- Diagrama de bloco do sistema unificado

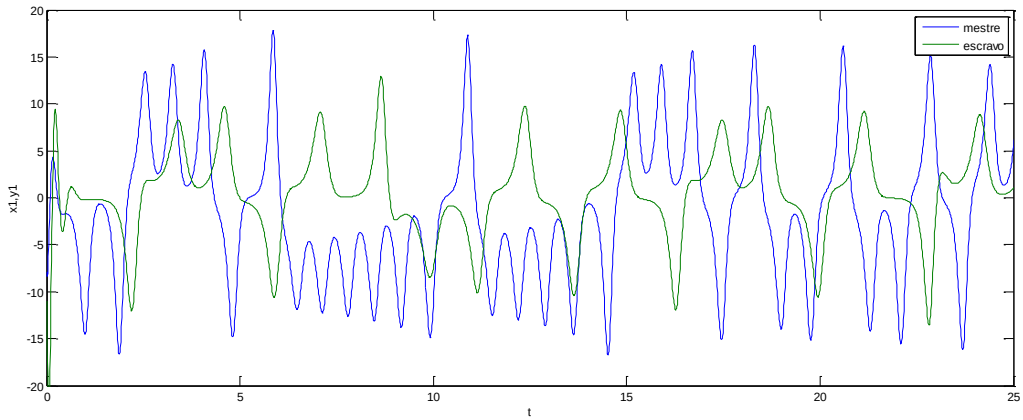

Figura 2- Gráfico de x1,y1 (mestre/escravo)

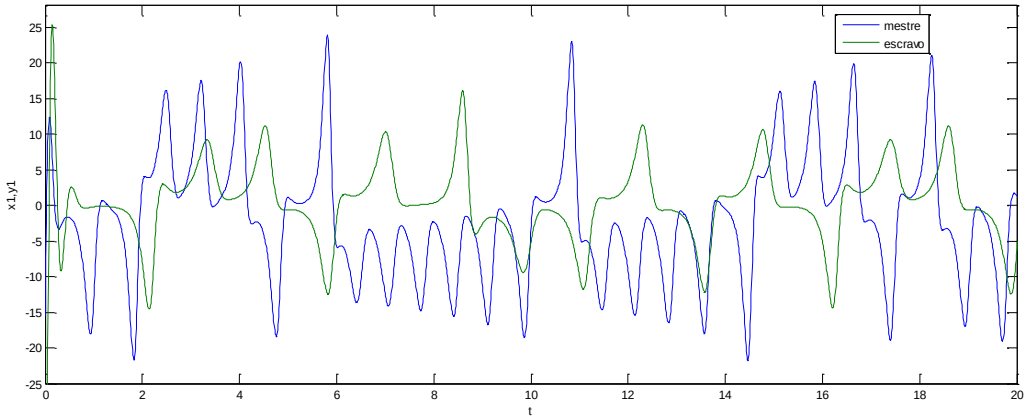

Figura 3- Gráfico de x2,y2 (mestre/escravo)

A Figura 2 e a Figura 3 mostram o comportamento de dois sistemas caóticos unificados idênticos com condições iniciais diferentes, sem a utilização de acoplamento ou controle. E como pode ser verificada, a alteração das condições iniciais do sistema, sem a aplicação de qualquer controle escalar e mantendo o restante dos parâmetros constantes, ocorre uma mudança no comportamento do mesmo, e essa mudança exemplifica uma das características do caos, que é a sensibilidade às condições iniciais. Observa-se, também, que os dois sistemas idênticos não entram em sincronismo. Logo, torna-se necessário a presença de um acoplamento ou controle escalar, para possibilitar a sincronização dos mesmos. Com isso, com o controle escalar U1, U2 e U3, foi possível colocar o sistema MESTRE/ESCRAVO em sincronismo, admitindo as mesmas condições iniciais. Como mostra os resultados computacionais abaixo.

3.3.2. Sincronismo do sistema caótico unificado

Tabela 2- Parâmetros de simulação do sistema unificado sincronizado

r=28	b=8/3	s=10	α=0	U1=-.6640	U2=-2.9605	U3=0

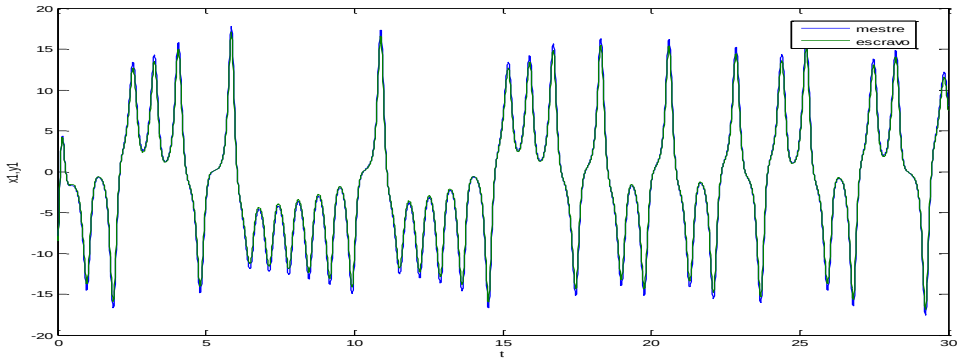

Figura 4-Gráfico de x1,y1(mestre/escravo)

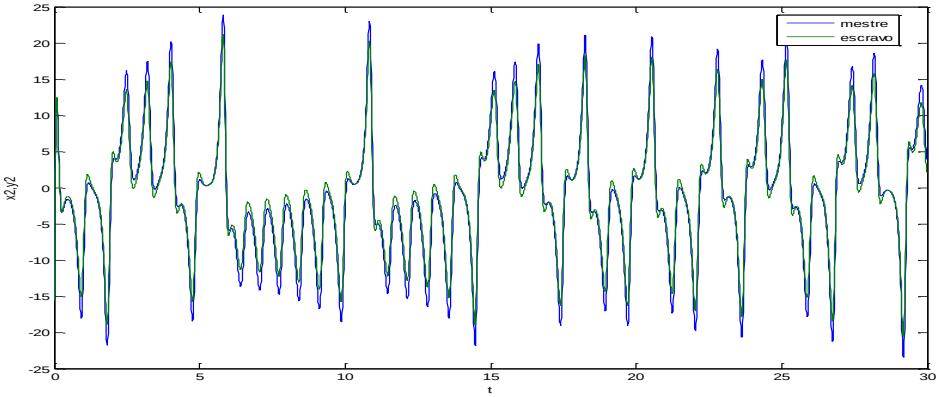

Figura 5 - Gráfico de x2,y2(mestre/escravo)

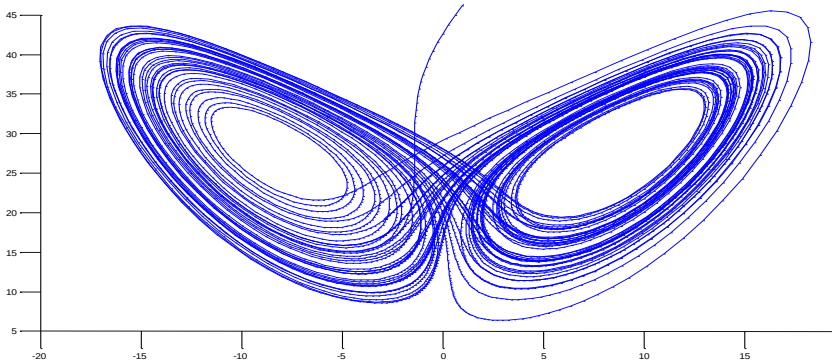

Figura 6 - Atrator de Lorenz, α=0

A Tabela 2 foi usada para fazer a simulação da sincronização do sistema, com o mesmo diagrama de bloco da Figura 1. A Figura 4 e a Figura 5 mostram o resultado da simulação do sistema via controle escalar. A Figura 5 mostra o fenômeno conhecido como efeito borboleta e os atratores estranhos. Com esse resultado, verifica-se a sincronização do sistema unificado, quando se admite valores não nulos para as variáveis de controle escalar.

2.3.3. Criptografia do sistema caótico unificado:

A técnica utilizada para atender à demanda por segurança e privacidade é a criptografia. O objetivo é transmitir as informações de uma maneira que somente o destinatário possa compreender, obtendo-se segurança das transmissões de dados. Assim, a mensagem distribuída em um canal de comunicação público passa a ser não inteligível aos usuários para os quais a mesma não foi endereçada ou autorizada. Neste caso, o transmissor responsável pela criptografia deve gerar uma palavra (conjunto de bits) secreta, conhecida como chave.

Através de um algoritmo de criptografia, a chave é usada para embaralhar o texto a ser enviado, sendo a mensagem criptografada resultante conhecida como criptograma. Para a recuperação da mensagem original, no receptor, faz-se necessária a utilização da mesma chave, sendo a mensagem praticamente inviolável para quem não possuí-la. Portanto, uma vez que a chave tenha sido escolhida no transmissor, ela deve ser transmitida ao receptor.

Logo, será desenvolvido um modelo de encriptação que dá uso à imprevisibilidade explícita na moderna "Teoria do Caos", um modelo não-linear que explica o funcionamento de sistemas complexos e dinâmicos, que terá como base o sistema caótico unificado, como mostra o conjunto de equações abaixo.

$$\begin{cases} \dot{x_1} = (25 \propto +S)(x_2 - x_1) \\ \dot{x_2} = -x_1 x_3 + (r - 35 \propto)x_1 + (29 \propto -1)x_2 \ + Am \\ \dot{x_3} = x_1 x_2 - \frac{(\propto + b)}{3} x_3 \end{cases} \quad (4)$$

$$\begin{cases} \dot{y_1} = (25 \propto +S)(y_2 - y_1) + U1 \\ \dot{y_2} = -y_1 y_3 + (r - 35 \propto) y_1 + (29 \propto -1) y_2 + U2 \\ \dot{y_3} = y_1 y_2 - \frac{(\propto + b)}{3} z + U3 \\ m = \frac{1}{A}(\dot{x_2} + (r - 35 \propto) y_1 - y_1 y_3 + (29 \propto -1) y_2) \end{cases} \quad (5)$$

Com a Equação (4) (transmissor) e a Equação (5) (receptor), será feita uma aplicação da sincronização e da criptografia de sistemas caóticos em comunicação. O processo consiste em duas etapas distintas: a sincronização dos osciladores e a transferência do sinal caótico que carrega a mensagem. Nas equações citadas, *m* é a mensagem, *A* é uma constante, que tem o objetivo de diminuir a amplitude da mensagem em relação ao sinal caótico, α é um parâmetro, e U1, U2, e U3 são sinais de controle. Na primeira etapa, os sistemas transmissor e receptor são sincronizados na forma mestre/escravo (item 3.3.2), onde o sistema receptor é controlado e sua trajetória é levada à do sistema transmissor, de forma que o erro entre as trajetórias seja levado a zero. Na segunda etapa, inicia-se com o transmissor, o processo de encriptação e transmissão do sinal $\dot{x_2}$, que é recebido e decriptado na quarta equação do receptor. No contexto da criptografia, o parâmetro α trabalha como a chave do sistema, cuja estrutura é pública. Dessa forma, o espaço da chave é o intervalo [0, 1].

Para decifrar a mensagem escondida, é necessário sincronizar emissor e receptor do sinal caótico. Uma vez obtida essa sincronização, pretende-se fazer o processo de criptografia do mesmo sistema dinâmico, no caso o sistema caótico unificado.

No geral, quando se gera a transmissão de sinais caóticos, falta o essencial: camuflar a mensagem que se quer enviar. Além do mais, emissor e receptor têm de ser sistemas caóticos semelhantes, sendo que, neste caso, ambos têm de estar a gerar sinais caóticos, e de forma independente. O que se faz, em seguida, é adicionar a mensagem ao emissor, quer isto dizer, a mensagem vai ser embebida na onda portadora caótica. Qualquer utilizador externo não autorizado detectará apenas ruído, porque o caos tem características semelhantes ao ruído.

Para o receptor extrair a mensagem enviada, injeta-se parte do caos no receptor, de modo a que emissor e receptor fiquem sincronizados. A sincronização faz que o emissor e o receptor gerem o mesmo sinal caótico.

3. CONSIDERAÇÕES FINAIS:

A pesquisa bibliográfica e as implementações de sistemas, a nível de simulação, vem contribuindo bastante na solidificação e sustentação do posterior desenvolvimento deste trabalho. Visto que, o trabalho proposto teve o objetivo de fazer um estudo sobre o sistema caótico e suas aplicações em sistemas dinâmicos e complexos não lineares, com parâmetros variáveis. Isto fora alcançado através das simulações feitas com os recursos do SIMULINK e MATLAB apresentadas neste trabalho. Enfatizou-se peculiaridades nos sistemas estudados, observando comportamento caótico e suas características, como a presença de atratores, a presença de sincronismo quando adicionado um controle escalar. Através da aplicação do controle escalar, obtivemos a sincronização do sistema caótico unificado. Nesse caso, a sincronização ocorreu de maneira rápida e eficiente.

Foi confirmado, também, por meio das simulações o que prega a teoria, que variando as condições iniciais que regem cada equação dos sistemas estudados, o mesmo vai perdendo a estabilidade e passando a oscilar cujo comportamento é de grande interesse na Engenharia.

Estudos baseados no processo de encriptação revelaram que, tanto a imagem quanto o texto encriptados tornam-se ininteligíveis após o processo de sincronismo e encriptação, sendo recuperados com absoluta perfeição no receptor. Em trabalhos futuros pretende-se aumentar o nível de segurança do algoritmo através da utilização de parâmetro α variável, usando a criptografia

4. AGRADECIMENTOS

Ao orientador Professor José A. L. Barreiros pelo apoio e orientação na elaboração desta pesquisa.

Ao Laboratório de Controle (LACUS) da Faculdade de Engenharia Elétrica da Universidade Federal do Pará (UFPA) pelo fornecimento do espaço para o desenvolvimento desta pesquisa.

Ao CNPQ (Conselho Nacional de Desenvolvimento Cientifico e tecnológico) que financiou esta pesquisa.

5. REFERÊNCIAS BIBLIOGRÁFICAS:

Z. Cao and Z. Zheng, “The chaos of nonlinear moving system for the synchronous motor,” in *Proc. China Society Electronic Engineering*, vol. 18, May 1998, pp. 318–322.

Z. Li and J. B. Park *et al.*, “Bifurcation and chaos in a permanent-magnet synchronous motor,” *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 3, pp. 383–387, Mar. 2002

Z.Li, B.Zhang and Z.Y.Mao, “Strange Attractors in Permanent-magnet Synchronous Motors”, Proc. *Of* the IEEE 1999 International Conference on Power - Electronics and Drive Systems, PEDS’99. Hong Kong. pp.150-1 *55*

SYNCHRONIZATION OF CHAOTIC SYSTEM

Abstract: *The construction of this paper objective to analyze technical controller design with domains in state space coincident with those chaotic attractors and techniques in order to force them to enter into pre-specified behavior. The control of chaos can be understood as the use of small perturbations to stabilize unstable periodic orbits, immersed in a chaotic attractor. Given that the chaos can occur in many natural processes, the idea of chaotic behavior is controlled by small perturbations of certain physical parameters, allows this type of behavior is desirable in many applications. Based on this literature, was made a study of*

the synchronism of a unified chaotic system, through of two systems (master-slave), who with the help of MATLAB software, it was possible to simulates them and to obtain time answers and the phase space of variables that governing each equation. Thus, was found that, with the variation of control parameters chosen for the system, the same acquires different behaviors for each given value, in other words for some values, the system has chaotic behavior, characterizing the nonlinearity of system and for others, periodicity.

***Key-words**: Nonlinear systems, Chaos, Synchronization, Cryptography.*