AUTÔMATOS CELULARES COM BORDA PSEUDOALEATÓRIA APLICADOS À CIFRAGEM DE IMAGENS DIGITAIS

MENEZES, Felipe A.[1]; SILVA, Eduardo C.[2]; LIMA, Danielli A.[3]

RESUMO: Tendo em vista o crescimento tecnológico a partir do século XX, diversas tecnologias e meios de comunicação foram criados, o acesso a informação nunca foi tão simples. Devido a isso, podemos nos comunicar através de textos, imagens, áudios com pessoas que estejam do outro lado do mundo instantaneamente. Com isso é necessário obter uma forte segurança dessa comunicação, uma vez que dependendo do conteúdo da informação, poderá trazer prejuízos a um indivíduo ou a um grupo. Os algoritmos de criptografia de dados foram essenciais para a segurança, a criptografia em si é utilizada pela humanidade desde tempos remotos. Tratando-se de criptografia de imagem é sempre necessário que seja rápida, segura e de baixo custo de processamento. Os autômatos celulares têm grande aplicabilidade em criptografia, uma vez que são sistemas dinâmicos emergentes e são associados à teoria do caos, propriedades adequadas a bons sistemas criptográficos. Este trabalho tem como objetivo otimizar o algoritmo de criptografia Border Chaotic Cellular Automata (BCCA) a fim de obter resultados mais satisfatórios através da aplicação de uma borda pseudoaleatória gerada por uma regra caótica de autômatos celulares.

Palavras-chave: Autômatos celulares unidimensionais, teoria do caos, criptografia de imagens, segurança da informação.

INTRODUÇÃO

A Era Digital (também chamada de Era da Informação ou Era Tecnológica) surgiu em meados de 1980. As tecnologias que eram originalmente para o Estado, empresas e pequenas partes privilegiadas da população, começaram a ser pessoais. Os meios de comunicação se desenvolveram a pontos jamais imaginados. Devido a esse incrível avanço, métodos para a proteção da privacidade e segurança da informação foram implementadas na computação.

A criptografia, que vem sendo utilizada pela humanidade desde tempos remotos, foi uma solução para manter a segurança dos usuários. Entretanto, escolher um método para criptografar a informação é um desafio. Para isso, é necessário um algoritmo que

[1] Estudante do curso de superior de Tecnologia em Análise e Desenvolvimento de Sistemas no Instituto Federal do Triângulo Mineiro (IFTM), Patrocínio, Minas Gerais; E-mail: felipeam01@hotmail.com;
[2] Professor coorientador no Instituto Federal do Triângulo Mineiro (IFTM), Patrocínio, Minas Gerais, E-mail: eduardocassiano@iftm.edu.br;
[3] Professora orientadora no Instituto Federal do Triângulo Mineiro (IFTM), Patrocínio, Minas Gerais, E-mail: danielli@iftm.edu.br.

possa cifrar a mensagem com tempo de execução baixo, pouco custo e segurança, de tal forma que a mensagem cifrada possa ser decifrada na mensagem original. A maioria dos algoritmos de criptografia clássicos Advanced Encrytion Standard (AES) e Data Encryption Standard (DES) largamente utilizados são implementados, de maneira geral, de forma sequencial aumentando o tempo de processamento (DAEMEN, 2005), (ZEGHID, 2007). Desse modo, a utilização de autômatos celulares em criptografia é uma forma simples de processar os dados em paralelo para solucionar o problema de tempo de execução (LIMA, 2012).

Os autômatos celulares (ACs) podem ser definidos como um grupo de unidades processadoras simples (células) que interagem entre si e que ao longo do tempo, podem apresentar um comportamento global (LIMA, 2012). Assim pode-se perceber que os ACs ganharam uma grande importância em sua aplicação e demonstraram resultados eficientes como demonstrados nos trabalhos de modelagem de sistemas naturais ou biológicos (LIMA, 2014), físicos (FELICIANI, 2016), e até mesmo na proposição de sistemas de controle de robôs (FERREIRA, 2014), (LIMA, 2017). Duas das principais vantagens em se aplicar modelos baseados em ACs reside na sua simplicidade de implementação e também na sua capacidade de processar dados em paralelo (VASANTHA, 2015).

Os principais objetivos deste estudo são: (i) estudar a teoria sobre autômatos celulares, criptografia e algoritmos relacionados; (ii) propor uma forma de otimizar o BCCA pela aplicação de uma regra do tipo caótica; (iii) analisar, executar e otimizar o algoritmo Border Chaotic Cellular Automata (BCCA) proposto em (SILVA; SOARES; LIMA, 2016); (iv) comparar e analisar se o algoritmo proposto é realmente eficiente em relação ao seu modelo anterior BCCA e aos demais modelos precursores.

FUNDAMENTAÇÃO TEORICA

Os algoritmos DES e AES são os mais amplamente utilizados e são considerados inerentemente sequenciais (STINSON, 2006) com pequenos trechos que podem ser realizados de forma concorrente (YANG, 2009). Autômatos Celulares são estruturas de tamanho finito representadas por uma cadeia de células que podem interagir entre si e evoluir através de regras de transição. Possuindo aplicabilidade na

criptografia (GUTOWITZ, 1995), (OLIVEIRA, 2004) e (OLIVEIRA, 2010), os ACs destacam-se pela capacidade de processar dados em paralelo, ideal para grandes quantidades de dados, e pela simplicidade de seus componentes (WOLFRAM, 2002). Adaptar e otimizar o modelo criptográfico BCCA altamente paralelizável, através da aplicação de uma borda pseudoaleatória gerada por uma regra caótica (LI, 1991), orientado às imagens digitais e utilizando ACs unidimensionais é a principal proposta deste trabalho. O modelo aqui proposto visa a confidencialidade dos dados transmitidos, tal como garantir o direito à privacidade digital. Para isso, os testes do modelo BCCA foram apresentados para mostrar o potencial de cifragem do método aqui proposto, uma vez que ambos se baseiam no cálculo de pré-imagens para a realização da cifragem. Porém, o modelo BCCA não apresenta a aplicação de uma regra caótica nos limites da mensagem que está sendo enviada, diminuindo a qualidade da cifragem.

O trabalho proposto em SILVA; SOARES; LIMA (2016) denominado BCCA foi altamente baseado em um modelo precursor que utiliza ACs unidimensionais (GUTOWITZ, 1995). As evoluções *backward* e *forward* representam, respectivamente, as etapas de cifragem e decifragem. Todavia, esse modelo apresentou uma otimização para diminuir o contínuo aumento do texto cifrado, uma desvantagem observada nos trabalhos (GUTOWITZ, 1995) e (OLIVEIRA, 2004). As regras (chaves) são sensíveis a um dos extremos da vizinhança (GUTOWITZ, 1995) e com característica de dinâmica caótica. O BCCA contempla adição de uma borda do lado inverso ao da sensitividade da chave criptográfica que estiver sendo utilizada. Esta borda foi a responsável por garantir que o reticulado final não aumentasse de tamanho para este lado, e está apresentada na Figura 1. A borda no BCCA foi uma sequência caótica representada por parte da chave – regra 30. Por outro lado, no trabalho que está sendo desenvolvido, a borda representa uma sequência pseudoaleatória gerada através de uma regra também caótica (LI, 1991). A Figura 2 representa a evolução *forward* da regra 110, que representa um AC caótico, sendo este adequado à sistemas de criptografia. Neste caso, ao invés de se utilizar parte da regra conhecida pelo emissor e receptor, será utilizado a sequência pseudoaleatória gerada pela regra 110, destacada em vermelho na Figura 2. Embora o tamanho da mensagem enviada seja aumentado, esse aumento será compensado pelo aumento da caoticidade, propriedade desejável em qualquer sistema criptográfico.

Tanto no modelo precursor BCCA, quanto no modelo apresentado neste trabalho, todas as linhas da imagem são cifradas de maneira paralela, sendo que a cifragem de uma linha não interfere na cifragem da linha posterior, tornando o processo altamente paralelizável.

Figura 1: Modelo proposto por (SILVA; SOARES; LIMA, 2016) denominado BCCA.

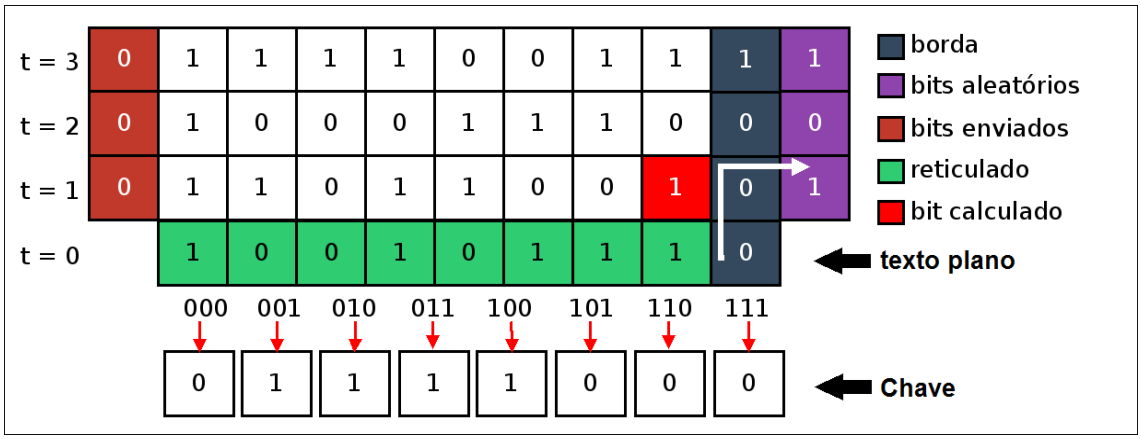
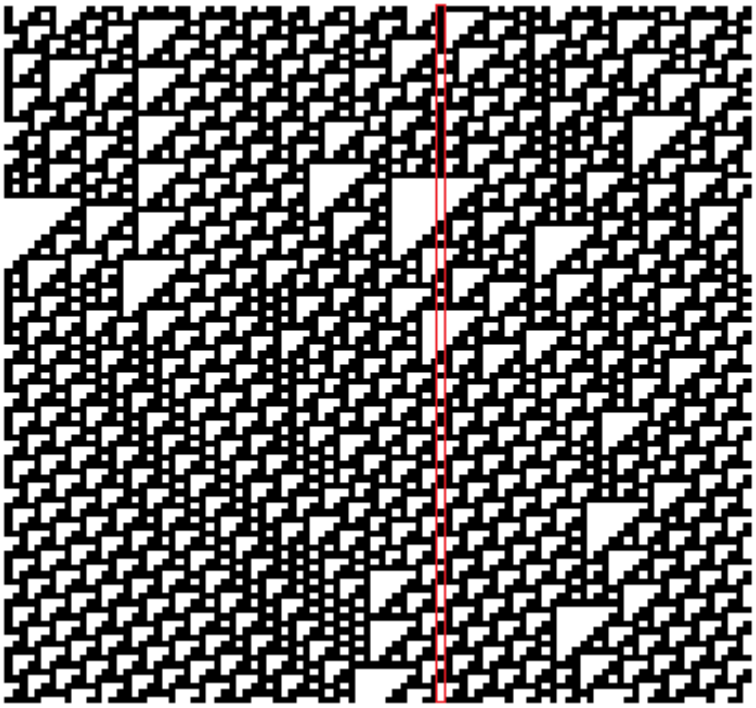


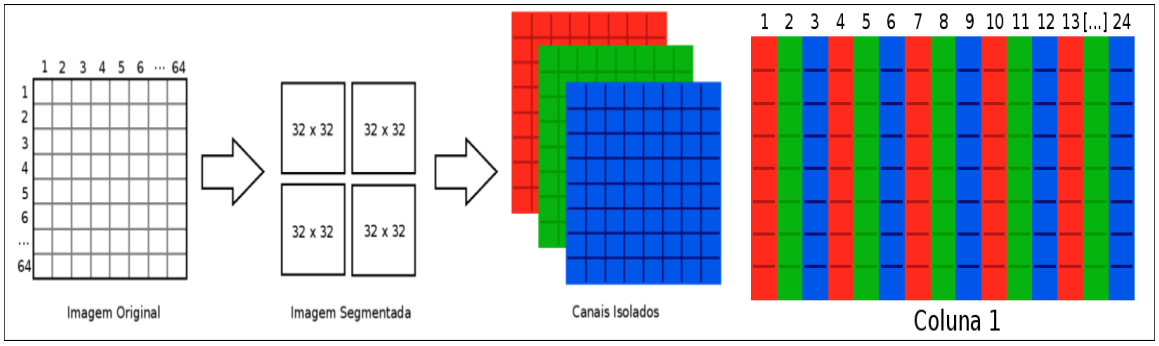
Figura 2: Evolução forward de um AC por 100 passos de tempo através da regra 110.



Para a aplicação do modelo em imagens coloridas de dimensão *m* x *n*, que apresentam uma paleta de cores mais complexa no padrão RGB, um pré-processamento inicial se faz necessário antes de aplicar o método criptográfico aqui proposto. Esse pré-

processamento é um embaralhamento que separa os bits de cada descritor e realiza concatenações formando novos blocos para encriptação. A Figura 3 apresenta essa etapa de pré-processamento, e divide uma imagem em *4* partes distintas de tamanhos idênticos. Posteriormente, concatena-se de forma alternada cada um dos bits separados em cada seção RGB. Em resultado disso, tem-se uma nova sequência de bits, que representa matrizes referentes à cada uma das colunas dos blocos. Neste exemplo, tem-se um total de *4* x *32* matrizes de bits, que podem ser cifradas separadamente pelo algoritmo aqui proposto.

Figura 3: Primeiros passos da cifragem colorida.

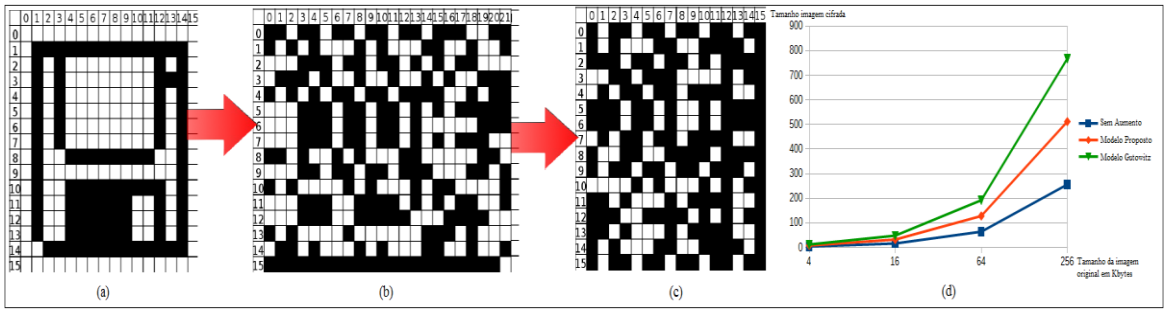


RESULTADOS PRELIMINARES DO BCCA

Os testes preliminares realizados no modelo BCCA tiveram por finalidade verificar os padrões de criptografia gerados após a cifragem de dados. Quanto mais distante for o padrão encontrado entre a imagem original e a cifrada, maior foi a qualidade da cifragem. Um primeiro experimento foi gerado para contrastar a imagem cifrada pelo algoritmo proposto em (GUTOWITZ, 1995) e o modelo BCCA. O resultado deste experimento pode ser observado na Figura 4. Como é possível perceber, a imagem final gerada pelo algoritmo de (GUTOWITZ, 1995) tem dimensão D muito superior a imagem original, o que dificulta muito a transmissão dessa informação ($D = N_1 \times (N_2 + T \times 2 \times r)$). Por outro lado, a imagem gerada pelo BCCA tem dimensões mais próximas a da imagem original ($D = N_1 \times (N_2 + T \times r)$). Essas propriedades seriam mantidas no algoritmo aqui proposto, exceto pelo fato de que o tamanho da chave também seria aumentado. Além disso, toda imagem que é dada como entrada, fornece

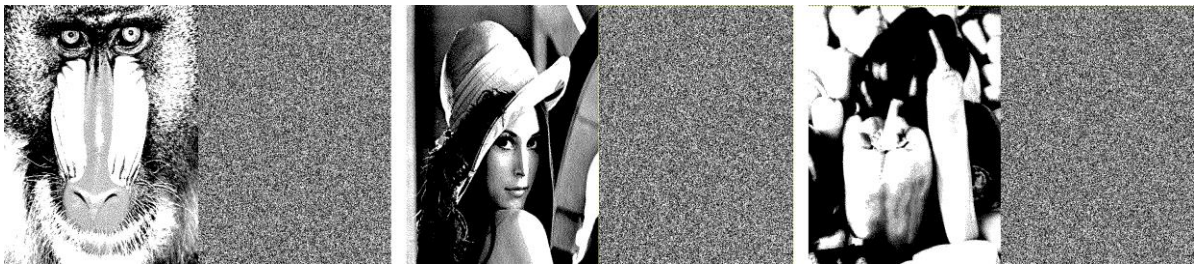
uma imagem cifrada como saída, diferentemente do algoritmo proposto em (LIMA, 2005).

Figura 4: (a) Imagem original. (b) Imagem cifrada algoritmo de (GUTOWITZ, 1995). (c) Imagem cifrada pelo algoritmo proposto no BCCA. (d) Gráfico de comparação do tamanho das imagens cifradas para cada um dos modelos.



Na Figura 5 são apresentadas imagens clássicas em preto e branco cifradas pelo algoritmo BCCA.

Figura 5: Imagens clássicas cifradas pelo algoritmo BCCA.



CONCLUSÕES E TRABALHOS FUTUROS

Cifrar e decifrar imagens preto e branco, além das imagens RGB foram objetivos alcançados com o uso do modelo de criptografia baseado em ACs chamado BCCA, contudo é possível otimizá-lo pelo do emprego de uma borda caótica. O modelo a ser desenvolvido tem como base a criptografia de (GUTOWITZ, 1995) bem como o modelo BCCA proposto em (SILVA; SOARES; LIMA, 2016). Todos esses modelos são baseados em ACs unidimensionais e é possível, a partir de algumas adaptações, aplicá-los em imagens digitais. Além de interromper o crescimento constante do modelo de (GUTOWITZ, 1995), o BCCA é um sistema capaz de cifrar qualquer texto de entrada com a introdução da borda fixa, diferentemente do trabalho precursor (OLIVEIRA, 2004). Como proposta deste trabalho será introduzida uma sequência

pseudoaleatória - gerada através de uma regra caótica (LI, 1991) - no modelo BCCA (SILVA; SOARES; LIMA, 2016). Dessa forma, espera-se obter melhores resultados, em relação ao modelo de (GUTOWITZ, 1995), (OLIVEIRA, 2004) e (SILVA; SOARES; LIMA, 2016). Para validação do modelo, testes em larga escala serão utilizados empregando-se a análise de perturbação, entropia de chaves e histograma de cores.

REFERÊNCIAS

DAEMEN, J.; RIJMEN, V. Rijndael/aes. **In: Encyclopedia of Cryptography and Security.** Springer US, 2005. p. 520-524.

FELICIANI, C.; NISHINARI, K. An improved Cellular Automata model to simulate the behavior of high density crowd and validation by experimental data. Physica A: **Statistical Mechanics and its Applications**, v. 451, p. 135-148, 2016.

FERREIRA, G. B. S; VARGAS, P. A.; OLIVEIRA, G. M. B. An improved cellular automata-based model for robot path-planning. In: **Conference Towards Autonomous Robotic Systems.** Springer International Publishing, 2014. p. 25-36.

GUTOWITZ, H. (1995). **Cryptography with dynamical systems**. Kluwer Academic Press.

LI, W. **Parameterizations of cellular automata rule space**. Santa Fe Institute TR, 1991.

LIMA, D. A. **Modelo criptográfico baseado em autômatos celulares tridimensionais híbridos.** 2012. 224 f. Dissertação (Mestrado) - Curso de Mestrado em Ciência da Computação, Faculdade de Computação FACOM, Universidade Federal de Uberlândia, Uberlândia, 2012.

LIMA, D. A.; OLIVEIRA, G. M. B. A cellular automata ant memory model of foraging in a swarm of robots. **Applied Mathematical Modelling**, v. 47, p. 551-572, 2017.

LIMA, H. A.; LIMA, D. A. Autômatos celulares estocásticos bidimensionais aplicados a simulação de propagação de incêndios em florestas homogêneas. **In:** Workshop of Applied Computing for the Management of the Environment and Natural Resources. 2014.

LIMA, M. J. L. (2005); **Criptografia baseado no cálculo genérico de pré-imagens de autômatos celulares**. Master's thesis, Universidade Presbiteriana Mackenzie. 2005.

OLIVEIRA, G. M., Martins, L. G., Alt, L. S., and Ferreira, G. B. (2010). Exhaustive evaluation of radius 2 toggle rules for a variable-length cryptographic cellular automata-based model. **In Cellular Automata**, pages 275–286. Springer.

OLIVEIRA, G. M. B., COELHO, A., and MONTEIRO, L. (2004). Cellular automata cryptographic model based on bi-directional toggles rules. Int. J. of Modern Physics C.

SILVA, E. C.; SOARES, J. A. J. P.; LIMA, D. A. Autômatos celulares unidimensionais caóticos com borda fixa aplicados à modelagem de um sistema criptográfico para imagens digitais. **Revista de Informática Teórica e Aplicada**, v. 23, n. 1, p. 250-276, 2016.

STINSON, D. (2006). **Cryptography: Theory and Practice**. Chapman & Hall/CRC, 3rd edition.

VASANTHA, S.; SHIVAKUMAR, N.; RAO, D. S. A new encryption and decryption algorithm for block cipher using cellular automata rules. **International Journal**, v. 130, 2015.

WOLFRAM, S. (2002). **A New Kind of Science**. Wolfram Media - (1st edition): 1197 2006-09-19T07:35:05.000+0200.

YANG, Y. S. et al. Parallel and pipeline processing for block cipher algorithms on a network-on-chip. **In: Information Technology**: New Generations, 2009. ITNG'09. Sixth International Conference on. IEEE, 2009. p. 849-854.

ZEGHID, M. et al. A modified AES based algorithm for image encryption. **International Journal of Computer Science and Engineering**, v. 1, n. 1, p. 70-75, 2007.