DINCON 2017
CONFERÊNCIA BRASILEIRA DE DINÂMICA, CONTROLE E APLICAÇÕES
30 de outubro a 01 de novembro de 2017 – São José do Rio Preto/SP

Criptografia de Imagens Baseada no Caos e na Dinâmica dos Autômatos Celulares

Polycarpo Souza Neto[1]

Laboratório de Teleinformática (LATIN),

Departamento de Teleinformática, Universidade Federal do Ceará (UFC), Fortaleza, CE

George André Pereira Thé[2]

Programa de Pós-graduação em Engenharia de Teleinformática (PPGETI),

Departamento de Teleinformática, Universidade Federal do Ceará (UFC), Fortaleza, CE

Resumo.O propósito da criptografia de dados é possibilitar a comunicação em um canal inseguro, de tal forma que nenhuma outra entidade consiga decifrar o dado.Uma abordagem interessante para este segmento são os Autômatos Celulares (AC), estudados por sua capacidade de processar grandes volumes de dados em paralelo.A metodologia aqui empregada é dividida empré-processamento da informação, evolução das regras de transição e pós-processamento, onde são corrigidos os erros e é aplicado o algorítimo reverso. Neste experimento são feitos testes com autômatos celulares reversíveis e irreversíveis, sendo feito o cálculo da entropia antes e depois da aplicação do método.

Palavras-chave. Criptografia, Autômatos celulares, Entropia, Caos

1 Introdução

Com a expansão da tecnologia, em especial a internet, aplicações que fazem uso de técnicas de processamento de imagens têm crescido bastante. No entanto, a maior barreira no desevolvimento de serviços e novas tecnologias que fazem uso de imagens digitais têm sido a segurança. Levando isso em consideração, a solução encontrada foi usar algoritmos de criptografia para o envio dos dados [7].

A implementação das técnicas de criptografia e seu aperfeiçoamento levaram a descoberta de modelos como *Data Encryption Standard* (DES), Idea *Data Encryption Algorithm* (IDEA), e o algoritmo desenvolvido por Rivest, Shamir e Adleman (RSA) [11]. No entanto, em oposto ao que acontece com strings, os dados de uma imagem digital possuem características especiais, como alta redundância e correlação entre píxels, além de terem uma grande pilha de dados, o que torna modelos criptográficos tradicionais inviáveis, dado o custo computacional com que são processados [2].

[1]policarponeto.pn@gmail.com
[2]geothe@hotmail.com

Como alternativa aos modelos tradicionais surge a construção de sistemas fundamentados no caos [10] e no estudo dos autômatos celulares, estudados por sua capacidade de processar grandes volumes de dados em paralelo [7]. Na primeira parte da metodologia deste trabalho propõe-se que uma imagem seja usada como parâmetro de entrada e passe por um pré-processamento, que consistirá numa preparação antes da aplicação de regras dos AC. Posteriormente a esse passo, haverá a evolução das regras dos autômatos e geração de um criptograma, que será a imagem que foi cifrada e que obedece a um código e a uma lógica pré-determinada para depois passar correção de erros e decriptagem, que fazem parte do pós-processamento.

2 Propósito

Neste trabalho, o propósito é a busca por um modelo criptográfico onde não hajam padrões conhecidos no criptograma, o que impossibilita ao criptoanalista reverté-lo sem conhecimento das funções de transição e das iterações de cada uma, o que justifica então utilizar um modelo baseado na criptografia caótica e na evolução dos autômatos celulares.

3 Fundamentação Teórica

3.1 Autômatos Celulares (AC)

Os AC podem ser definidos como sendo uma quadrupla $\gamma = [L, z, \sigma, \phi\ ]$, onde L é o lattice ou formato do autômato, z são os estados assumíveis, para c sendo o estado em si, o σ é a vizinhança que depende do raio r e ϕ é a regra de transição [8]. Autômatos celulares são um modelo simples para física, para representação de sistemas biológicos e computacionais. A característica distinta dos AC é que regras subjacentes simples podem funcionar de forma muito eficiente por comportamentos complexos que podem ser a base para desenvolvimento de algorítimos criptografico baseados no caos [10].

Autômatos celulares são a modelagem matemática de um sistema, esse com entradas e saídas discretas. Os AC representam o comportamento sequencial de uma série de células interligadas que estão dispostas de forma regular, cada um com um conjunto finito de valores possíveis. Usando AC, um algorítimo criptográfico deve evoluir em passos de tempo discretos e o valor de um determinado célula (estado local) é afetada pelos valores das célula em sua mais próxima vizinhança no passo anterior [5], de acordo com uma função conhecida como a regra ϕ.

3.2 Regras ou funções de transição dos AC

A alteração dos estados celulares ocorrem de forma síncrona para todas as células na rede [10]. Adotando a notação em que c é o estado da *i-ésima* célula num tempo t, na próxima etapa, num tempo $t + 1$, o estado da célula será c(t+1).Essa relação pode ser vista em (1):

$$c_i(t+1) = \phi[c_i - 1(t), c_i(t), c_i + 1(t)], \tag{1}$$

em (2) temos uma dada regra de transição simples [11] e (3) a regra complementar pelo qual podemos recuperar a informação [1].

$$c_i(t+1) = \phi[c_i - 1(t) + c_i(t) + c_i + 1(t)] mod 2 \quad (2)$$

$$c_i(t+1) = \phi[\overline{c_i - 1(t)} + \overline{c_i(t)} + \overline{c_i + 1(t)}] mod 2 \quad (3)$$

3.3 Caos determinístico

O comportamento instável de um AC num sistema determinístico influenciado por um número razoável de fatores é o que definimos como caos determinístico. As características que determinam o caos são a transitividade, os pontos temporalmente periódicos densos [1] e a dependência das iterações anteriores e das condições iniciais, que gera uma amplificação dos erros existentes e um comportamento pseudo-aleatório [6].

3.4 Reversibilidade do AC

Existem alguns AC reversíveis que procedem de um estado desordenado para um ordenado, isto é, de um estado de alta entropia para um estado de baixa entropia [11]. Como um contraste, autômatos celulares irreversíveis podem exibir uma diminuição no número de possíveis configurações ao longo do tempo (compressão de estados), portanto, uma diminuição da entropia [11].

A reversibilidade em autômatos celulares é um efeito raro mas acontece em alguns AC, como o caso das regras 15, 51, 85, 170, 204 e 240. No caso da regra 15 há condição inicial aleatória no domínio de transição. Um AC pode começar em qualquer linha e ir para trás em passos de tempo usando a regra rotação de 180º.Com isso sua regra comutativa é a Regra 85 (e, portanto, também reversível). Em seguida, a regra considerada seria a 204. O mesmo que é válido para a regra 15 e 85, acontece agora onde aplicando a rotação, sua regra comutativa é a 51. Por último, o mesmo raciocínio é usado para o uso do par de 170 e regra 240 [11].

4 Métodos

Na metodologia empregada, foram feitos testes com duas imagens do tipo *bitmap*(.bmp), em escala de cinza e de dimensões 256x256. No entanto, para facilitar o tratamento pelo algorítimo, a imagem é convertida em um vetor de 1x65536.

4.1 Pré-processamento

O pré-processamento consiste em preparar a imagem para que o algoritmo de correção de erros venha a corrigi-los. Os erros serão introduzidos pelo uso de regras não reversíveis completamente (pares 43 - 113 e 212 - 142). Num primeiro estágio se transforma a matriz relativa a composição da imagem em um vetor, onde serão inseridos bits de paridade. Na redundância de informação, bits extras são armazenados ou transmitidos junto a informação, sem que contenham qualquer informação útil. Esses bits extras têm, como fim

base a detecção de erros [4]. O bit extra indica apenas se o número de bits com valor 1 nos restantes n bits é par. Bits de paridade servem para detecção de falhas simples.

4.2 Evolução nos AC

Com a adição dos bits de paridade, o conjunto de informações composto pela imagem e bits de paridade encontra-se pronto para ser criptografado. Agora este conjunto pode ser visto como um autômato celular. As regras de evolução dos AC neste trabalho foram usadas na seguinte ordem, tanto no processo de encriptagem como na decriptagem. Como pode ser visto na Tabela 1:

Tabela 1: Regras para evolução.

Regra	Regra Complementar	Iterações
15	85	1
51	51	5
170	240	2
204	204	4
43	113	1
212	142	1

4.3 Pós-processamento

O criptograma resultante segue para o algoritmo de correção de erros. Esta etapa do pós-processamento consiste na remoção dos caracteres extras que foram adicionados durante a etapa de pré-processamento. Como código corretor de erro foi usado um código de bloco binário do tipo FEC (*Foward Error Correction*). Um código desse tipo funciona com k bits de informação. A codificação atribui a isso uma palavra código de n bits codificados, com $n>k$. A taxa de código é a divisão da quantidade de informação útil pelo tamanho do bloco, ou seja, $R= k/n$ [4]. A palavra código de um código de bloco (n,k) pode ser expressa por um vetor de comprimento n descrito descrito como:

$$C = [C_0 C_1 ... C(n-1)] = vG, \tag{4}$$

em que v é um vetor de dados de tamanho k e G é uma matriz (k,n) [4]. Como cada palavra código é gerada do produto do vetor pela matriz geradora, ela é então a matriz geradora do código. No caso deste trabalho, para cada *byte*, metade da informação será de bits extras e metade informação real, útil, logo $R= 1/2$. Essa metodologia implica que, para um conjunto de informações de uma imagem de dimensões 256x256, com a adição dos bits extras o código corretor terá o dobro de informação a ser percorrida, sendo então a imagem criptografada de tamanho 512x512.

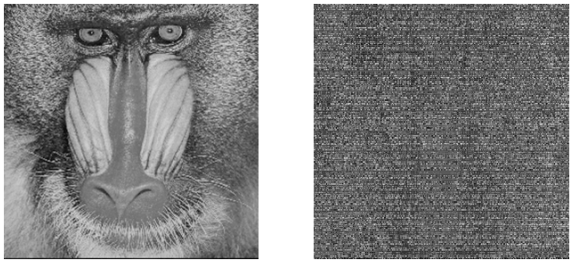

Figura 1: A esquerda a imagem baboon.bmp e a direita o resultado da sua criptografia.

Figura 2: A esquerda a imagem lena.bmp e a direita o resultado da sua criptografia.

5 Resultados

Como método de análise dos resultados, foi calculada a entropia nas imagens utilizadas e nas obtidas. A entropia de Shanon [3] é utilizada para medir a quantidade de informação no dado cifrado.A equação que mostra como esse cálculo é feito pode ser vista em (5):

$$H = -\sum_{i=0}^{z} P_i \log_2 P_i, \tag{5}$$

em que P_i é a probabilidade de células vivas ou mortas ($z = 2$ são s estados)a cada configuração. Abaixo segue a tabela com os resultados obtidos:

Tabela 2: Entropia de Shannon

Imagem	Original	Criptografada
Lena	7.4604	7.992
Baboon	7.3649	7.993

Da mesma forma, foi analisada a distribuição estatística do teste com as imagens utilizadas. Foram gerados os histogramas das imagens originais e criptografadas, mostradas na mesma figura (Figuras 3 e 4). Como pode ser observado, os histogramas das imagens criptografadas possuem uma distribuição diferente da observada para as imagens originais.

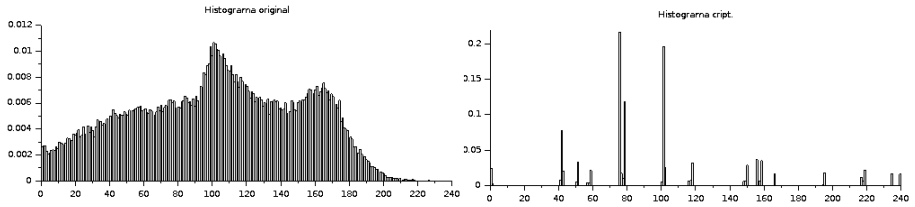

Figura 3: Histograma da imagem original e da imagem criptografada.

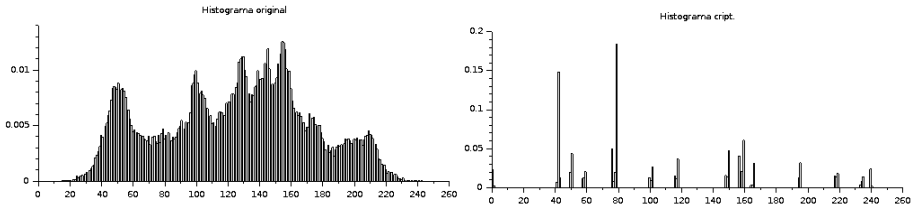

Figura 4: Histograma da imagem original e da imagem criptografada.

6 Discussões

Como pode ser visto nas Figuras 1 e 2, as imagens tiveram suas disposições originais modificadas, não tendo padrões conhecidos no criptograma, nem mostragem de artefatos, o que é consequência da escolha por imagens em tons de cinza.

O histograma de imagem é um dos parâmetros analisados para checagem dos padrões. Caracteriza-se pela distribuição dos píxels da imagem, traçando o número de píxels em cada nível de intensidade. Quanto as Figuras 3 e 4, pode ser visto que a configuração dos histogramas são diferentes, o que evidencia alta sensibilidade ao uso das regras. A disposição dos histogramas é diferente de [5] e [8] devido ao uso de regras não perfeitamente inversíveis, no entanto, é conseguida a decriptagem da imagem sem prejuízos.

Na Tabela 3 é mostrada a comparação dos resultados da entropia da imagem Lena, em tons de cinza, usando o método proposto e os métodos em [9] e [12]. Como pode ser visto na tabela, o valor de entropia encontrado muda a partir da terceira casa decimal, dando um erro de 0,005. A entropia menor do que nos outros casos se dá devido a diminuição de configurações devido aos uso de auômatos não completamente inversíveis, o que não tira o carácter caótico da técnica.

Tabela 3: Comparação com a imagem da Lena

Métodos	Entropia
Ref[10]	7.997
Ref[13]	7.997
Proposto	7.992

7 Conclusões

Neste artigo foi realizado o estudo sobre uma técnica de criptografia de imagens alternativa as já existentes. Os erros apresentados por regras de AC não completamente inversíveis (43 - 113 e 212- 142)foram corrigidos por um código corretor de erro. Conclui-se que existe a comutatividade entre algumas regras, e os pares não completamente inversíveis não geram erros para uma iteração. Quanto ao tempo gasto no processo, precisa ser diminuido o custo computacional, pois mostrou-se um pouco elevado.

Referências

[1] K. Bhattacharjee, N. Naskar, S. Roy e S. Das, A Survey of Cellular Automata: Types, Dynamics, Non-uniformity and Applications, (2016), arXiv preprint arXiv:1607.02291.

[2] E. B. Corrochano, Handbook of Geometric Computing, Springer, (2005).

[3] T. M .Cover e J. A. Thomas, Elements of information theory. John Wiley and Sons, 2012.

[4] S. Hyakin e M. Moher.Sistemas de Comunicação, 5ª ed., Bookman Editora, (2011).

[5] J. Jin, An image encryption based on elementary cellular automata, Optics and Lasers in Engineering, vol. 50(12), p. 1836-1843, (2012).

[6] M. Sablik, Directional dynamics for cellular automata: A sensitivity to initial condition approach, Theoretical Computer Science, vol. 400, p. 1-18, (2008).

[7] E. C. Silva, J. A. J. P. Soares e D. A. Lima, Autômatos celulares unidimensionais caóticos com borda fixa aplicados à modelagem de um sistema criptográfico para imagens digitais, Revista de Informática Teórica e Aplicada, vol. 23, n. 1, p. 250-276, (2016).

[8] A. Souyah e K. M. Faraoun, An image encryption scheme combining chaos-memory cellular automata and weighted histogram. Nonlinear Dynamics, vol. 86, n. 1, p. 639-653, (2016).

[9] X. Wang, L. Liu e Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering, vol. 66, p. 10-18, (2015).

[10] S. Wolfram, A New Kind of Science, Wolfram Media, 1ª ed.,(2002)

[11] S. Wolfram, One-dimensional cellular automata, Cap. 3, (2015).

[12] L. Xu, Z. Li, J. Li e W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Optics and Lasers in Engineering, vol. 78, p. 17-25, (2016).