UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MÉTODO CRIPTOGRÁFICO BASEADO EM AUTÔMATOS CELULARES BIDIMENSIONAIS PARA CIFRAGEM DE IMAGENS

TARCÍSIO ABADIO DE MAGALHÃES JÚNIOR

Uberlândia - Minas Gerais
2010

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

TARCÍSIO ABADIO DE MAGALHÃES JÚNIOR

MÉTODO CRIPTOGRÁFICO BASEADO EM AUTÔMATOS CELULARES BIDIMENSIONAIS PARA CIFRAGEM DE IMAGENS

Dissertação de Mestrado apresentada à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como parte dos requisitos exigidos para obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Inteligência Artificial.

Orientadora:
Prof[a]. Dr[a]. Gina Maira Barbosa de Oliveira

Uberlândia, Minas Gerais
2010

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU

M188m Magalhães Júnior, Tarcísio Abadio de, 1985-
Método criptográfico baseado em autômatos celulares bidimensionais para cifragem de imagens [manuscrito] / Tarcísio Abadio de Magalhães. - 2010.
174 f. : il.

Orientadora: Gina Maira Barbosa de Oliveira.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Ciência da Computação.
Inclui bibliografia.

1. Inteligência artificial - Teses. 2. Criptografia de dados (Computação) - Teses. I. Oliveira, Gina Maira Barbosa de. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Ciência da Computação. III. Título.

CDU: 681.3:007.52

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Os abaixo assinados, por meio deste, certificam que leram e recomendam para a Faculdade de Computação a aceitação da dissertação intitulada "**Método Criptográfico Baseado em Autômatos Celulares Bidimensionais para Cifragem de Imagens**" por **Tarcísio Abadio de Magalhães Júnior** como parte dos requisitos exigidos para a obtenção do título de **Mestre em Ciência da Computação**.

Uberlândia, 12 de Dezembro de 2010

Orientadora: _____

Profª. Drª. Gina Maira Barbosa de Oliveira
Universidade Federal de Uberlândia

Banca Examinadora:

_____

Prof. Dr. José Demísio Simões da Silva
Instituto Nacional de Pesquisas Espaciais

_____

Prof. Dr. Daniel Gomes Mesquita
Universidade Federal de Uberlândia

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Data: Dezembro de 2010

Autor:	**Tarcísio Abadio de Magalhães Júnior**
Título:	**Método Criptográfico Baseado em Autômatos Celulares Bidimensionais para Cifragem de Imagens**
Faculdade:	**Faculdade de Computação**
Grau:	**Mestrado**

Fica garantido à Universidade Federal de Uberlândia o direito de circulação e impressão de cópias deste documento para propósitos exclusivamente acadêmicos, desde que o autor seja devidamente informado.

_____

Autor

Dedicatória

Aos meus pais.

Agradecimentos

Primeiramente, à Deus.

Ao meus pais por me darem todo o suporte necessário para o cumprimento desta etapa da minha vida.

Às minhas irmãs Ana Paula e Ana Gabriela, por não terem me atrapalhado.

À minha namorada Tatiane pela compreensão e ajuda.

Aos amigos Robson e Lígia pela ajuda e parceria em disciplinas.

Aos amigos e ao pessoal do trabalho por compreenderem a minha ausência.

À professora Dra. Gina M. B. de Oliveira, por ter acreditado em meu potencial e me oferecido esta oportunidade.

Resumo

Neste trabalho é proposto um novo modelo criptográfico de chave simétrica baseado em autômatos celulares bidimensionais com vizinhança von Neumann, heterogêneos e não aditivos. A cifragem do método é realizada através do cálculo de pré-imagens consecutivas e a decifragem a partir da evolução temporal para frente do autômato celular.

O modelo proposto baseou-se em um trabalho anterior que utilizava autômatos celulares unidimensionais como método de cifragem, chamado *Hybrid Cellular Automata* (HCA). A não homogeneidade do autômato, herança do HCA, se dá pelo uso de duas regras no processo do cálculo de pré-imagens. Uma das regras é utilizada apenas nas células do contorno do reticulado a fim de garantir a existência da pré-imagem. Sua função é realizar apenas um deslocamento dos bits. A outra regra é de característica caótica e é a responsável pela cifragem efetiva do reticulado.

A proposição de um novo modelo para cifrar imagens é justificada, pois os modelos convencionais de uma única dimensão não se preocupam com características espaciais das imagens. Além disso, os autômatos celulares por serem estruturas muito simples e intrinsecamente paralelos facilitam a implementação eficiente em hardware. Devido ao modelo proposto utilizar uma cifragem espacial, o resultado da criptografia tem uma maior qualidade, aumentando assim a segurança das informações.

A validade e a eficiência do modelo foi avaliada a partir de vários testes realizados com diferentes conjuntos de imagens e com amostras de regras com vizinhança von Neumann de raio 1 e raio 2. No caso das regras com vizinhança de raio 1, o conjunto completo de chaves de 16 bits foi testado de forma exaustiva. Os resultados confirmam que o método possui as propriedades de confusão e difusão.

A partir dos resultados obtidos nos testes, foi possível especificar um novo sistema criptográfico que foi denominado *Two-Dimensional Hybrid Cellular Automata* (THCA). O THCA pode ser aplicado tanto em cifragem de imagens, quanto na cifragem de textos lineares. Quando aplicado à cifragem de textos lineares, o THCA opera com chaves de 256 bits, blocos de 1024 bits e utiliza 15 passos de cálculo de pré-imagens na cifragem. Quando aplicado à cifragem de imagens, o THCA opera com chaves de 256 bits e cada imagem é tratada com um único bloco, que é cifrado em no máximo 25 passos de pré-imagens, desde que sua matriz binária não ultrapasse 512 Kbytes e sua maior dimensão não ultrapasse 2048 bits. Caso seja maior que essas dimensões, a imagem deve ser quebrada em blocos de 2048×2048 bits, que serão cifrados em 25 passos de pré-imagens.

Palavras chave: autômato celular bidimensional, criptografia simétrica, cálculo de pré-imagem, criptografia de imagens

Abstract

This work proposes a new symmetric-key cryptographical model based on von Neumann two-dimensional, heterogeneous and non-additive cellular automata. The encryption process is performed by calculating consecutive pre-images and decryption process by the forward evolution of cellular automata.

The proposed model was based on earlier work which used one-dimensional cellular automata, called *Hybrid Cellular Automata* (HCA). The inhomogeneity of the automaton, a legacy of HCA, is achieved by using two rules in the process of calculating pre-images. One of the rules is used only in boundary lattice cells to ensure the existence of the pre-image, their only function is to perform a shift of the bits. The other rule is chaotic and it is responsible for perform the process of effective scrambling the lattice.

The proposition of a new model to encrypt images is justified, because the conventional models of a single dimension are not concerned with spatial characteristics of images. Moreover, cellular automata structures because they are very simple and inherently parallel facilitate the efficient implementation in hardware. Due to the proposed model to use an spacial encryption, the result of cryptography has a higher quality, thus increasing the security of information.

The validity and efficiency of the model was assessed from multiple tests performed with different sets of images and samples of rules with von Neumann neighborhood of radius 1 and radius 2. In the case of rules with a neighborhood radius 1, the full set of keys of 16 bits has been tested thoroughly. The results confirm that the method has the properties of confusion and diffusion.

From the results obtained in the tests, it was possible to specify a new cryptographic system which was named *Two-Dimensional Hybrid Cellular Automata* (THCA). The THCA can be applied in encryption of image or linear texts. When applied to the scrambling of linear texts, the THCA operates with 256-bit keys, blocks of 1024 bits and uses 15 steps of calculating pre-images in encryption. When applied to the encryption of images, the THCA operates with 256-bit keys, and each image is treated with a single block, which is encrypted in a maximum of 25 steps of pre-images, since its binary matrix does not exceed 512 Kbytes and the biggest dimension does not exceed 2048 bits. If it is larger than these dimensions, the image must be broken into blocks of 2048×2048 bits, which will be encrypted in 25 steps of pre-images.

Keywords: two-dimensional cellular automata, symmetric encryption, calculation of pre-image, image encryption

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Com o advento da internet tornou-se comum e frequente a troca de dados entre as mais diversas entidades. Na maioria das vezes é necessário que os dados transmitidos estejam protegidos contra interferências externas, como em uma transferência bancária, em que a senha deve ser conhecida apenas pelo cliente e pelo banco.

A criptografia torna possível garantir aspectos importantes em uma transmissão de dados, como confidencialidade, integridade e autenticidade e, atualmente, existem diversos modelos de criptografia capazes de garanti-los. Com a popularização de equipamentos eletrônicos capazes de produzir imagens, tornou-se comum transmiti-las através de diversos meios não muito seguros, tal como a internet. Esta afirmação leva a seguinte pergunta: será que os modelos tradicionais de criptografia se preocupam com a redundância e com o grande volume de informação, características inerentes às imagens? Além dos aspectos já citados, esta pergunta também motivou para a criação de um novo campo na criptografia denotado por "Criptografia de Imagens" [Yu et al. 2008].

A criptografia de imagens tem aplicação em diversos campos, tais como, internet, sistemas de multimídia, imagens médicas, telemedicina, comunicação militar, etc. Na criptografia de imagens, os métodos geralmente propõem variações aos algoritmos tradicionais desenvolvidos originalmente para cifrar blocos unidimensionais de dados. Cifrar imagens através da utilização de algoritmos de criptografia de textos unidimensionais pode, entretanto, gerar artefatos indesejados no resultado, chamados zonas de texturas [Yu et al. 2008].

Os autômatos celulares são sistemas dinâmicos que possuem variáveis discretas na representação do tempo, do espaço e dos estados das células [Wolfram 1986]. Além de intrinsecamente paralelos, os autômatos celulares podem ser facilmente implementados em hardware e possibilitam alterar facilmente o espaço de chaves através da ampliação do raio da vizinhança da regra de transição, características desejáveis em um sistema criptográfico. Diversos modelos criptográficos baseados em autômatos celulares foram propostos anteriormente, desde o trabalho precursor de Wolfram [Wolfram 1986]. A criptografia baseada em autômatos celulares pode ser dividida em três classes de modelos: i)

criptografia através da geração de números pseudo-aleatórios onde a regra do autômato celular não é utilizada efetivamente como processo de cifragem [Wolfram 1986], [Guan e Tan 2003], [Hameed e Eldin 2007] ; ii) criptografia utilizando autômatos celulares aditivos, onde a atividade das regras de transição é aproveitada para a concepção de autômatos celulares periódicos onde o ciclo é conhecido [Nandi et al. 1994], [Sen et al. 2002]; iii) criptografia através do cálculo de pré-imagens, utilizando autômatos celulares não aditivos no qual se realiza a evolução para trás (calculo das pré-imagens) para cifragem e a decifragem é obtida através da evolução temporal para frente [Gutowitz 1995], [Oliveira et al. 2004], [de Macedo 2007], [Oliveira et al. 2010c].

O modelo criptográfico a ser investigado nesse trabalho pertence à terceira classe de modelos, pois utiliza a evolução para trás como método de cifragem. Gutowitz (1995) foi o primeiro a propor o uso do cálculo de pré-imagens de autômatos celulares na cifragem. Posteriormente, outros autores também investigaram métodos de criptografia que utilizam o cálculo de pré-imagens na etapa de cifragem [Oliveira et al. 2004] e [Oliveira et al. 2010c]. Em [de Macedo 2007] é apresentado um modelo de criptografia de textos lineares através do cálculo de pré-imagens fazendo uso de autômatos celulares unidimensionais caóticos, não homogêneos e não aditivos. Esse modelo emprega duas regras diferentes na evolução das células do autômato celular: a primeira delas, de dinâmica caótica, é similar à empregada por Gutowitz em seu modelo e é aplicada na maioria das células do reticulado, enquanto a segunda regra, de dinâmica ponto-fixo, provoca apenas um deslocamento e é aplicada apenas nas células da borda do reticulado. A combinação dessas duas regras produz uma cifragem de boa qualidade, mantendo o tamanho do texto cifrado igual ao do texto original.

Este trabalho propõe um novo modelo de criptografia de imagens baseado no modelo unidimensional proposto em [de Macedo 2007]. Diferentemente, o modelo de autômato celular investigado nessa dissertação é em duas dimensões, justificando assim o seu estudo aplicado à criptografia de imagens. Espera-se que a aplicação de um modelo bidimensional torne a cifragem mais segura, devido à criptografia espacial, a qual realiza a cifragem considerando o plano como um todo. A criptografia espacial será obtida utilizando-se o cálculo de pré-imagens de autômatos celulares bidimensionais. A cada passo do processo de cifragem, os bits serão alterados observando-se uma relação espacial. Essa transição espacial será realizada de forma a garantir propriedades desejadas no processo de cifragem, como a confusão e a difusão [Zeghid et al. 2007].

1.1 Objetivo

O objetivo deste trabalho é propor um novo modelo de criptografia através do cálculo de pré-imagens em duas dimensões utilizando autômatos celulares bidimensionais caóticos, não homogêneos e não aditivos. Nesse novo modelo, as características principais do

modelo unidimensional proposto em [de Macedo 2007] são preservadas. Ou seja, o processo de cifragem é realizado através do cálculo de pré-imagens de um autômato celular bidimensional, no qual são aplicadas duas regras de transição na evolução dos estados das células (não-homogêneo). A primeira regra é caótica e sensível a um dos bits da vizinhança e é aplicada na maior parte dos bits do reticulado para garantir uma forte propagação de perturbações. A segunda regra é ponto-fixo e produz apenas um deslocamento dos bits do reticulado, mas garante a existência da pré-imagem para qualquer reticulado. Ela é aplicada em um número menor de células do reticulado, que formam a borda do reticulado. O processo de decifragem é realizado aplicando-se a evolução temporal para frente no autômato celular.

A proposição de um novo modelo criptográfico deve buscar garantir que algumas características sejam atendidas, tais como, segurança contra ataques de criptoanálise, o tamanho do espaço de chaves e a facilidade em aumentá-lo, desempenho no processo de cifragem e decifragem, bem como a quantidade de recursos necessários para realizá-los. No decorrer deste trabalho serão apresentados diversos testes e análises que visam demonstrar que o método proposto possui às características citadas.

1.2 Estrutura do Texto

Os demais capítulos estão organizados da seguinte maneira:

Capítulo 2: apresenta a definição de autômato celular, características das regras e a construção de modelos unidimensionais e bidimensionais.

Capítulo 3: apresenta de forma breve a história da criptografia, terminologias utilizadas no ambiente da criptografia, os métodos clássicos e modernos, e conclui com algumas formas de criptoanálise existentes.

Capítulo 4: apresenta a revisão de alguns métodos criptográficos propostos na literatura relacionados ao modelo desse dissertação. Primeiramente, discute os trabalhos relacionados com criptografia de imagens e por fim os trabalhos de criptografia baseados em autômato celulares que servirão de base para o novo modelo proposto.

Capítulo 5: apresenta o modelo proposto nesse trabalho e suas duas variações.

Capítulo 6: apresenta os resultados de testes aplicados no modelo proposto com o objetivo de validá-lo.

Capítulo 7: apresenta a especificação para utilização do sistema criptográfico proposto neste trabalho.

Capítulo 8: apresenta as considerações finais e sugestões para trabalhos futuros.

Capítulo 2

Autômatos Celulares

Os autômatos celulares (ACs) foram introduzidos por Ulam e von Neumann na década de 50 e tinham como objetivo projetar mecanismos artificiais de auto-reprodução. Von Neumann motivado pela seguinte pergunta "Que tipo de organização lógica é suficiente para um autômato ser capaz de reproduzir a si mesmo?", propôs-se a encontrar uma máquina de Turing que resolvesse tal questionamento [de Oliveira 2003]. Em seus estudos, von Neumann utilizou ACs bidimensionais com mais de 50 estados.

John Conway e Wolfram foram outros importantes pesquisadores responsáveis pela popularização dos ACs no meio acadêmico. Conway propôs um AC bidimensional com apenas dois estados conhecido por "Game of Life" capaz de suportar estruturas de uma complexidade inesperada (como os *gliders*, que são padrões de células que se deslocam pelo reticulado criados a partir de um AC) [Gardner 1970]. Wolfram (1984) tornou-se uma referência devido a suas diversas publicações na década de 80, especialmente às relativas ao comportamento dinâmico dos ACs, nas quais ressalta a existência de ACs capazes de exibir comportamento complexo mesmo utilizando-se de ACs unidimensionais com dois estados [de Oliveira 2003].

Um autômato celular é uma estrutura computacional discreta no espaço, no tempo e nos estados das variáveis. Os ACs possuem uma variedade de aplicações, tais como modelagem de sistemas complexos, compactação de dados, reconhecimento de padrões e criptografia [Ganguly et al. 2003].

Um AC é definido por seu espaço celular e por sua regra de transição. O espaço celular é um reticulado de N células idênticas dispostas em um arranjo n-dimensional, cada uma com um padrão idêntico de conexões locais para outras células, e com condições de contorno para as células nos extremos do reticulado [de Oliveira 2003]. A cada instante, um estado é assumido por cada célula, dentre um conjunto de estados possíveis. A regra de transição faz um mapeamento entre células vizinhas para determinar o novo estado da célula central da vizinhança. Um passo de tempo é contado após a aplicação da regra de transição em todas as células do reticulado. A evolução temporal do AC, nada mais é que a aplicação das regra de transição por vários passos de tempo.

Segundo a notação adotada em [Mitchell 1996], $\sum$ é o conjunto de todos os estados possíveis em cada célula, onde o tamanho desse conjunto (k) é denotado por $|\sum|$. Para cada célula, é atribuído um índice i e em um dado tempo t seu estado é definido por S_i^t, onde $S_i^t \in \sum$. O estado S_i^t da célula i, junto com os estados das células às quais a célula i está conectada, são chamados vizinhança η_i^t da célula i. A regra de transição de estados é representada por Φ, ao aplicar $\Phi(\eta_i)$ obtém-se o estado S_i^{t+1} para a célula i. Uma unidade de tempo t consiste em aplicar $\Phi(\eta_i)$ em todas as células.

2.1 AC Unidimensional

Os ACs mais comuns encontrados na literatura são os unidimensionais, binários (dois estados possíveis) e que evoluem de forma síncrona. O reticulado desse tipo de autômato normalmente é representado por um vetor de 0s e 1s, no qual cada posição representa uma célula.

O raio de um AC determina a abrangência da vizinhança. O tamanho da vizinhança (m) de um AC unidimensional pode ser definido em função do raio da seguinte maneira $m = 2r+1$, onde r é o raio. A figura 2.1 mostra um reticulado unidimensional de tamanho 16, vizinhança formada por 3 células (ou raio 1).

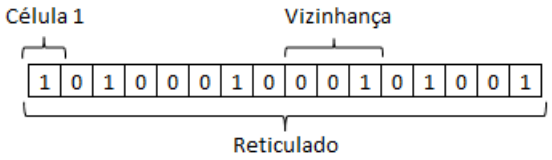


Figura 2.1: Reticulado 1D

A regra de transição determina como os estados das células do reticulado serão alteradas ao longo do tempo. Ela pode ser qualquer função aplicada às células da vizinhança que determine o novo estado da célula central. Suponha um AC unidimensional de raio 1 e $\sum = \{0, 1\}$, logo o número de vizinhanças diferentes possíveis é dado por $2^m = 8$. A regra de transição $\Phi = \{b_0b_1b_2b_3b_4b_5b_6b_7\}$ determina que a vizinhança 000 leve o estado da célula central para o bit b_0, a vizinhança 001 leve para o bit da célula central para b_1, e assim sucessivamente. A figura 2.2 exemplifica graficamente a regra de transição $\Phi = \{01101001\}$.

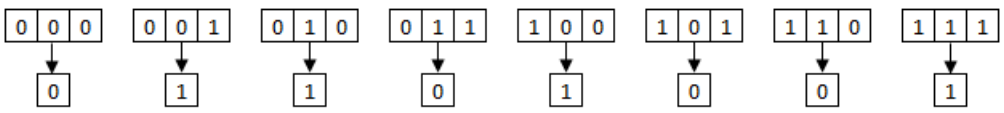


Figura 2.2: Regra de transição de raio 1

Antes de aplicar a regra de transição é necessário definir a condição de contorno do reticulado, que se refere à vizinhança das células no extremo do reticulado. Por exemplo,

em um AC unidimensional de raio 1, para completar a vizinhança da primeira célula do reticulado é necessário um bit à esquerda, enquanto que para completar a vizinhança da última célula é necessário um bit à direita. A condição de contorno mais usual é a periódica. A condição de contorno periódica pode ser definida como $S_i^t = S_{i \ mod \ N}^t$, onde N é o tamanho do reticulado. Neste caso, as extremidades do reticulado estão conectadas formando um anel, conforme apresenta o exemplo da figura 2.3.

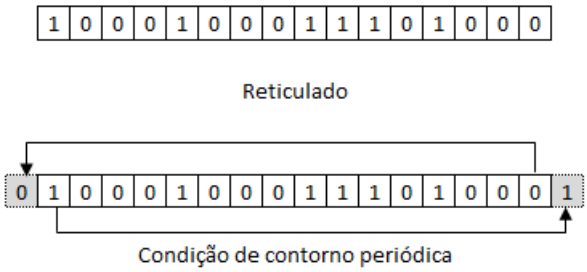


Figura 2.3: Condições de contorno periódica

Dado o modelo de um AC unidimensional e os estados das células no instante inicial (t_0), é possível realizar uma evolução temporal aplicando-se a regra de transição sucessivamente. A figura 2.4 mostra a evolução temporal por três unidades de tempo do reticulado inicial da figura 2.1, utilizando-se da regra de transição apresentada na figura 2.2 e uma condição de contorno periódica.

1	0	1	0	0	0	1	0	0	0	1	0	1	0	0	1	t0
0	0	1	1	0	1	1	1	0	1	1	0	1	1	1	0	t1
0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	t2
0	1	1	0	0	1	1	1	0	0	0	0	1	1	0	1	t3

Figura 2.4: Reticulado após 3 evoluções

Wolfram propôs uma notação para as regras dos autômatos celulares, em que é possível representá-las simplesmente através de números inteiros [Wolfram 2002]. Suponha a regra de raio 1 representada pela tabela 2.1. Para obter o valor numérico da regra é necessário combinar os valores da saída da regra, da direita para a esquerda, formando um valor binário, que neste caso é 01011001_2. A representação desse número na base decimal fornece o valor numérico da regra: para o exemplo da tabela 2.1 o valor é 89.

Vizinhança	000	001	010	011	100	101	110	111
Saída	1	0	0	1	1	0	1	0

Tabela 2.1: Regra transição 89

Os autômatos celulares possuem duas modalidades de iteração, que podem ser definidas como:

Progressivo (*Forward*): dado um reticulado num instante t, aplica-se a regra de transição para obter-se o reticulado num instante $t+1$. Neste caso, o novo reticulado é obtido de forma determinista pela regra de transição.

Regressivo (*Backward*): a partir de um reticulado num instante t, determina-se qual seria um possível reticulado no instante $t-1$, que daria origem ao reticulado em t após a aplicação da regra de transição. Este processo é também conhecido como o cálculo da **pré-imagem**. Dependendo da regra de transição e do reticulado em t, pode ser possível mais de uma pré-imagem ou mesmo nenhuma. Um AC é dito reversível se, para qualquer configuração do reticulado, existe sempre uma pré-imagem e esta é única.

2.2 AC Bidimensional

Os ACs bidimensionais (AC 2D) têm definição similar aos unidimensionais, sendo sua principal diferença o espaço celular, onde o AC 2D evolui no espaço bidimensional. Geralmente este tipo de autômato é representado por uma matriz de 0s e 1s, no qual cada posição da matriz representa uma célula. De forma similar aos ACs unidimensionais, a evolução temporal é obtida a partir da aplicação da regra de transição por alguns passos de tempo. No caso do AC 2D as vizinhanças não se restringem apenas às células vizinhas da direita e da esquerda, mas sim em todas as direções.

As vizinhanças de ACs bidimensionais mais conhecidas são a von Neumann e a Moore, que podem ser vistas respectivamente nas figuras 2.5 e 2.6 [Wolfram 2002]. As células que estão marcadas com um "**x**" correspondem à vizinhança da célula central "**y**".

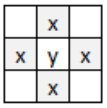


Figura 2.5: Vizinhança de von Neumann

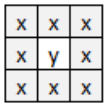


Figura 2.6: Vizinhança de Moore

A condição de contorno do AC bidimensional também pode ser periódica: tanto as linhas extremas do reticulado estão conectadas (norte e sul), quanto as colunas (leste e oeste). Seja um reticulado qualquer de ordem $m \times n$ com condição de contorno periódica, onde m é número de linhas e n é o número de colunas, e seja b_{ij} um bit em uma posição qualquer do reticulado, então a linha $b_{(m+1)}$ é igual à linha b_1 e a coluna $b_{(n+1)}$ é igual à coluna b_1.

Para a evolução temporal para frente, basta aplicar a regra de transição em todas a células do reticulado simultaneamente, assim como ocorre no modelo unidimensional. Na figura 2.7 pode-se observar a regra de transição com vizinhança do tipo von Neumann de

raio 1 que foi utilizada para a evolução do AC bidimensional da figura 2.8. Para a evolução foi utilizada a condição de contorno periódica. Na figura 2.8, $t0$ indica o reticulado inicial, enquanto que $t1$ e $t2$ representam o reticulado após a evolução temporal para frente depois de 1 e 2 unidades de tempo, respectivamente.

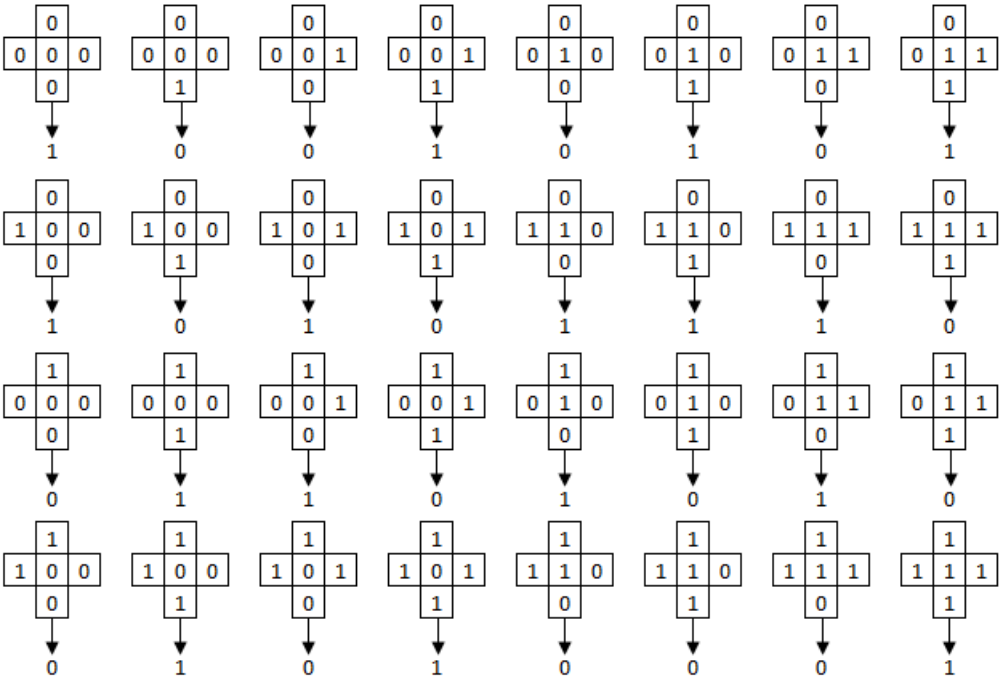


Figura 2.7: Regra de transição de raio 1 para um AC 2D

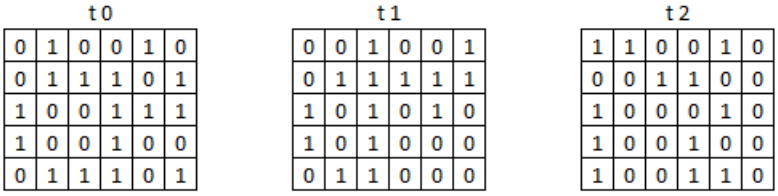
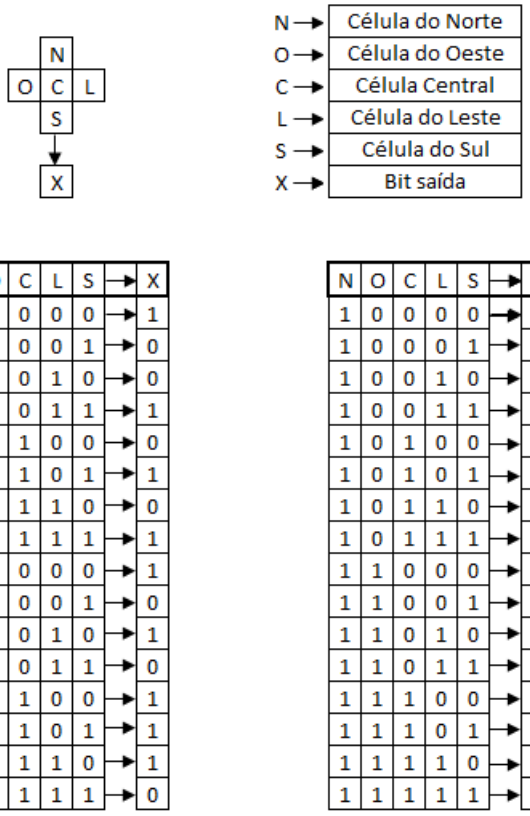


Figura 2.8: Evolução AC 2D

Para facilitar a representação das vizinhanças de uma regra de transição bidimensional, estas podem ser linearizadas. Por exemplo, no caso da vizinhança von Neumann pode-se linearizar a vizinhança como $\eta = (N, O, C, L, S)$, onde N, O, C, L e S representam os bits do norte, oeste, central, leste e sul respectivamente. Existem outras maneiras de linearizar as regras de transição, por exemplo, $\eta = (N, C, S, O, L)$, ou qualquer outra permutação das células da vizinhança. Porém, este trabalho utilizará a forma descrita anteriormente, uma vez que adotamos regras com sensitividade ao bit do norte na maioria dos exemplos e assim o bit sensível sempre será o mais a esquerda da vizinhança. A figura 2.9 apresenta a regra da figura 2.7 utilizando essa linearização.



N	O	C	L	S	→	X
0	0	0	0	0	→	1
0	0	0	0	1	→	0
0	0	0	1	0	→	0
0	0	0	1	1	→	1
0	0	1	0	0	→	0
0	0	1	0	1	→	1
0	0	1	1	0	→	0
0	0	1	1	1	→	1
0	1	0	0	0	→	1
0	1	0	0	1	→	0
0	1	0	1	0	→	1
0	1	0	1	1	→	0
0	1	1	0	0	→	1
0	1	1	0	1	→	1
0	1	1	1	0	→	1
0	1	1	1	1	→	0

N	O	C	L	S	→	X
1	0	0	0	0	→	0
1	0	0	0	1	→	1
1	0	0	1	0	→	1
1	0	0	1	1	→	0
1	0	1	0	0	→	1
1	0	1	0	1	→	0
1	0	1	1	0	→	1
1	0	1	1	1	→	0
1	1	0	0	0	→	0
1	1	0	0	1	→	1
1	1	0	1	0	→	0
1	1	0	1	1	→	1
1	1	1	0	0	→	0
1	1	1	0	1	→	0
1	1	1	1	0	→	0
1	1	1	1	1	→	1

Figura 2.9: Linearização da regra de transição da figura 2.7

2.3 Classificação Dinâmica

Apesar da construção de um AC ser simples, eles são capazes de gerar um comportamento extremamente complexo. Wolfram (1984) classificou o comportamento dinâmico dos ACs em quatro diferentes classes, são elas:

Classe 1: o AC evolui para um estado homogêneo.

Classe 2: configuração simples separadas por estruturas periódicas.

Classe 3: exibe um comportamento caótico ou pseudo-aleatório.

Classe 4: algumas configurações iniciais resultam em estruturas localizadas complexas, algumas vezes bastante duradouras.

A figura 2.10 apresenta exemplos de evolução temporal de regras unidimensionais para cada classe dinâmica. Para facilitar a visualização, as células com o valor 1 estão destacadas, enquanto que as células com o valor 0 possuem o fundo branco. Este trabalho dará ênfase às regras pertencentes à classe 3, por serem muito sensíveis à configuração inicial do reticulado e gerarem resultados com alto grau de aleatoriedade, o que as credencia para utilização em sistemas criptográficos.

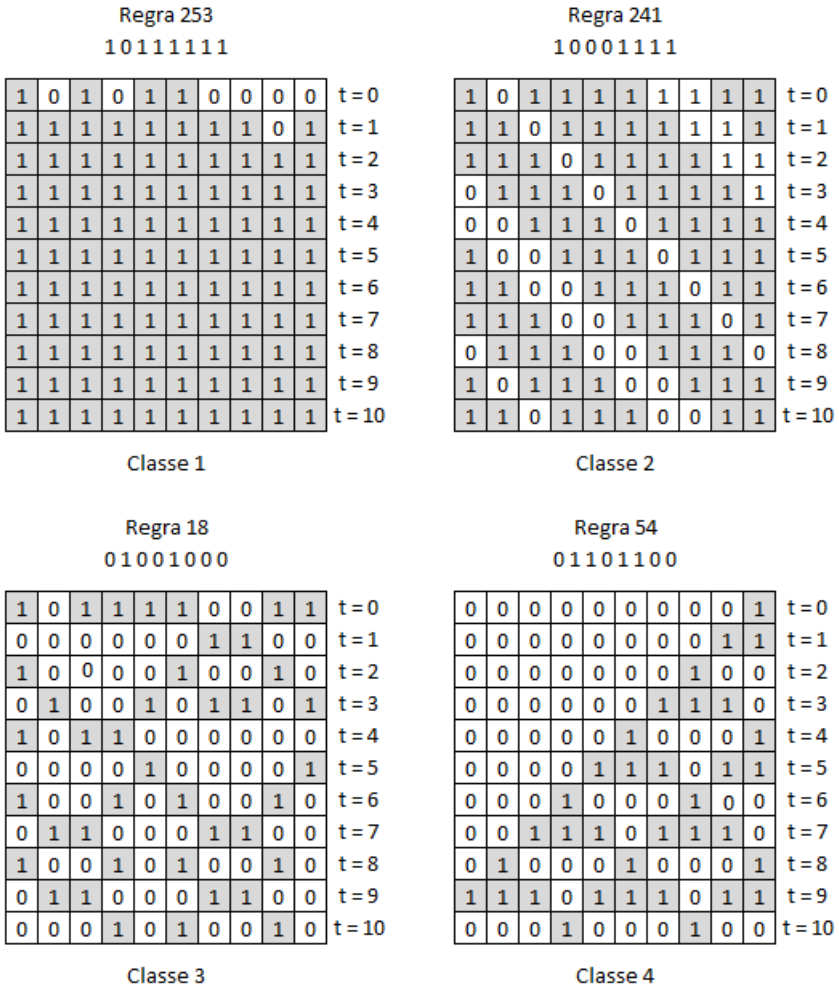


Figura 2.10: Exemplos de evoluções para cada classe dinâmica

2.4 Sensitividade

A sensitividade é uma característica que pode ser encontrada em algumas regras de transição de ACs. Regras com essa característica garantem sempre a existência de pré-imagens a partir de qualquer reticulado inicial, propriedade importantíssima para o modelo proposto neste trabalho. Para ACs unidimensionais, existem três tipos de sensitividades a uma das células no extremo da vizinhança: à esquerda, à direita e bidirecional. Suponha um AC unidimensional binário de raio 1, as sensitividades podem ser assim formalizadas:

Sensível à esquerda: Se $\Phi(S_{i-1}^t, S_i^t, S_{i+1}^t) \neq \Phi(\overline{S_{i-1}^t}, S_i^t, S_{i+1}^t)$

Sensível à direita: Se $\Phi(S_{i-1}^t, S_i^t, S_{i+1}^t) \neq \Phi(S_{i-1}^t, S_i^t, \overline{S_{i+1}^t})$

Sensitividade Bidirecional: Se $\Phi(S_{i-1}^t, S_i^t, S_{i+1}^t) \neq \Phi(\overline{S_{i-1}^t}, S_i^t, S_{i+1}^t) \wedge \Phi(S_{i-1}^t, S_i^t, S_{i+1}^t) \neq \Phi(S_{i-1}^t, S_i^t, \overline{S_{i+1}^t})$, sendo $\overline{S_k^t}$ o complemento binário de S_k^t.

As figuras 2.11 e 2.12 apresentam respectivamente uma regra de transição sensível à direita e outra à esquerda, enquanto que a figura 2.13 apresenta uma regra com sensitivi-

dade bidirecional, ou seja, sensível a ambos os lados.

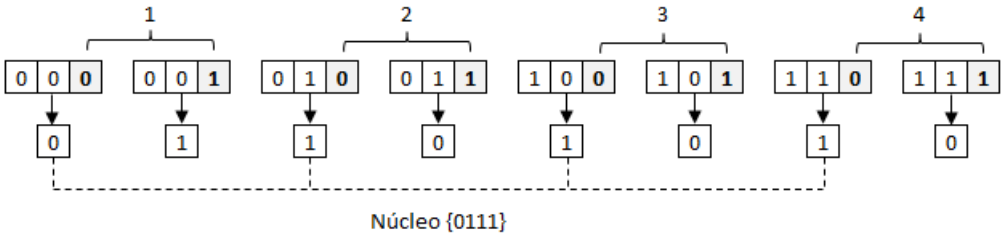


Figura 2.11: Regra de transição sensível ao bit da direita

A sensitividade da regra da figura 2.11 é caracterizada à direita, pois a alteração do bit da direita da vizinhança provoca necessariamente uma alteração no bit de saída, enquanto que na figura 2.12 os bits da esquerda determinam a saída, caracterizando uma regra sensível à esquerda. Já na regra da figura 2.13, tanto os bits da direita, quanto os bits da esquerda provocam alterações nos bits de saída. Portanto, a sensitividade da regra de transição é caracterizada como bidirecional.

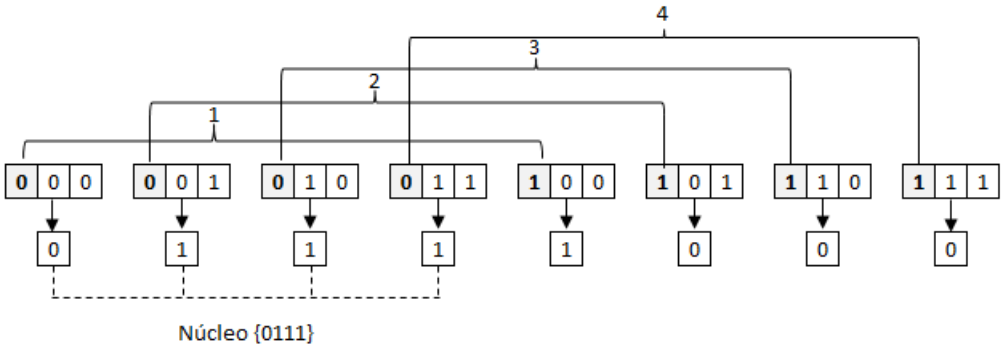


Figura 2.12: Regra de transição sensível ao bit da esquerda

O núcleo da regra é uma maneira simples de expressar uma regra de transição sensível à um dos extremos a partir de um número reduzido de bits. Suponha a regra de raio 1, $\Phi = \{b_0b_1b_3b_4b_5b_6b_7\}$, para construir o núcleo de uma regra sensível à direita são necessários os bits $\{b_0b_2b_4b_6\}$, uma vez que pela sensitividade da regra temos $b_1 = \overline{b_0}$, $b_3 = \overline{b_2}$, $b_5 = \overline{b_4}$ e $b_7 = \overline{b_6}$. Por outro lado, para uma regra sensível à esquerda são necessários os bits $\{b_0b_1b_2b_3\}$, uma vez que $\{b_4b_5b_6b_7\} = \{\overline{b_0b_1b_2b_3}\}$. O processo inverso para construir uma regra de transição sensível à direita a partir do núcleo $\{n_0n_1n_2n_3\}$ é dado por $\{n_0\overline{n_0}n_1\overline{n_1}n_2\overline{n_2}n_3\overline{n_3}\}$, onde n_i representa o bit na posição i do núcleo. A construção de uma regra sensível à esquerda a partir do núcleo é definida por $\{n_0n_1n_2n_3\overline{n_0n_1n_2n_3}\}$.

O núcleo da regra {01101010} (figura 2.11) é definido por {0111}, assim como o núcleo da regra representada na figura 2.12 {01110001}, sendo que no primeiro caso o núcleo é usado para gerar uma regra sensível à direita e no segundo caso ele é usado para gerar uma regra sensível à esquerda. O núcleo da regra é uma informação importante para este

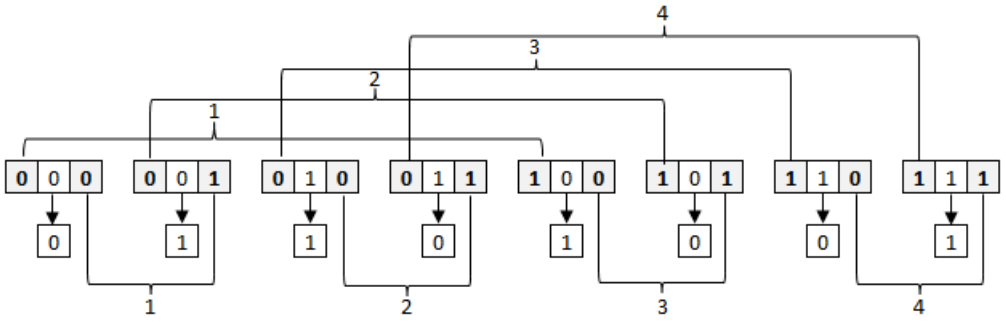


Figura 2.13: Regra de transição bidirecional

trabalho e as regras sensíveis a um dos extremos serão expressas pelo núcleo e pela direção da sensitividade: esquerda ou direita.

As regras de transição que possuem sensitividade à direita, à esquerda ou bidirecional, são exemplos de ACs que geralmente exibem comportamento caótico [de Oliveira et al. 2003].

De forma similar às regras de transição dos ACs unidimensionais, também é possível definir regras dos ACs bidimensionais que tenham sensitividade a uma das células extremas. Em uma vizinhança von Neumann é possível determinar quatro tipos de sensitividade: sensitividade ao bit do norte, do sul, do oeste e do leste.

Os ACs bidimensionais também permitem a criação de regras sensíveis a um dos extremos a partir de número reduzido de bits, o chamado núcleo da regra. Suponha um AC 2D de raio 1 utilizando-se da vizinhança de von Neumann. Para a construção do núcleo são necessários 16 bits, ao passo que o tamanho total da regra é de 32 bits.

Neste trabalho será empregada a vizinhança von Neumann, pois como poderá ser visto mais adiante o formato da vizinhança permite o cálculo da pré-imagem proposto neste trabalho. A construção do núcleo a partir da regra obedecerá a um processo semelhante ao utilizado para o AC 1D em regras sensíveis à esquerda descrito na seção 2.1. Suponha um AC 2D e a regra $\Phi = \{b_0 b_1 b_3 b_4 ... b_{30} b_{31}\}$ de raio 1 linearizada da forma explicada na seção 2.2. Portanto, o núcleo é definido por $\{b_0 b_1 ... b_{14} b_{15}\}$, onde b_i representa o bit b na i-ésima posição da regra Φ. A construção da regra de transição sensível à célula do norte da vizinhança, a partir do núcleo $\{n_0 n_1 .. n_{14} n_{15}\}$ é dada por $\{n_0 n_1 .. n_{14} n_{15} \overline{n_0 n_1 .. n_{14} n_{15}}\}$.

2.5 Variações do AC padrão

Uma característica básica de qualquer AC é que suas transições se baseiam em relações locais (vizinhança). Contudo, a construção de ACs não se dá apenas pelas formas apresentadas nas seções anteriores. Existem variações na construção de um AC, seja na condição de contorno da regra, na forma de atualização das células, na forma de aplicação de uma ou mais regras no reticulado, ou na dimensão do espaço celular. Diversas variações foram propostas e a seguir são apresentadas algumas mais conhecidas.

2.5.1 Condição de contorno

A condição de contorno determina com serão preenchidas a vizinhanças dos extremos do reticulados e influenciam diretamente no novo reticulado gerado a partir de evoluções. Os dois tipos mais conhecidos de condição de contorno são: a periódica e a nula. A condição de contorno periódica considera o reticulado como um anel. A figura 2.4 apresenta a evolução de uma AC unidimensional utilizando uma regra transição com contorno periódico. Na condição de contorno nula, ao aplicar a regra de transição nas células do extremo do reticulado, os bits necessários para completar a vizinhança são sempre considerados como 0.

A figura 2.14 apresenta a evolução do reticulado inicial t_0 em três passos de tempo (t_1, t_2 e t_3) utilizando um AC unidimensional de raio 1 com condição de contorno nula. Note que o estado das células do extremo utilizadas para o contorno (células destacadas com contorno pontilhado) é sempre zero.

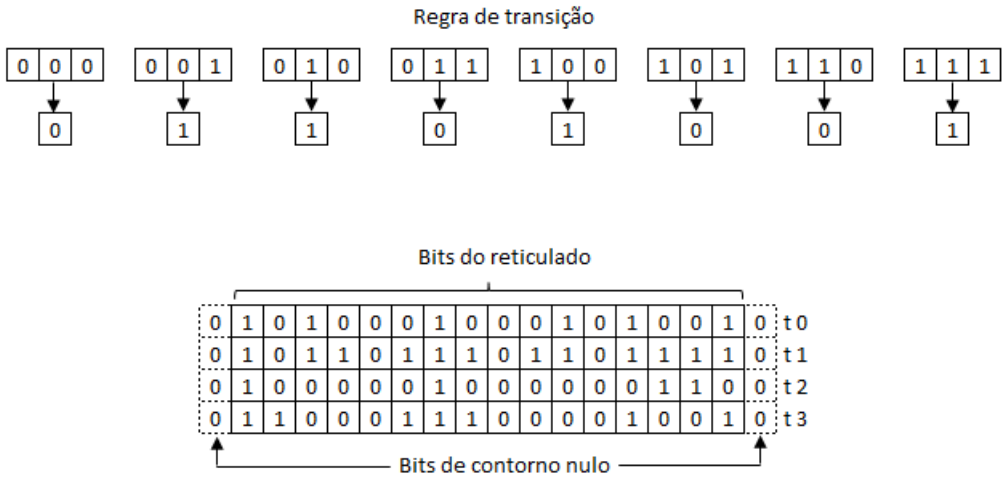


Figura 2.14: Evolução reticulado com condição de contorno nula

2.5.2 Atualização das células

A atualização das células do reticulado pode ser realizada de diversas maneiras. A atualização síncrona ou paralela ocorre quando todas as células do reticulado são atualizadas ao mesmo tempo. Para uma atualização sequencial, cada célula é atualizada separadamente e seu novo valor utilizado para a atualização da próxima célula adjacente. Outro tipo de atualização é a aleatória, semelhante à atualização sequencial, porém a seleção da próxima vizinhança a ser utilizada é escolhida de forma aleatória.

A figura 2.15 mostra uma atualização síncrona realizada no reticulado inicial (t_0) com condição de contorno nula, aplicando-se a mesma regra da figura 2.14. Como pode ser visto na figura, todas as células do reticulado são atualizadas simultaneamente tomando apenas uma unidade de tempo do processador.

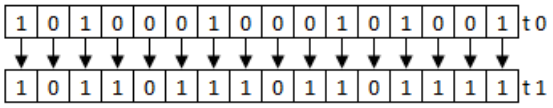


Figura 2.15: Evolução síncrona ou paralela

O processo atualização sequencial das células é exemplificado na figura 2.16 utilizando-se a mesma regra e reticulado inicial da figura 2.14. Note que são necessárias mais unidades de tempo do processador para realizar uma evolução completa do reticulado. Outro ponto importante a ser observado, é que o novo estado da S_i é utilizado para o cálculo da célula S_{i+1}, e assim sucessivamente até o cálculo da última célula.

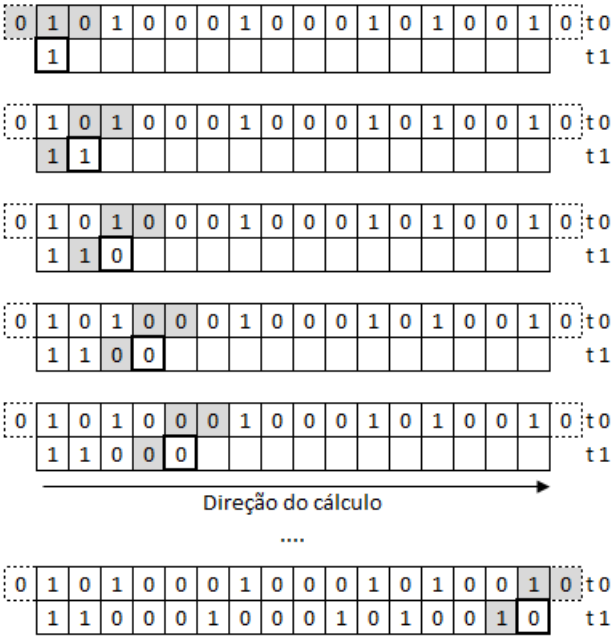


Figura 2.16: Evolução sequencial

Por fim, a figura 2.17 exemplifica uma atualização aleatória. Neste caso, como pode ser visto a ordem para o cálculo das células foi selecionada aleatoriamente.

2.5.3 Aplicação das regras

Para a evolução de um AC, não necessariamente é exigido que uma única regra de transição seja aplicada a todas as células do reticulado. Quando mais de uma regra é utilizada, o AC é denominado heterogêneo ou híbrido. Em contrapartida, quando apenas uma regra é utilizada, o AC é definido como homogêneo.

A figura 2.14 apresenta a evolução de um AC homogêneo, pois utilizou uma única regra na evolução do reticulado. A figura 2.18 mostra uma evolução heterogênea, onde metade dos bits do reticulado utiliza a regra (a), e outra metade utiliza a regra (b). Em alguns exemplos de aplicação de ACs heterogêneos, N regras diferentes são aplicadas em um reticulado de N células [Nandi et al. 1994].

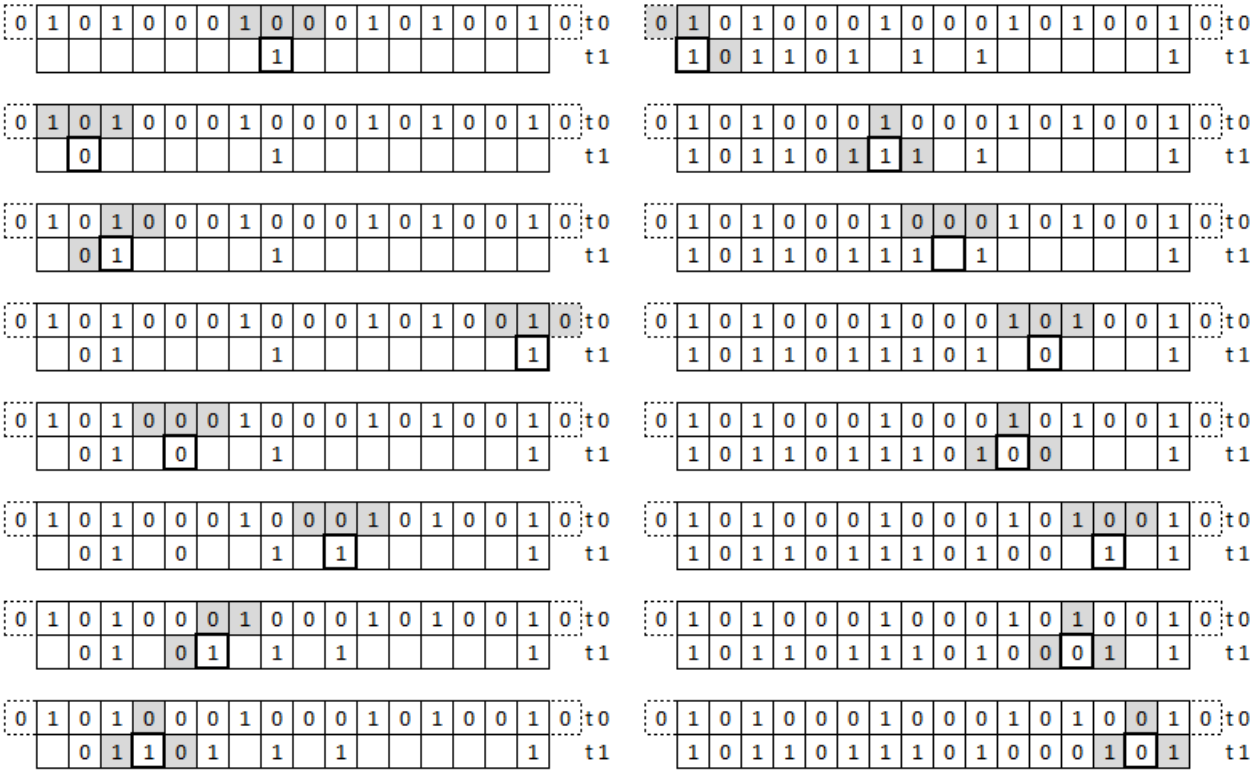


Figura 2.17: Evolução aleatória

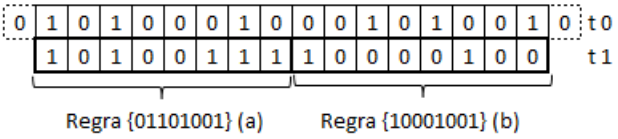


Figura 2.18: Evolução heterogênea

2.5.4 Dimensão

Os ACs podem variar quanto à sua dimensão, não se restringindo aos ACs unidimensionais e bidimensionais. Um AC pode ter K dimensões, onde K é um número inteiro maior que 0. Por exemplo, enquanto um AC 1D é representado de forma linear (*array*) e um AC 2D é representado através de um plano (matriz), um AC 3D pode ser representado através de um cubo tridimensional, como pode ser visto na figura 2.19. Nesse caso, 0 é representado por uma célula vazia e 1 por uma célula preenchida.

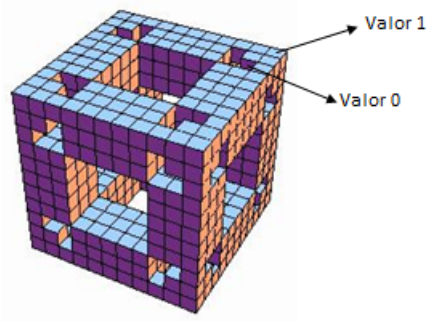


Figura 2.19: Reticulado AC 3D

2.6 Considerações Finais

Neste capítulo foram apresentados alguns modelos de ACs existentes e características que consideramos importantes para o entendimento de ACs, tais como, a dimensão do reticulado, a classificação do comportamento dinâmico, a heterogeneidade na aplicação das regras, os tipos usuais de condição de contorno, os modos de atualização das células e a propriedade da sensitividade. Especificamente, no modelo criptográfico proposto neste trabalho (que será detalhado no capítulo 5) podemos listar algumas características dos ACs empregados:

- Reticulado em duas dimensões;
- Regras de transição que pertencem à classe 3 de comportamento dinâmico;
- Aplicam duas regras de transição diferentes ao longo do reticulado, ou seja, são heterogêneos;
- Regras de transições sensíveis a um dos extremos;
- Condição de contorno periódica;
- Atualização síncrona das células.

Capítulo 3

Criptografia

Criptografia do grego *kryptos* e *grapho* que significam "escondido" e "escrever", refere-se à ciência de proteger a transmissão ou o armazenamento de dados de adulterações e interceptações não autorizadas. No entanto, esta definição não retrata a essência da criptografia moderna. Hoje a criptografia engloba muito mais que uma comunicação secreta, mas também trata de autenticação de mensagens, assinaturas digitais, protocolo de trocas de chaves secretas, protocolos de autenticações e muito mais, ganhando assim os rigores de estudo de uma ciência.

Não é possível falar em criptografia sem citar a criptoanálise. A criptoanálise é a arte de quebrar os modelos criptográficos, possibilitando a leitura das informações secretas, ou ainda substituí-la por diferentes informações. Esse tema será tratado em um tópico mais adiante.

3.1 História

A criptografia tem suas raízes por volta de 2000 a.c. no Egito onde hieróglifos eram utilizados para decorar tumbas para contar a história de seus falecidos. A prática não era empregada para esconder mensagens, mas para enobrecer seus rituais. Por volta de 400 a.c., os espartanos utilizaram de um método mecânico de codificação que ficou conhecido como *escitala*. Entre 60 e 50 a.c. Julius Ceaser desenvolveu um método simples que consistia em realizar um deslocamento nas letras do alfabeto. A evolução da criptografia continuou na Europa refinando suas práticas com novos métodos, práticas, ferramentas em toda época medieval. Por volta do ano de 1800, a criptografia começou a ser mais comumente utilizada em métodos de comunicação entre facções militares. A partir de 1900, muitas máquinas de criptografia foram criadas, bem como máquinas para decifrar mensagens, dentre elas pode-se citar o Enigma e a Colossus, [Harris 2007].

3.2 Terminologia

No ambiente da criptografia existem diversos termos que são utilizados para expressar os elementos envolvidos e os componentes utilizados. Esta seção se encarrega de apresentá-los:

Mensagem: informação, textual ou não, a ser transmitida através de um meio de comunicação não seguro.

Texto claro: mensagem na forma original (legível). A terminologia utilizada no inglês é *"plain text"*, o que leva a uma tradução usual em português para *"texto plano"*.

Texto cifrado: mensagem que passou por um processo de cifragem, tornando-se incompreensível para pessoas não autorizadas.

Cifragem: processo aplicado ao texto claro para transformá-lo em texto cifrado.

Decifragem: processo aplicado ao texto cifrado para transformá-lo em texto claro.

Chave: sequência de bits secreta que é utilizada na cifragem do texto claro e que também é necessária para decifrar o texto cifrado.

Espaço de chaves: valores possíveis que podem ser utilizados para construção das chaves.

A figura 3.1 apresenta o esquema do modelo de um sistema criptográfico.

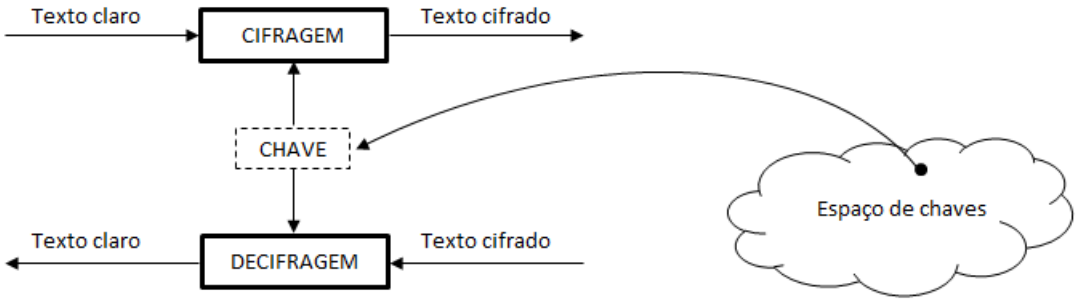


Figura 3.1: Modelo criptográfico

3.3 Métodos Clássicos

A seguir serão apresentados alguns modelos clássicos de criptografia, que vão dos mais simples até os mais complexos. Antes de iniciar a apresentação dos modelos serão definidos os componentes necessários para entendimento de um sistema criptográfico. São eles:

A: remetente ou Alice (termo muito utilizado para exemplificar).

B: destinatário ou Bob (termo muito utilizado para exemplificar).

M: mensagem ou texto claro.

C: texto cifrado.

E_k: chave utilizada para cifragem.

D_k: chave utilizada para decifragem.

E: função de cifragem ou transformação.

D: função de decifragem ou transformação.

Logo, o processo de cifragem é definido por $C = E(E_k, M)$, enquanto que o processo de decifragem é definido por $M = D(D_k, C)$.

3.3.1 Métodos de Substituição

O modelo mais simples de cifragem de substituição consiste em substituir as letras do texto claro por outras letras, números ou símbolos. Este modelo pode ser representado escrevendo abaixo da ordem convencional das letras, uma nova ordem de letras permutadas. Para exemplificar, suponha que Alice queira enviar para Bob a mensagem "MENSAGEM DE TESTE", utilizando-se da substituição proposta na tabela 3.1. Logo, a mensagem cifrada seria "GQFMUKQG RQ LQMLQ". Nesse caso, a tabela de substituição é a chave utilizada tanto na cifragem quanto na decifragem ($E_k = D_k$).

A	B	C	D	E	F	G	H	I	J	K	L	M
U	A	S	R	Q	J	K	D	O	T	X	Y	G
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	B	C	P	E	M	L	V	N	I	W	Z	H

Tabela 3.1: Exemplo de tabela de substituição

No exemplo apresentado, o espaço de chaves total é dado por 26!, contudo apesar do grande número de chaves possíveis, já é sabido que este método é vulnerável a um ataque conhecido como análise de frequência. Este ataque explora o fato da linguagem natural possuir um elevado volume de redundância [Mao 2003], por exemplo, na lingua portuguesa sabe-se que a frequência da letra "A" é muito maior que a da letra "B". Assim, o ataque consiste em analisar a frequência das letras no texto cifrando e tentar descobrir qual a letra correspondente no texto claro.

Pode-se também citar como métodos de substituição a cifra de Atbash, que consiste em inverter as letras dos alfabeto, e a cifra de César que realiza um deslocamento das letras do alfabeto em 3 posições (o fato do método realizar apenas um deslocamento é conhecido como *shift cipher*). Ambos são métodos frágeis, uma vez que baseiam-se na mesma ideia apresentada no exemplo anterior.

3.3.2 Métodos de Transposição

Nos métodos que utilizam a transposição, a ordem das letras ou das palavras na mensagem é alterada de acordo com algum esquema previamente combinado. Suponha que Alice queira enviar para Bob a seguinte mensagem "MENSAGEM DE TESTE", utilizando uma cifra de transposição. Primeiramente, a mensagem é distribuída na forma de uma matriz, onde o número de colunas é dado pelo tamanho da chave e a quantidade de linhas é determinada pelo tamanho da mensagem. Para o exemplo utilizado na tabela 3.2, considere a chave "312645". Para se obter o texto cifrado basta seguir a ordem das colunas fornecida pela chave e concatenar a letra de cada linha, ao finalizar a linha inicia-se a próxima coluna e assim sucessivamente até completar todas as colunas. Neste caso o texto cifrado será "EMEN SMETAEEG SDT". Para o processo de decifragem será necessário realizar o processo inverso, ou seja, reconstruir a matriz a partir das colunas obedecendo a ordem da chave utilizada na cifragem. O espaço de chaves para o exemplo anterior é dado por 6!.

Chave	3	1	2	6	4	5
Texto Claro	M E T	E M E	N S	S D T	A E E	G

Tabela 3.2: Exemplo de tabela de transposição

Segundo [Stallings 2003], cifras que utilizam apenas métodos de transposição são facilmente identificadas, pois a frequência das letras no texto cifrado e no texto claro são idênticas. Uma criptoanálise para o exemplo de transposição citado anteriormente consistiria em distribuir o texto cifrado na matriz e tentar reorganizar o texto claro fazendo o uso de pares de letras que possuem uma alta frequência, por exemplo, dígrafos ou então analisar os possíveis anagramas. Uma opção para melhorar a segurança do exemplo seria realizar o processo de cifragem mais de uma vez e, de preferência, com chaves diferentes.

3.4 Criptografia Moderna

A criptografia moderna é uma disciplina notável, é a junção entre a computação e a segurança em comunicações. Segundo [Mihir Bellare 2005], a criptografia moderna traz consigo campos populares da matemática, mas também campos mais complexos, tais como, a teoria dos números, teorias de complexidade computacional, e a teoria da probabilidade.

Uma nova dimensão é introduzida pela criptografia moderna: o poder computacional disponível. A criptografia moderna visa produzir uma segurança além do poder computacional dos adversários que pretendem quebrar o método. Em princípio, os algoritmos são

quebráveis, porém na prática isto não ocorre devido ao poder computacional existente. Os ataques são inviáveis, contudo não impossíveis de serem realizados.

A criptografia pode ser dividida em duas categorias: algoritmos que realizam cifragem por bloco e algoritmos que realizam cifragem por fluxo. Na cifragem por bloco (*block cipher*), o texto claro é dividido em blocos de tamanho fixo. Cada bloco é processado e produz a saída em blocos correspondentes a cada bloco de entrada. Na cifragem por fluxo (*stream cipher*), também conhecida como cifragem por demanda, o texto claro é processado continuamente, produzindo como saída um elemento por vez [Stallings 2003].

A criptografia moderna também pode ser dividida em algoritmos de chave simétrica e algoritmos de chave assimétrica, que serão apresentados a seguir. Em uma criptografia de chave simétrica uma única chave é utilizada no processo de cifragem e decifragem, enquanto que, a criptografia de chave assimétrica, ou também conhecida como criptografia de chave pública, utiliza uma chave para a cifragem e outra chave para a decifragem. O método investigado nessa dissertação pertence à criptografia de chave simétrica.

3.4.1 Criptografia de Chave Simétrica

Os algoritmos de criptografia de chave simétrica, também conhecidos como criptografia de chave única, ou ainda chave secreta ou chave privada, são os métodos em que a chave utilizada para o processo de decifragem é idêntica à chave utilizada no processo de cifragem, ou seja, $E_k = D_k$.

Os algoritmos de chave simétrica necessitam da utilização da mesma chave no processo de cifragem e decifragem, logo há a necessidade da troca da chave entre o remetente e o destinatário, o que pode levar a um intruso descobri-la. A segurança do sistema é totalmente dependente de como os envolvidos protegem a chave, pois se a chave do sistema for comprometida, então todas a mensagens cifradas poderão ser decifradas e lidas por um intruso.

Devido às chaves de cifragem e decifragem serem idênticas e ambos os usuários do sistema criptográfico precisarem conhecê-las, sistemas simétricos podem prover a confidencialidade, mas não podem prover a autenticidade ou a não repudiação.

Os algoritmos de chave simétrica são rápidos, diferentemente dos algoritmos assimétricos que veremos adiante, e difíceis de serem quebrados. Eles podem cifrar e decifrar um grande volume de dados, que poderia levar um tempo inaceitável caso utilizassem um algoritmo de chave assimétrica [Harris 2007].

Muitos dos algoritmos de criptografia de bloco simétrico utilizam uma estrutura proposta por Feistel, que ficou conhecida como *Estrutura de Feistel* [Anderson 2008]. Segundo Feistel, é possível aproximar de um cifrador de substituição simples utilizando o conceito de cifrador de produto, que consiste em combinar dois ou mais cifradores básicos em sequência, de forma que o resultado final é criptograficamente mais forte que qualquer um

dos envolvidos. Na estrutura de Feistel, o bloco de mensagem do texto claro convertido em bits é dividido em duas partes (L_1, R_1). As duas metades passam por n etapas (*rounds*) e então são combinadas para produzir um bloco contendo o texto cifrado. Em cada etapa é executada uma operação aplicada na metade direita do bloco de texto (R_1), juntamente com uma função F e a sub-chave correspondente àquela etapa. Em seguida, a operação XOR é realizada entre a metade esquerda do bloco de texto (L_1) e a saída da função F, como pode ser visto na figura 3.2. Ao final de cada etapa, os bits da metade esquerda são trocados de lado com a parte direita, que então, servem de entrada para a próxima etapa. Todas as etapas possuem a mesma estrutura, a função F é parametrizada com sub-chaves diferentes para cada etapa, onde estas são derivadas da chave do sistema criptográfico.

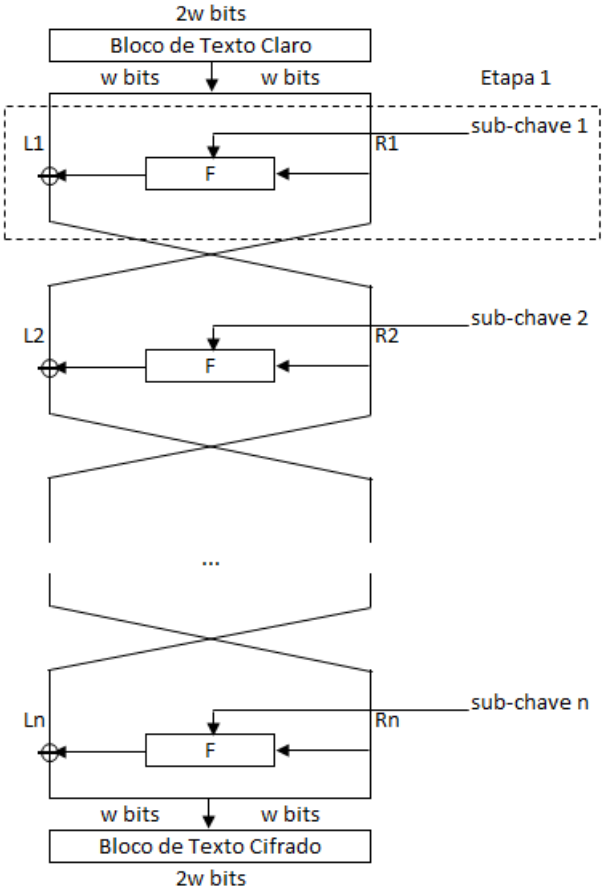


Figura 3.2: Estrutura de Feistel

DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), Blowfish, dentre outros, são exemplos de algoritmos de chave simétrica. Este trabalho apresentará um novo modelo de algoritmo de chave simétrica que não segue a Estrutura de Feistel.

DES (Data Encryption Standard)

O algoritmo DES baseia-se na estrutura de Feistel, porém com uma pequena diferença, possui uma permutação no início e sua permutação inversa correspondente no final.

O bloco de entrada do sistema, contém um texto claro de 64 bits que é transformado utilizando-se uma chave de 56 bits. São efetuadas 16 etapas, onde cada etapa possui uma sub-chave diferente, de tamanho igual à 48 bits produzida a partir da chave original. Para gerar as sub-chaves, é realizada uma permutação entre os 56 bits da chave, em seguida os bits são separados em duas metades E_0 e D_0 de 28 bits cada. A cada etapa, E_i e D_i sofrem separadamente um deslocamento circular de duas posições, exceto nas etapas de números 1, 2, 9 e 16, que possuem deslocamento de uma posição. O resultado do deslocamento efetuado nas metades servem de entrada para a geração da sub-chave da próxima entrada, além de ser utilizado como entrada para a segunda permutação que produz 48 bits de saída. Estes 48 bits correspondem a sub-chave que é utilizada como parâmetro para a função F.

Antes de ser processado pelas 16 etapas, o texto claro passa por uma permutação inicial. Ao final das 16 etapas, ocorre uma troca entre a metade dos bits do lado direito com a outra metade dos bits do lado esquerdo, a fim de que o mesmo algoritmo seja utilizado no processo de decifragem.

O bloco de texto de 64 bits é dividido em duas partes de 32 bits (L, R). Uma vez que R possui 32 bits, uma tabela de permutação/expansão é utilizada gerando 16 bits, resultando em 48 bits que sofrem a operação XOR com os 48 bits da sub-chave. Os bits resultantes em seguida são submetidos a 8 funções conhecidas por tabelas *S-box*. As tabelas *S-box* têm como entrada 6 bits e como saída 4 bits. A figura 3.4 apresenta a *S-box* S_5 utilizada no DES. Assim, após submetidos às tabelas *S-box*, os 48 bits resultarão em 32 bits. Os 32 bits de saída das tabelas *S-box* passam por uma permutação e então sofrem a operação XOR com os bits de L_{i-1}, produzindo então os bits R. Uma etapa está representada na figura 3.3, bem como a estrutura de Feistel utilizada (função F).

O DES foi o principal algoritmo de criptografia simétrica utilizado por muitos anos, porém o tamanho da chave utilizada pelo DES não é mais adequado, visto que já existem máquinas capazes de quebrar o sistema em minutos com um ataque de força bruta. Dessa forma, novas versões surgiram para contornar este problema, tais como o 2DES e o 3DES, que operam com chaves de 112 bits e 168 bits, respectivamente.

AES (Advanced Encryption Standard)

O AES trabalha com blocos de tamanho de 128 bits e utiliza chave de 128, 192 e 256 bits. O AES faz uso de uma estrutura como rede de substituição e permutação (SPN). Uma SPN utiliza etapas (*rounds*) contendo caixas de substituição conhecidas como *S-box* e caixas de permutação denominadas *P-box*, onde cada etapa geralmente é combinada com a chave através de alguma operação de grupo, como a operação XOR.

O número de etapas executadas depende do tamanho da chave. Para chave de 128, 192 ou 256 bits, são executadas 10, 12 e 14 etapas, respectivamente. O bloco de texto é formado por 128 bits que será copiado para uma matriz $S_{4\times4}$ (*State array*), onde cada

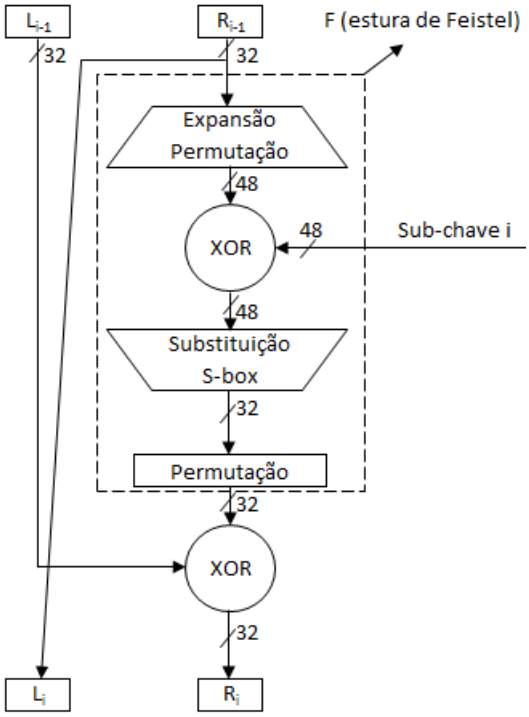


Figura 3.3: Representação de uma etapa do DES

S_5		4 bits de entrada															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Bits de saída	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0001

Figura 3.4: *S-box* S_5

célula da matriz possui 8 bits. As quatro funções executadas no processo de cifragem (tabela 3.3) e as outras quatro executadas no processo de decifragem são realizadas sobre $S_{4\times4}$, que ao final do processo de cifragem ou decifragem realiza a cópia inversa à efetuada inicialmente. Todas as etapas são formadas pelas mesmas funções, exceto a última que não contém a função *MixColumns()*.

Cifragem	Decifragem
SubBytes()	*InvSubBytes()*
ShiftRows()	*InvShiftRows()*
MixColumns()	*InvMixColumns()*
AddRoundKey()	*AddRoundKey()*

Tabela 3.3: Funções realizadas sobre $S_{4\times4}$

A figura 3.5 exibe a sequência de execução das funções em uma etapa da cifragem [National Institute of Standards and Technology 2001].

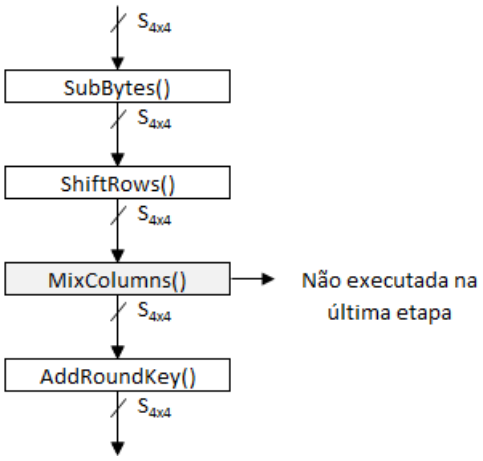


Figura 3.5: Representação de uma etapa do AES

3.4.2 Criptografia de Chave Assimétrica

Em um modelo criptográfico assimétrico, o par de chaves do modelo é composto de uma chave pública e uma chave privada. A chave pública é conhecida por qualquer indivíduo, enquanto que a chave privada é conhecida apenas pelo remetente. A chave pública e a privada estão matematicamente relacionadas, mas não podem ser derivadas uma da outra.

Algoritmos de chave pública garantem a autenticidade e a confidencialidade. Quando a chave privada é utilizada para cifrar as mensagens, garante-se que, apenas o dono da chave privada poderia ter cifrado a mensagem que foi decifrada com a chave pública, caracterizando assim a autenticidade. A confidencialidade é garantida quando, para cifrar as mensagens é utilizada a chave pública, logo apenas quem obtiver a chave privada é capaz de decifrar as mensagens.

RSA (Ron Rivest, Adi Shamir e Len Adleman) [RSA Laboratories 2000], DSA (Digital Signature Algorithm) [RSA Laboratories 2000], Diffie-Hellman, dentre outros, são exemplos de modelos criptográficos de chave assimétrica.

3.5 Criptoanálise

A criptoanálise se encarrega de encontrar fraquezas nos métodos criptográficos, e quem pratica a criptoanálise é denominado criptoanalista.

A expressão "quebrar um sistema criptográfico" não significa exatamente que o criptoanalista conseguirá ter acesso completo ao texto cifrado, mas sim a parte dele, ou ainda descobrir que o espaço de chaves do sistema é menor do que se esperava, ou descobrir parte da chave que foi utilizada para cifragem. Para isto, o criptoanalista pode utilizar diversas estratégias que dependem do esquema do sistema criptográfico utilizado e da quantidade disponível de informação.

Existem diversos tipos de ataques que podem ser realizados nos sistemas criptográficos

e podem ser classificados de acordo com a disponibilidade de informações que podem ser obtidas pelo criptoanalista, conforme pode ser visto na tabela 3.4 [Conrad 2007].

Informação	Tipo de Ataque		
Texto claro	Texto claro conhecido	Texto claro escolhido	Texto claro escolhido adaptável
Texto cifrado	Apenas texto cifrado	Texto cifrado escolhido	Texto cifrado escolhido adaptável

Tabela 3.4: Principais tipos de ataques

Texto claro conhecido (*known plaintext*): é um tipo de ataque no qual o criptoanalista tem acesso ao texto claro e o seu texto cifrado correspondente e procura uma correlação entre os dois.

Apenas texto cifrado (*ciphertext-only*): é um tipo de ataque no qual o criptoanalista tem acesso ao texto cifrado, mas não tem acesso ao texto claro. Em métodos criptográficos simples, como a cifra de Caesar, através de uma análise de frequência é possível quebrar o sistema criptográfico.

Texto claro escolhido (*chosen plaintext*): é um tipo de ataque no qual o criptoanalista pode cifrar um texto claro de sua escolha e estudar o texto cifrado resultante. Este é o ataque mais conhecido contra sistemas criptográficos assimétricos, no qual o criptoanalista tem acesso à chave pública.

Texto cifrado escolhido (*chosen ciphertext*): é um tipo de ataque no qual o criptoanalista escolhe um texto cifrado e tenta encontrar um texto claro correspondente. Isto pode ser feito através de uma máquina que decifra sem expor a chave. Este também é utilizado em métodos de cifragem de chave pública.

A criptoanálise diferencial e a linear são dois métodos que merecem destaque no estudo da criptoanálise. As próximas seções apresentarão uma descrição de cada um dos métodos.

Outra forma de criptoanálise é o ataque de força bruta, conhecido como *brute force attack*, que consiste em testar sistematicamente todo espaço de chaves possíveis. Este método é geralmente utilizado em ataques do tipo texto claro conhecido ou do tipo apenas texto cifrado.

3.5.1 Criptoanálise Diferencial

A criptoanálise diferencial é um ataque do tipo texto claro escolhido, principalmente aplicado em métodos de cifragem por blocos, mas também em cifradores de fluxo e funções hash criptográficas. De maneira geral, a criptoanálise diferencial estuda como as diferenças realizadas na entrada podem afetar a diferença resultante na saída [Natarajan 2002].

A ideia básica do método é usar pares de texto claro relacionados por uma diferença constante. A diferença pode ser definida de várias maneiras, mas a operação $\oplus$ (*XOR, ou exclusivo*) é mais frequente. O criptoanalista então calcula as diferenças dos textos cifrados correspondentes, na esperança de detectar padrões estatísticos em sua distribuição.

3.5.2 Criptoanálise Linear

A criptoanálise linear é um ataque do tipo texto claro conhecido, foi criada por Matsui em 1994 e teve como alvo o algoritmo criptográfico DES [Matsui 1994]. O método tenta tirar vantagem da alta probabilidade de ocorrer uma expressão linear entre os bits do texto claro, texto cifrado e a sub-chave.

A ideia básica é aproximar uma porção do texto cifrado e texto claro com uma expressão linear, onde a linearidade diz respeito a operação $\oplus$ (*XOR, ou exclusivo*), tal como a expressão apresentada abaixo:

$$X_{i_1} \oplus X_{i_2} \oplus ... \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus ... \oplus Y_{j_v} = 0 \tag{3.1}$$

Onde X_i representa o i-ésimo bit da entrada $X = [X_1, X_2, ...]$ e Y_j representa j-ésimo bit da saída $Y = [Y_1, Y_2, ...]$. Esta equação indica a soma do operador XOR entre os "u" bits de entrada e os "v" bits de saída.

Se o sistema criptográfico apresentar uma tendência para a equação 3.1 ocorrer com alta ou baixa probabilidade, este sistema possui grande dificuldade em tornar o texto cifrado aleatório, tornando-se vulnerável ao ataque.

3.6 Considerações em Relação ao Modelo Criptográfico Proposto

Neste capítulo foram apresentados definições e alguns modelos criptográficos tradicionais, com o intuito de contextualizar e contrastar com o modelo proposto que será apresentado mais adiante. Como pode ser visto nos exemplos de modelos apresentados, a cifragem é tradicionalmente realizada através de transposições e operações XOR do texto claro, diferentemente do modelo deste trabalho, que utiliza a estrutura de ACs. Apesar do processo de cifragem/decifragem não se assemelhar aos modelos tradicionais, o modelo deste trabalho pertence a classe dos algoritmos que realizam a cifragem por bloco e utilizam chave simétrica. A criptoanálise diferencial ajudou a realizar testes a fim de verificar a validade e a segurança do método proposto.

Capítulo 4

Métodos Criptográficos Correlatos

Neste capítulo serão apresentados métodos relacionados ao modelo proposto, e será dividido em duas seções. Na primeira seção, será realizada uma revisão de trabalhos envolvendo métodos de cifragem de imagens e na segunda seção será feita uma revisão de trabalhos anteriores que aplicam ACs em criptografia de uma forma geral.

4.1 Criptografia de Imagens

Imagens possuem características intrínsecas, tais como o grande volume de informação e alta redundância de dados, o que muitas vezes não é encontrada em texto lineares. Portanto, a proposição de métodos específicos para cifragem de imagens se torna importante, visto que buscam melhorar estes aspectos não abordados nos métodos tradicionais de textos lineares. A seguir são apresentados modelos criptográficos específicos para imagens encontrados na literatura.

O método proposto em [Zeghid et al. 2007], sugere uma alteração no método tradicional AES para adequá-lo à cifragem de imagens. A modificação é realizada pela adição de um gerador de chaves no algoritmo de cifragem do AES. Embora seja proposto na cifragem de imagens, o método utiliza uma cifragem linear em blocos, sendo assim, não utiliza a informação espacial da imagem no processo de cifragem.

Na referência [Socek et al. 2005], propõe-se o melhoramento do CKBA (Chaotic-Key Based Algorithm) que é baseado em um mapa caótico unidimensional [J.C. Yen 2000] e proposto originalmente para cifragem de textos lineares. O melhoramento é conseguido de três formas: i) a troca do mapa caótico Logistic de 1-D por um mapa caótico linear Piecewise; ii) aumento do tamanho da chave para 128 bits; iii) adicionadas mais duas primitivas de criptografia e aumento do esquema de operar em múltiplos *rounds*. Apesar das alterações propostas, o método ainda é realizado em uma única dimensão, de forma que a informação espacial também é perdida nesse método.

Em [Chen et al. 2004], é apresentado um método de criptografia no qual a cifragem de imagens é realizada através de mapas caóticos. Diferente dos demais métodos, este

utiliza um mapeamento em três dimensões. Segundo [Chen et al. 2004], a cifragem é propagada por toda a imagem através do mapa caótico 3D. Um segundo mapa é utilizado para embaralhar a relação entre a imagem cifrada e a imagem plana.

A cifragem de imagens a partir de um AC unidimensional é proposta em [Yu et al. 2008]. Antes do processo de cifragem, a imagem e a chave são divididas em duas partes H e L, onde H possui a metade mais significativa dos bits e L outra metade com os bits menos significativos. O procedimento de cifragem/decifragem difere em apenas dois pontos, um na direção da rotação dos registradores, e outro, na ordem da operação de rotação com a operação XOR. Este método utiliza ACs na cifragem, entretanto, utiliza uma única dimensão e o processo de cifragem não é realizado através do cálculo de pré-imagens, mas através de rotações e de aplicações do operador XOR. Além disso, a cifragem proposta também é linear.

O método proposto em [Maleki et al. 2008] aborda a utilização de um tipo especial de AC unidimensional que utiliza um mecanismo de memória, porém neste método há perda de dados no processo de cifragem/decifragem. Segundo o autor essa perda de dados tem como objetivo aumentar a segurança do método e não prejudica o visual da imagem após o processo de cifragem/decifragem. O método proposto nesta dissertação visa manter a integridade total da imagem, ou seja, sem perda de dados.

Machhout e colegas (2009) propõem um modelo criptográfico que utiliza um AC 2D com vizinhança von Neumann. A ideia básica do método é substituir o valor dos pixels da imagem através de operações XOR com valores gerados a partir de um AC 2D, ou seja, o processo de cifragem é realizado pela operação XOR. Apesar do método empregar um AC 2D, ele apenas o utiliza como um gerador de números aleatórios diferenciando do modelo proposto neste trabalho, que efetivamente usa a estrutura espacial do AC 2D no contexto da cifragem/decifragem, [Machhout et al. 2009].

O modelo proposto em [Encinas et al. 2002] também utiliza um AC 2D e a vizinhança empregada no método é a de Moore. O espaço celular do modelo é a imagem, o conjunto de estados do autômato é definido pela quantidade de cores da imagem e, a chave do sistema é composta pelo número de iterações que será utilizada pelo AC e a quantidade de cores utilizada no sistema. O sistema utiliza AC no processo, porém a cifragem não é realizada através do cálculo de pré-imagem, como no algoritmo aqui proposto.

Jun (2009) propõe um modelo criptográfico que utiliza um autômato celular elementar (AC unidimensional binário de raio 1). O artigo exemplifica o processo de cifragem em imagens em escala de cinza que possuem 256 tonalidades, porém não especifica como esse modelo poderia ser portado para ser utilizado em imagens com um maior número de cores, além de utilizar um modelo unidimensional de AC [Jun 2009].

Na referência [Chen e Lai 2007], propõe-se um novo modelo criptográfico em que a ideia básica consiste em fazer transformações nos valores dos pixels da imagem, pela modificação e substituição realizadas por um AC. Neste modelo um AC 2D também é

utilizado, porém serve apenas para geração de números aleatórios, diferente do modelo proposto no presente trabalho.

Em [Blundo et al. 2000] e [Hou 2003] também são descritos modelos de criptografia de imagens, porém diferentemente dos descritos acima, estes métodos adotam uma criptografia visual, que é uma vertente da criptografia de imagens, criada por Naor e Shamir. A criptografia visual propõe um modelo onde um conjunto pré-definido de participantes pode decodificar a imagem sem nenhum conhecimento de criptografia e sem realizar qualquer tipo de computação, a imagem original pode ser vista através da superposição das camadas criadas no processo de cifragem. O método do artigo restringe o universo de utilização, uma vez que não é necessário um método computacional para realizar a decifragem.

O método aqui investigado neste projeto emprega uma cifragem espacial através de ACs bidimensionais, o que não ocorre em [Zeghid et al. 2007], [Socek et al. 2005] e [Yu et al. 2008] que adotam uma cifragem linear. Este trabalho propõe um modelo em que a cifragem e a decifragem podem ser realizadas de forma paralela, uma característica que não pode ser observada em [Chen et al. 2004]. Apesar dos métodos propostos em [Yu et al. 2008], [Maleki et al. 2008], [Jun 2009] utilizarem ACs no processo de criptografia, além dos mesmos serem unidimensionais, não se assemelham ao deste trabalho, uma vez que não utiliza o calculo de pré-imagens para fazê-lo. Apesar dos modelos proposto em [Chen e Lai 2007], [Encinas et al. 2002] e [Machhout et al. 2009] utilizarem ACs bidimensionais, efetivamente não utilizam a estrutura espacial do AC 2D para realizar a cifragem, mas apenas para gerarem valores aleatórios para posteriormente serem aplicados na cifragem.

4.2 Métodos de Criptografia Baseados em ACs

Wolfram (1986) propôs um modelo pioneiro de cifragem por fluxo baseado em ACs, [Wolfram 1986]. A ideia principal é utilizar um autômato celular binário unidimensional com condição de contorno periódica, capaz de gerar sequências de bits o mais aleatório possível, dado um reticulado inicial de tamanho N. A chave criptográfica deste sistema criptográfico são os N bits que correspondem ao reticulado inicial. Os valores do reticulado são atualizados de forma síncrona em passos de tempo discreto de acordo com a regra elementar 30. Esta regra é não-aditiva e tem uma dinâmica classificada como caótica. Uma "coluna" da evolução temporal do AC unidimensional (ou seja, a evolução de uma única célula) é utilizada para gerar uma palavra aleatória que é combinada com o texto plano para gerar o texto cifrado. A figura 4.1 exemplifica o esquema de cifragem proposto por Wolfram (1986).

Em [Nandi et al. 1994], é proposto um modelo de criptografia baseado nas propriedades algébricas dos ACs aditivos heterogêneos. O método utiliza ACs aditivos de grupo com ciclo de duração não-máxima com n ciclos de tamanho x, onde x é par e é

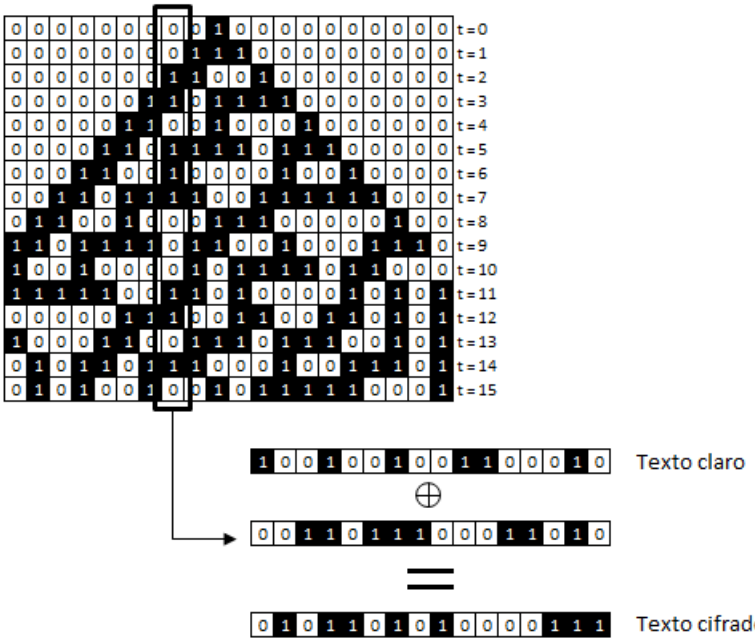


Figura 4.1: Esquema de cifragem proposto por Wolfram (1986)

uma potência de 2. O método consiste em montar p funções de cifragem E_i, $i = 1, ..., p$, em que, cada uma das funções é composta por q transformações fundamentais, onde cada transformação fundamental é um arranjo composto pelas regras elementares 51, 153 e 191, formando assim um vetor de regras de tamanho N. Cada uma dessas transformações geram ciclo de tamanho 8. Dessa forma, o processo de cifragem é obtido pela evolução do reticulado inicial M por 4 passos de tempo, para cada transformação fundamental. Logo o texto cifrado C é obtido por $C = (v(u(z(y(s(M))))))$, onde v, u, z, y e s são as transformações fundamentais. Para o processo de decifragem, é necessário evoluir cada uma das transformações fundamentais por mais 4 passos de tempo na ordem inversa, portanto: $M = (s(y(z(u(v(C))))))$.

Gutowitz (1995) propôs um sistema criptográfico, de cifragem em bloco, baseado na teoria dos sistemas dinâmicos [Wolfram 1984]. O modelo utiliza-se do calculo de pré-imagens para cifrar a mensagem e através da evolução temporal para frente pode-se decifrar a mensagem. As regras a serem utilizadas devem possuir sensitividade a uma das extremidades ou em ambas, pois assim é possível garantir a geração da pré-imagem. A regra de transição do autômato é utilizada como chave do sistema criptográfico. O reticulado inicial corresponde a um bloco da mensagem a ser cifrada. Nesse método o texto cifrado tem um tamanho maior que o texto original. Este modelo será melhor detalhado na seção 4.2.1, uma vez que serviu de base para este trabalho.

Oliveira e colaboradores (2004) apresentaram uma proposta para resolver um problema identificado como a propagação de perturbação no modelo de Gutowitz. A solução foi utilizar regras com sensitividade bidirecional no lugar de regras com sensitividade em apenas uma das extremidades. Neste caso o cálculo de pré-imagem pode começar com bits

iniciais consecutivos em qualquer célula da pré-imagem, e então, os demais bits decorrem da utilização da regra. Entretanto, nesse método, assim como no modelo de Gutowitz, o texto cifrado permanece com um tamanho maior que o texto original.

Macedo (2007) apresenta um modelo baseado em ACs caóticos, não homogêneos e não aditivos. A cifragem é obtida através do cálculo de pré-imagem, assim como nos modelos apresentados em [Gutowitz 1995] e [Oliveira et al. 2004], porém soluciona o problema de aumento do texto após a cifragem. Esse problema é resolvido utilizando-se duas regras no processo de cifragem, uma das regras é caótica e sensível a um dos bits (ou ambos) utilizada para propagar a perturbação, enquanto que a outra é ponto-fixo e produz apenas um deslocamento dos bits, contudo garante a existência da pré-imagem. Este modelo é a base deste trabalho e será detalhado na seção 4.2.2.

Em [Oliveira et al. 2010a], [Oliveira et al. 2010b] e [Oliveira et al. 2010c], é proposto e investigado um novo método de cifragem simétrica que utiliza ACs unidimensionais. O processo de cifragem utiliza o cálculo de pré-imagem, assim como o modelo desta dissertação, porém a regra de transição utilizada no processo não necessita ser sensível à um dos extremos. Logo, dado um reticulado e uma regra de transição, pode ser que a pré-imagem não exista. Para contornar este problema, o método aumenta o tamanho do reticulado quando necessário, garantindo assim sempre a realização da cifragem. O resultado é que o texto cifrado possui um tamanho variável, podendo ter o comprimento do texto original ou o comprimento do texto cifrado no método do Gutowitz. Entretanto, através de uma especificação adequada da chave [Oliveira et al. 2010c], o texto cifrado tende ao tamanho do texto plano.

Wolfram (1986) utiliza ACs apenas para gerar uma sequência aleatória para posteriormente ser aplicado no método criptográfico, o que diverge do trabalho proposto, que efetivamente utiliza os ACs no processo de cifragem/decifragem. Diferentemente de [Nandi et al. 1994] que utiliza ACs aditivos, este trabalho utiliza ACs não aditivos. Este trabalho propõe uma variação do método em [de Macedo 2007], porém utiliza duas dimensões. Os problemas encontrados em [Gutowitz 1995] e [Oliveira et al. 2004] são solucionados uma vez que o método aqui investigado herda as características do método em [de Macedo 2007]. Enquanto o método em [de Macedo 2007] utiliza um AC unidimensional, o método investigado nesse trabalho utiliza um AC bidimensional, tornando-o mais adequado à cifragem de imagens.

4.2.1 Método proposto por Gutowitz

A ideia mais direta para se utilizar ACs como método de criptografia, seria considerar o texto claro como reticulado inicial e aplicar uma regra de transição por alguns passos de iteração até se chegar no texto cifrado. Em seguida, seria necessário um esquema para decifrar, para que pudesse obter o texto claro novamente. Para que isso seja possível,

a regra do AC deveria ser reversível, ou seja, para dado qualquer reticulado inicial é possível calcular sua pré-imagem e esta deve ser única. No entanto o modelo proposto por Gutowitz (1995) utiliza o caminho inverso, ou seja, realiza a cifragem através do cálculo de pré-imagens.

Nesse modelo, o texto claro é o reticulado de um AC. Então, uma pré-imagem possível é obtida a partir deste reticulado. Este processo é repetido por algumas iterações (n) até que se chegue a um possível reticulado que seja associado à n-ésima pré-imagem, que será o texto cifrado. Posteriormente, se for aplicada a evolução temporal para frente (*forward*) com a mesma regra sobre o reticulado que representa o texto cifrado, após o mesmo número de iterações, chega-se ao texto claro.

Porém para que o esquema de cifragem funcione, a regra de transição do AC escolhida necessariamente deve garantir a existência de pelo menos uma pré-imagem para qualquer reticulado e que seja possível calculá-la. Para isso, Gutowitz utilizou da característica da sensitividade das regras de transições, vista no capítulo 2. A característica de uma regra de transição ser sensível a um dos extremos permite que seja calculado uma das pré-imagens do reticulado, a partir de um pedaço do reticulado iniciado aleatoriamente.

Por exemplo, seja a regra de transição elementar 30 (figura 4.2) e o reticulado da figura 4.3. Para iniciar o cálculo da pré-imagem, 1 bit é adicionado em cada extremidade do reticulado. Devido à regra escolhida ser sensível à esquerda, os dois bits que deverão ser escolhidos aleatoriamente serão os bits mais à direita da pré-imagem. Se a regra fosse sensível ao bit da direita, o cálculo deveria iniciar com os bits mais à esquerda da pré-imagem. Neste exemplo foram escolhidos os bits iniciais "00". Após a escolha das células inicias, os demais bits da pré-imagem decorrem a partir da regra de transição e do reticulado utilizado como base. Para determinar o estado da próxima célula à esquerda da pré-imagem, busca-se na regra de transição a vizinhança cujo estado da célula central é "0", à direita é "0" e que resulte como estado da célula central, o bit de saída "0". No caso deste exemplo que utiliza da regra 30, trata-se da transição $\underline{0}00 \rightarrow 0$, pois a transição da outra vizinhança possível é $\underline{1}00 \rightarrow 1$. Portanto, o estado da célula a esquerda é obtido de forma determinista e neste caso é "0". Uma vez obtido o valor da terceira célula da direita para a esquerda, o próximo passo é calcular o valor da quarta célula e assim sucessivamente até o preenchimento total da pré-imagem. A característica da regra de transição ser sensível, garante que todas as células da pré-imagem podem ser obtidas de forma determinista. Ao final, as células acrescentadas na pré-imagem são mantidas no reticulado.

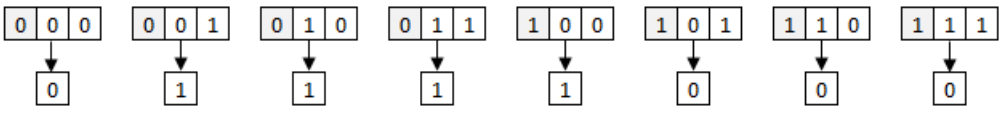


Figura 4.2: Regra 30

Uma observação importante a ser considerada no modelo proposto por Gutowitz é o

aumento do reticulado a cada pré-imagem calculada. O aumento do tamanho (δ) é uma função do raio r da regra de transição, de modo que $\delta = 2 \times r$. Dado um reticulado inicial de tamanho tr_0, o tamanho do reticulado final, em P passos de cálculo de pré-imagem, é dado por $tr_n = P \times \delta + tr_0$.

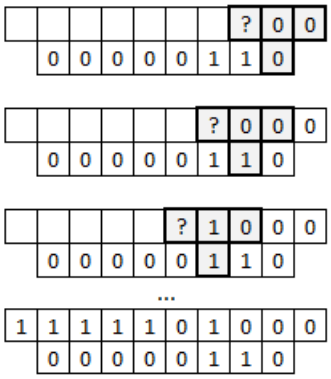


Figura 4.3: Exemplo evolução reticulado a partir da regra 30

No modelo proposto por Gutowitz, as chaves devem ser sempre regras de ACs sensíveis a um dos bits extremos. Seja o reticulado dado pelo texto claro a ser cifrado. Calculam-se pré-imagens sucessivamente, iniciando-se os primeiros bits da pré-imagem (δ células) durante P passos de cifragem. O texto cifrado é dado pelo último reticulado obtido no n-ésimo passo. O processo de decifragem prevê que o agente que estiver recebendo o texto cifrado conheça também a regra do AC e o número de passos utilizados na cifragem. O espaço de chaves do método é definido pelo tamanho da vizinhança (m) utilizado no método e pode ser definido por $2^{2^{m-1}}$.

Após a realização de testes, Gutowitz percebeu que o método possuía uma falha que poderia ser explorada por um criptoanalista. Ao cifrar um texto qualquer e em seguida realizar uma perturbação no texto inicial e cifrá-lo novamente, após realizar a operação *XOR* entre os dois textos cifrados, ele constatou que a perturbação do reticulado propaga-se para o lado da sensitividade, permanecendo igual no lado oposto. Logo, esta falha poderia tornar o método menos confiável. A figura 4.4 ilustra esse problema, para o exemplo foi utilizada a regra transição {10101001} sensível à direita. A perturbação do reticulado representado na figura 4.4 (a) ocorreu na quarta célula. Na figura 4.4 (b), as células que sofreram alteração estão representadas por "#", enquanto que as células que não foram modificadas estão representadas por "-". Para resolver este problema, Gutowitz propôs um algoritmo em duas fases. Na primeira, a cadeia binária da chave (núcleo da regra) é utilizada na configuração de uma regra de transição com sensitividade à esquerda, que é aplicada por 32 passos. Na segunda fase, uma regra com sensitividade à direita é configurada a partir da mesma chave (mesmo núcleo) e é aplicada também por 32 passos. Gutowitz sugeriu a utilização de um AC de raio de tamanho 5, o que resulta em chaves de 1024 bits.

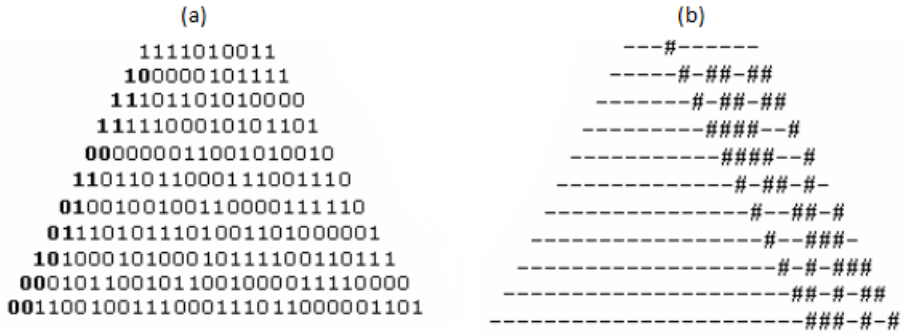


Figura 4.4: (a) Evoluções reticulado (b) Propagação da perturbação

4.2.2 Método Unidimensional da Patente PI0703188-2

O modelo investigado em [de Macedo 2007] foi registrado como solicitação de patente no INPI (Instituto Nacional de Propriedade Industrial) em setembro de 2007 e recebe o registro PI0703188-2 [Oliveira e Macedo 2007]. Este método é baseado no modelo proposto por Gutowitz e também é um sistema simétrico de cifragem por blocos baseados em regras de ACs com sensitividade ao extremo. Sua grande vantagem em relação ao modelo de Gutowitz é o não aumento do reticulado durante a etapa de cifragem. A maior mudança em relação ao modelo anterior é o fato de serem utilizadas duas regras de transição ao invés de uma única.

Uma das regras utilizadas no método é utilizada apenas nas células dos extremos do reticulado e é denominada por *regra de contorno*. O número de células que representam a região de contorno é dado por $(2 \times r)$, onde r é o tamanho do raio utilizado. Esta regra é responsável por fazer com que não sejam necessários bits adicionais a cada passo do cálculo de pré-imagem. Sendo assim, esta regra garante que qualquer reticulado inicial possua uma pré-imagem de mesmo tamanho.

A outra regra utilizada no modelo é responsável pela caoticidade do AC. Portanto, é esta regra que realiza de fato o processo de cifragem através do cálculo de pré-imagens. Esta regra de transição é denominada por *regra principal*. A regra principal é aplicada na atualização de todas as células do reticulado, exceto nas células que estão na região de contorno. Assim como no método proposto por Gutowitz, a regra principal deve ser sensível a um dos extremos.

O espaço de regras de contorno é formado por apenas 4 regras, independentemente do tamanho do raio utilizado, sendo que duas delas são sensíveis à esquerda e as outras duas são sensíveis à direita. A figura 4.5 mostra o formato das possíveis regras de contorno, tanto sensíveis a direita, quanto sensíveis à esquerda. Para as duas regras sensíveis à esquerda, metade dos bits são 1s e a outra metade são 0s, e vice-versa. Para as outras duas regras que são sensíveis à direita, os bits ocorrem intercalados, uma iniciando em 1, e a outra regra iniciando em 0. A figura 4.6 apresenta as quatro regras de contorno existentes no caso dos ACs unidimensionais de raio 1.

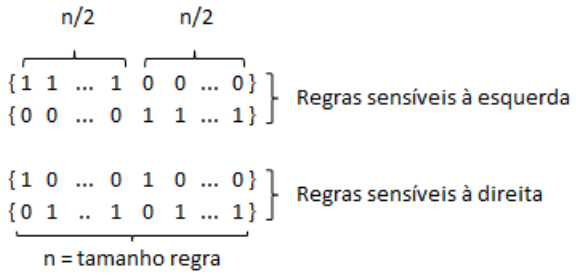


Figura 4.5: Espaço das regras de contorno possíveis em qualquer raio

A regra de contorno que será utilizada no método de cifragem deve obedecer a mesma sensitividade da regra principal, pois dessa forma será possível extrair uma maior paralelismo do método. Além disso, o primeiro bit da regra de contorno deverá ser complementar ao primeiro bit da regra principal, em [de Macedo 2007] foi comprovado através de testes que esta operação proporciona uma melhor cifragem. Por exemplo, se o primeiro bit da regra principal for 1 e ela for sensível à direita, então a regra de contorno será a que iniciar em 0 e possuir a mesma sensitividade (quarta regra da figura 4.6). Caso a regra principal inicie com 0, então a regra de contorno a ser escolhida deverá ser a que possui a mesma sensitividade e inicie em 1 (primeira regra da figura 4.6). Suponha a regra principal {01001011} sensível a esquerda, logo a regra de contorno será a regra {11110000}, que é sensível à esquerda e inicia com o bit oposto ao da regra principal.

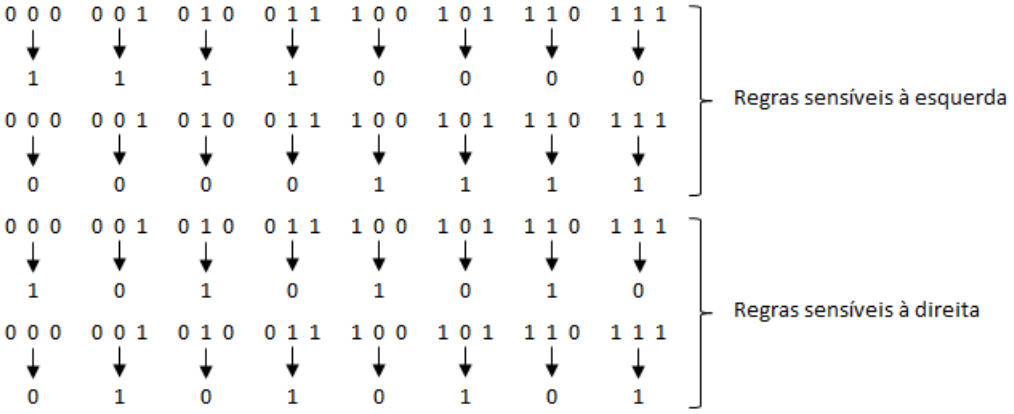


Figura 4.6: Espaço das regras de contorno possíveis para raio 1

A ideia principal do método de cifragem baseia-se no modelo inicial proposto por Gutowitz, ou seja, o texto claro é o reticulado inicial do AC e o texto cifrado é obtido após n passos do cálculo de pré-imagens. Entretanto, duas regras são aplicadas no reticulado ao invés de uma única: a regra principal e a regra de contorno.

Antes de ser explicada a versão final do modelo proposto por Macedo (2007), será apresentada a versão inicial do modelo para facilitar a compreensão dos modelos. Nesta primeira versão, a idéia principal consiste em apenas aplicar a regra principal em todas as células do reticulado, exceto naquelas pertencentes à região de contorno.

A figura 4.7 mostra um exemplo do cálculo de uma pré-imagem pelo modelo básico,

utilizando-se um AC de raio 1. A figura 4.7 (a) exibe o reticulado inicial {0100101} e a pré-imagem, onde os bits $p1$, $p2$, ... e $p7$ representam os bits da pré-imagem a serem encontrados. A quantidade de células que utilizará a regra de contorno é definida por $(2 \times r)$, onde r é o raio. Portanto, para o exemplo, devido ao AC utilizar uma regra de raio 1, a quantidade de células que utilizará a regra de contorno será 2. Devido à regra principal ser sensível à esquerda, o cálculo da pré-imagem deverá ser realizado da direita para a esquerda. As duas células do reticulado que são atualizadas pela regra de contorno estão destacadas nas figura 4.7 (a). Os bits $p1$ e $p7$ são determinados pela regra de contorno e dependem exclusivamente do bit de saída. Ou seja, para o bit $p1$ é necessário descobrir qual vizinhança da regra de contorno leva ao bit 1 presente no reticulado. Neste caso, devido à característica da regra de contorno, as únicas possibilidades são as vizinhanças que iniciam em 0, portanto o valor do bit $p1$ será 0. Seguindo o mesmo raciocínio, o valor do bit $p7$ é 1, uma vez que as às únicas vizinhanças da regra de contorno que resultam no bit de saída 0, iniciam com o bit 1. Obtidos os bits iniciais, o cálculo segue do bit $p2$ até o bit $p6$ utilizando-se a regra principal, que é sempre determinista ao definir o próximo bit da vizinhança esquerda. Na figura 4.7 (c) o valor do bit $p6$ é 0, pois a única vizinhança, do tipo {?10}, que resulta no bit de saída 1, é a {010}. O cálculo da pré-imagem é finalizado quando todas as células forem calculadas, como pode ser visto na figura 4.7 (g). Utilizando-se esse cálculo, a pré-imagem sempre existe, é única e preserva o tamanho do reticulado inicial.

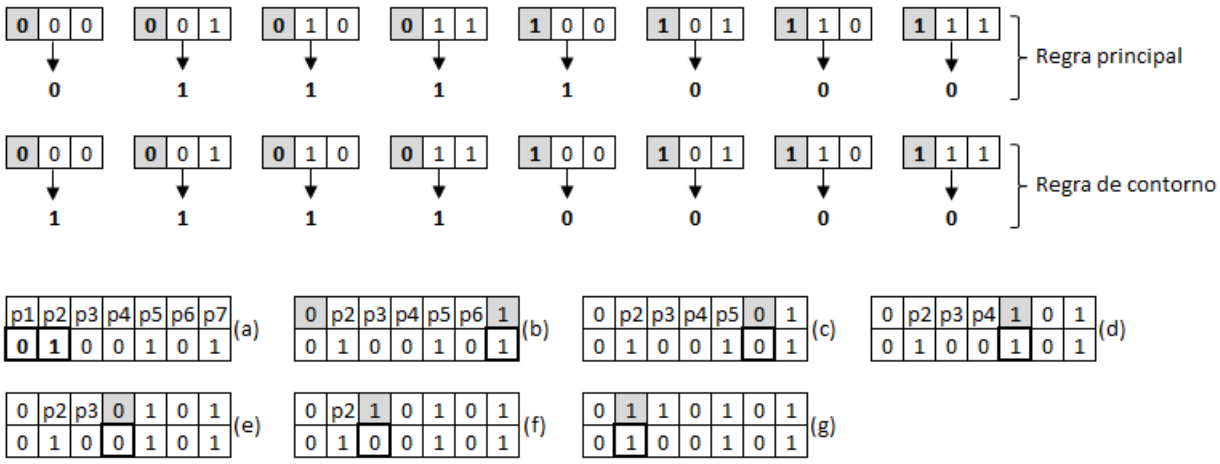


Figura 4.7: Cálculo pré-imagem modelo básico proposto em [de Macedo 2007]

Para o modelo final, duas modificações foram realizadas no modelo inicial: o deslocamento da borda do reticulado e a rotação do núcleo da regra.

O deslocamento da borda do reticulado visa aumentar o paralelismo no cálculo de várias pré-imagens, mas também contribui no aumento da propagação de perturbações na cifragem. Devido ao AC do modelo utilizar um contorno periódico, o cálculo da pré-imagem pode ser iniciado em qualquer posição do reticulado. Aplicando-se o deslocamento da borda, a cada cálculo de pré-imagem, a célula de início do cálculo deverá ser deslocada

em $(r + 1)$ posições, onde r é o tamanho do raio. Com esse deslocamento o cálculo da próxima pré-imagem pode iniciar, sem que o cálculo da pré-imagem anterior tenha finalizado, garantindo assim que os próximos cálculos de pré-imagens possam ser executados simultaneamente, caso o método fosse implementado em um hardware paralelo. A figura 4.8 exibe um reticulado sendo calculado por um AC de raio 1 com uma regra principal sensível ao bit da esquerda. Note que as células pintadas de cinza representam as células que estão sendo calculadas ao mesmo tempo, e as células com a borda destacada representam as células da região de contorno e um início de cálculo de uma pré-imagem. Na figura 4.8 (d), o cálculo da segunda pré-imagem iniciou antes de terminar o cálculo da primeira pré-imagem, pois já havia células necessárias para fazê-lo. Da mesma forma, o cálculo da terceira pré-imagem é iniciado antes mesmo antes da primeira pré-imagem ser finalizada (figura 4.8 (d)). Na figura 4.8(g) é possível observar que quando a primeira pré-imagem é completada, as outras duas pré-imagens estão adiantadas. A figura 4.8 (h) exibe o momento em que a última célula da terceira pré-imagem é calculada.

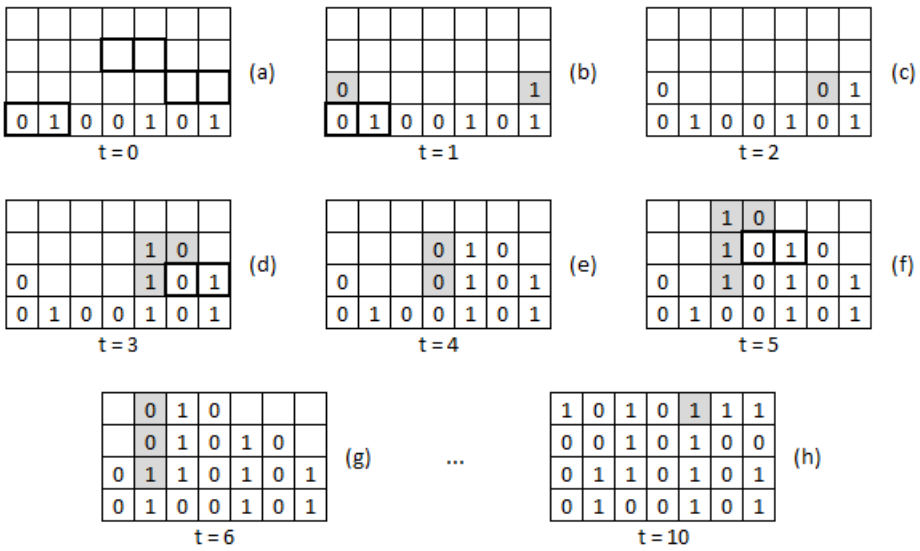


Figura 4.8: Cálculo pré-imagem em paralelo

A rotação do núcleo da regra tem como objetivo, exclusivamente, aumentar a aleatoriedade do método, contribuindo assim para o aumento da qualidade do texto cifrado, que foi avaliado experimentalmente em [de Macedo 2007]. A cada cálculo de uma pré-imagem, o núcleo da regra inicial é rotacionado para esquerda e uma nova regra principal e de contorno são criadas. Por exemplo, suponha a regra principal inicial {01111000} sensível à esquerda, logo seu núcleo é definido por {0111}. Após uma rotação do núcleo para a esquerda, o novo núcleo será {1110}, originando a seguinte regra principal {11100001} sensível à esquerda. Para a evolução para frente, basta rotacionar o núcleo da regra para a direita realizando assim o processo inverso.

Para exemplificar o processo de cifragem da versão final, serão realizados 3 cálculos de pré-imagem, utilizando-se as regras de transição da figura 4.9 e o mesmo reticulado inicial

da figura 4.8 (a). Devido ao raio da regra inicial ser igual a 1, o número de células que utilizarão a regra de contorno será igual a 2. Primeiramente seleciona-se qualquer bit do reticulado para iniciar o cálculo da pré-imagem. Neste exemplo, o cálculo será iniciado na segunda célula do reticulado como pode ser visto na figura 4.10 (a). As letras A, B e C, que podem ser vistas na figura 4.9, representam as regras principais obtidas pela rotação do núcleo da regra, enquanto as letras D e E, representam as regras de contorno que são utilizadas. Iniciando o cálculo da pré-imagem, seleciona-se a regra principal inicial (regra A) e sua regra de contorno (regra E). Para obter o valor da primeira célula da pré-imagem é necessário descobrir qual vizinhança da regra de contorno leva para o bit 1. Devido à definição das regras de contorno, qualquer uma das vizinhanças {**0**00}, {**0**01}, {**0**10}, {**0**11}, leva ao bit de saída 1, então o único valor possível para o primeiro bit da pré-imagem é 0. Em virtude do método utilizar uma condição de contorno periódica e o exemplo utilizar uma regra sensível à esquerda, o proximo bit da pré-imagem a ser calculado é o da esquerda, sétimo bit da pré-imagem. Realizando a mesma operação anterior, é possível concluir que as vizinhanças possíveis da regra E que resultam em 0, são: {**1**00}, {**1**01}, {**1**10}, {**1**11}. Logo o único valor possível para o sétimo bit é 1. Após ter calculado os bits de contorno, os bits restantes do reticulado utilizarão a regra principal (a regra A). Para realizar o cálculo do sexto bit do reticulado será necessário encontrar a vizinhança que resulta em 0 e termina em 10. A única vizinhança possível é a {**0**10}, logo o valor do sexto bit é 0. O cálculo da primeira pré-imagem estará finalizado assim que os demais bits tiverem seus valores computados. Note na figura 4.10 (d) que não é necessário esperar o termino do cálculo da primeira pré-imagem, para que o cálculo da segunda pré-imagem seja iniciado. Dessa forma, o método pode ser paralelizado reduzindo o tempo de cifragem. Para iniciar o cálculo da segunda pré-imagem é necessário realizar uma rotação para a esquerda do núcleo da regra, obtendo então a regra B como principal (figura 4.9) e a regra D como contorno. Seguindo os mesmos passos descritos acima, obtém-se os 2 primeiros bits a partir da regra de contorno (regra D) e em seguida calcula-se os demais bits a partir da regra principal B. O processo de cifragem é finalizado assim que último bit da última pré-imagem é calculado, como pode ser visto na figura 4.10 (k). É possível perceber pelo exemplo que apenas 10 passos de tempo são necessários para cifrar 21 células (7 por pré-imagem, destacando-se o paralelismo do método).

Para o processo de decifragem basta apenas realizar a evolução temporal para frente utilizando as regras de contorno e as regras principais, lembrando que a cada evolução o núcleo da regra deverá ser rotacionado para direita, ao invés da esquerda, além da borda também ser deslocada no sentido contrário.

A configuração padrão proposta utiliza blocos de 128 bits, regras de transição de raio 4 e 128 passos de pré-imagens. Como o núcleo tem 256 bits, o espaço de chaves é de 2^{256}.

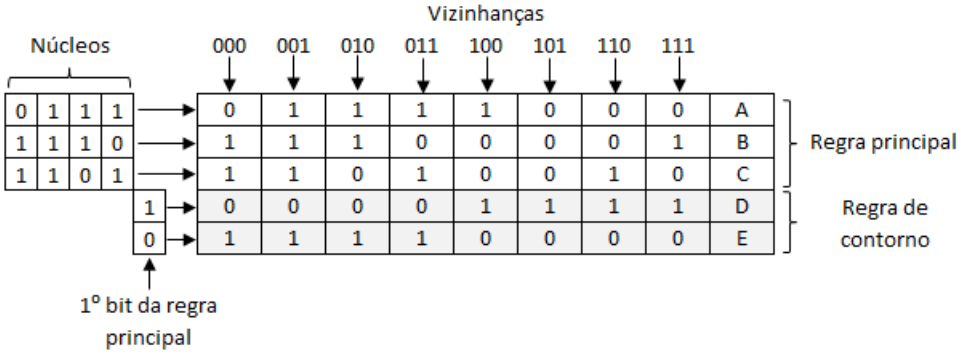


Figura 4.9: Regras de utilizadas no exemplo

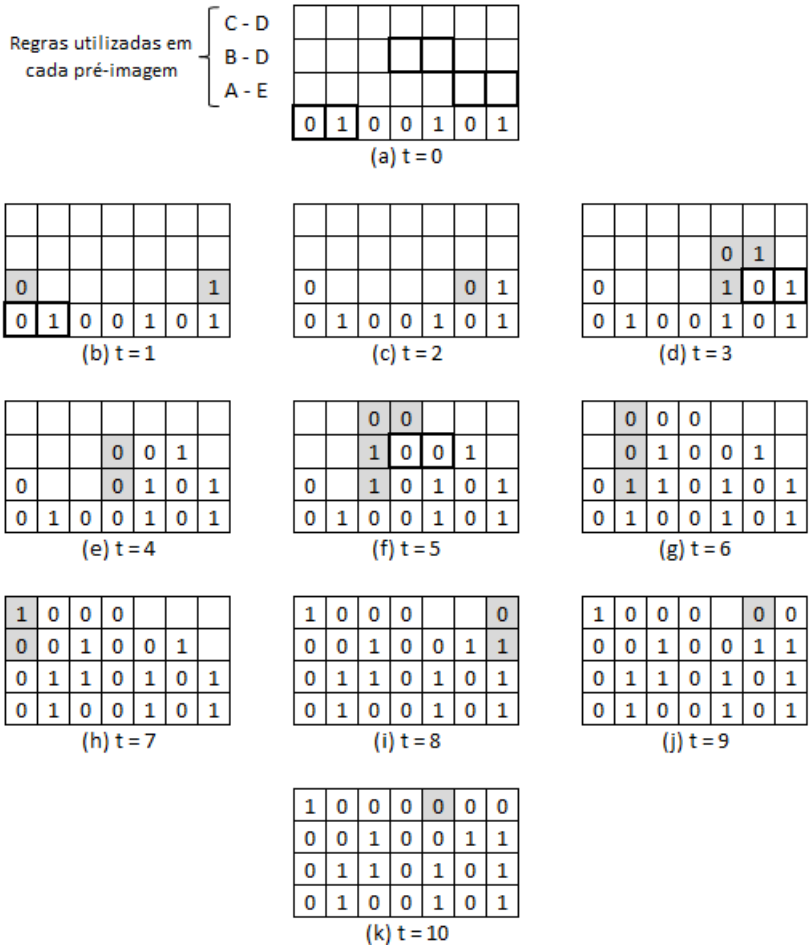


Figura 4.10: Exemplo da evolução dos reticulados

4.3 Modelo Bidimensional

No próximo capítulo será apresentado o método investigado neste trabalho. Ele é fortemente baseado no modelo unidimensional proposto em [de Macedo 2007] adaptado para uma grade bidimensional. Dessa forma o novo modelo é mais adequado para a cifragem de imagens, contudo não o descredencia para a utilização em textos lineares.

Capítulo 5

Modelo AC2D

Os modelos de criptografia por blocos, ao cifrarem um texto claro que possui um tamanho maior que o tamanho do bloco utilizado pelo método, precisam realizar particionamentos do texto em vários blocos menores. Ao final do processo de cifragem, os blocos cifrados são combinados, gerando assim o texto cifrado por completo. No método proposto neste trabalho, esta característica de quebrar a cifragem em vários blocos também pode ser utilizada, porém devido à utilização de uma cifragem espacial, esta quebra apenas resultaria em uma cifragem de pior qualidade. O modelo que será apresentado utiliza um único bloco no processo de cifragem, o que torna sua aplicação em imagens interessante, pois as imagens possuem características particulares, tais como o grande volume de informações e muita redundância. Assim, ao utilizar um único bloco em uma cifragem espacial é possível que o pixel mais superior da imagem interfira na cifragem do pixel mais inferior, bem como no pixel central. Ou seja, não existe relação entre os blocos particionados, mas sim entre os pixels da imagem como um todo.

Por exemplo, suponha a imagem em preto e branco de tamanho 128×128 representada na figura 5.1. Nessa imagem cada pixel (ponto da imagem) pode ser representado por um único bit, 1 quando o pixel é preto e 0 quando o pixel é branco. Utilizando-se um algoritmo convencional qualquer que particione a imagem em blocos de tamanho 128 bits, se o algoritmo particionasse os blocos como as linhas da imagem, devido à existência de linhas idênticas, resultariam em blocos cifrados idênticos. Dependendo do modo de operação do método de cifragem em blocos, que determina a forma como os blocos cifrados são compostos para gerar a imagem cifrada, essa cifragem poderia ocasionar zonas similares na imagem final cifrada, que poderiam fornecer a um criptoanalista indícios para a realização de um ataque e/ou descoberta de padrões da imagem original. A figura 5.1 exemplifica uma cifragem ruim para a imagem apresentada na figura 5.2. Mesmo com imagens mais complexas, pode ocorrer o problema das zonas de texturas. A figura 5.3 exibe uma imagem mais complexa do que a apresentada anteriormente, e sua imagem cifrada. É notável que a imagem cifrada possui regiões similares à imagem original.

Conforme já foi mencionado, o modelo bidimensional apresentado neste trabalho

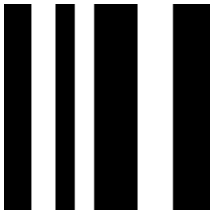


Figura 5.1: Imagem simples de tamanho 128x128 com um padrão bem definido

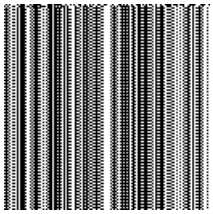


Figura 5.2: Exemplo de um cifragem ruim para imagem da figura 5.1

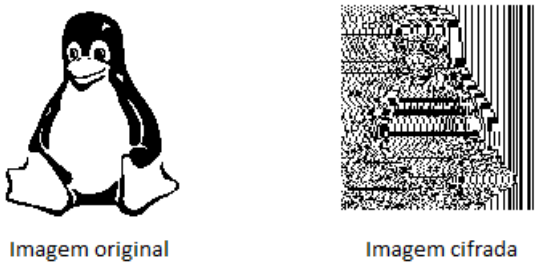


Figura 5.3: Imagem complexa e sua cifragem

baseia-se no modelo apresentado em [de Macedo 2007]. Assim, como o modelo unidimensional, este modelo também utiliza um AC heterogêneo, e a etapa de cifragem também é realizada através do cálculo de pré-imagens.

Até que se chegasse à versão final do modelo bidimensional, diversas alterações foram realizadas a fim de melhorá-lo. A seguir serão apresentadas algumas versões iniciais do modelo até que se chegasse à versão final. A não ser quando especificado, por simplicidade, os exemplos apresentados nas próximas seções utilizam regras de raio 1 e sensíveis ao bit do norte.

5.1 Modelo Básico

A primeira versão do método consistiu apenas em criar um modelo bidimensional que utilizasse o mesmo princípio do modelo básico proposto em [de Macedo 2007]. Ou seja, realizar a cifragem através do cálculo de pré-imagens e a utilização de duas regras, uma chamada regra de contorno, que é utilizada apenas nas células dos extremos do reticulado e outra, chamada regra principal, utilizada nas demais células.

A figura 5.4 mostra a diferença entre as células utilizadas para a borda do método unidimensional [de Macedo 2007] e a borda utilizada pelo método bidimensional proposto

neste trabalho. As células destacadas (conteúdo igual à "y") na figura compõem as bordas para os modelos unidimensional e bidimensional, ambos utilizando-se regras de raio 1. A espessura da borda do reticulado do modelo bidimensional, no qual será aplicada a regra de contorno, é função do tamanho do raio da regra utilizada, sendo que a quantidade total de células é dada por:

$$2rm + 2rn - 4r^2 \tag{5.1}$$

Onde m é a quantidade de linhas, n a quantidade de colunas e r o raio.

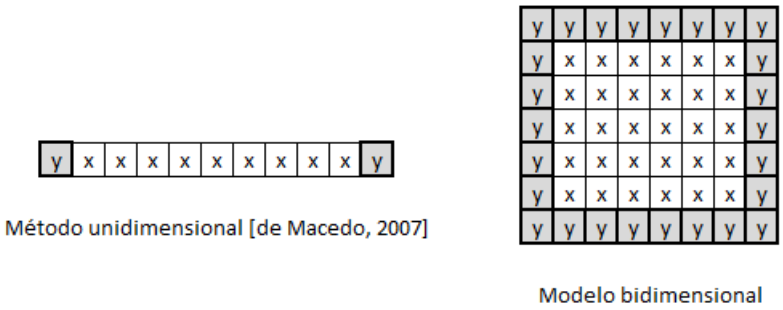


Figura 5.4: Células da borda nos modelos unidimensional e bidimensional

O AC bidimensional utilizado pelo modelo utiliza a vizinhança von Neumann com raio 1. Nos exemplos apresentados nesse capítulo, as regras têm raio 1, ou seja, têm 32 bits. A linearização das regras de transição, bem como a construção, obedecerão ao formato explicado no capítulo 2. A sensitividade ao bit do norte foi adotada para explicar a versão inicial, contudo as demais sensitividades podem ser adotadas.

5.1.1 Cálculo de Pré-imagens no Modelo Básico

A figura 5.5 exibe o reticulado inicial 5×5 que será utilizado como exemplo, enquanto que a figura 5.6 mostra os bits de saída para a regra principal e de contorno. Assim como no modelo unidimensional, o reticulado possui um contorno periódico, ou seja, a última coluna do reticulado é vizinha da primeira coluna, e a última linha é vizinha da primeira linha. A regra principal foi construída a partir do núcleo {0100010111010110} e com sensitividade à célula do norte. Devido à regra principal ser sensível ao bit do norte, a regra de contorno deverá também ser sensível ao bit do norte, assim como ocorre no método proposto em [de Macedo 2007]. Se analisarmos a regra de contorno veremos que o novo valor da célula central (y) é dado pelo complemento do estado atual da célula do norte da vizinhança (N), independentemente do valor atual da célula central (C) ou dos estados das outras células do reticulado (O, L e S). Ou seja, quando o AC é evoluído para frente o único efeito dessa regra é fazer um deslocamento para baixo (de norte para sul) do reticulado, realizando um complemento do valor no passo de tempo anterior. A sensitividade da regra determina por onde o cálculo da pré-imagem deverá ser iniciado.

Neste caso, devido à regra ser sensível ao bit do norte, o cálculo da pré-imagem iniciará do sul para o norte. O primeiro passo é obter os bits da borda da pré-imagem, e para isto deverá ser utilizada a regra de contorno.

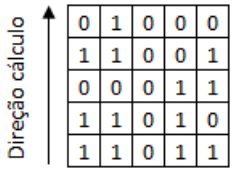


Figura 5.5: Reticulado inicial para o exemplo

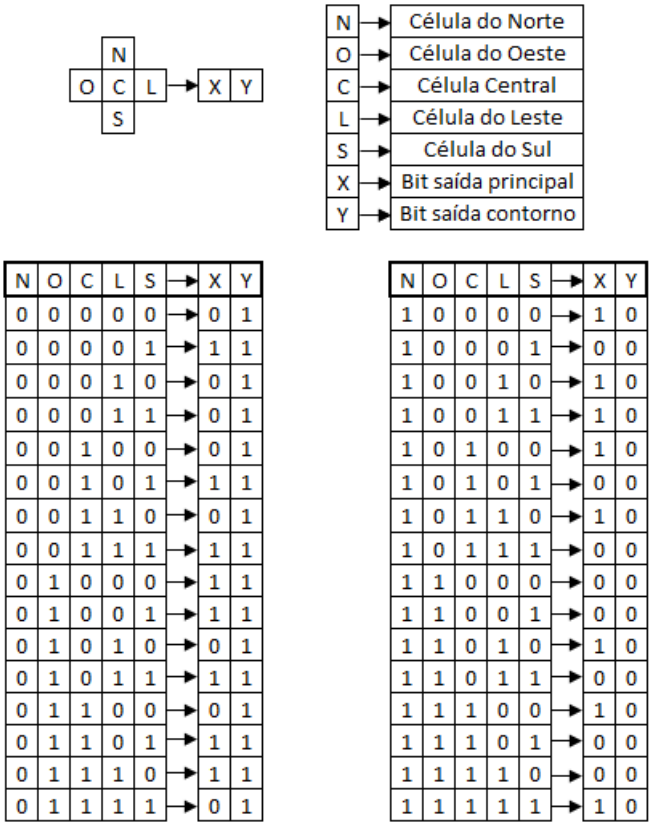


Figura 5.6: Exemplos de regra principal e de contorno de raio 1 sensíveis ao bit do norte

Para determinar o primeiro bit da pré-imagem representado na figura 5.7 (a), é necessário descobrir qual a vizinhança da regra de contorno que possui o bit de saída com o valor 0 (ver figura 5.7 (a) a célula do reticulado em destaque). Todas as vizinhanças da regra de contorno que resultam no bit de saída 0, iniciam com o bit 1, logo o valor do bit da pré-imagem só pode ser o valor 1. Isto ocorre devido à característica das regras de contorno. A figura 5.7 (b) mostra o próximo bit da linha borda da pré-imagem sendo calculado. A figura 5.7 (d) exibe todos os bits da última linha da borda calculados e o cálculo do primeiro bit da primeira coluna. Após finalizado o cálculo dos bits da primeira coluna, segue o cálculo dos bits da primeira linha, como pode ser visto na figura 5.7(e). Da mesma forma, os demais bits da borda (última coluna - figura 5.7(f)) são calculados

resultando na pré-imagem parcial da figura 5.7(g). É importante frisar que os bits da borda da pré-imagem dependem exclusivamente do bit de saída que está no reticulado. Portanto, todos os bits da borda podem ser calculados simultaneamente.

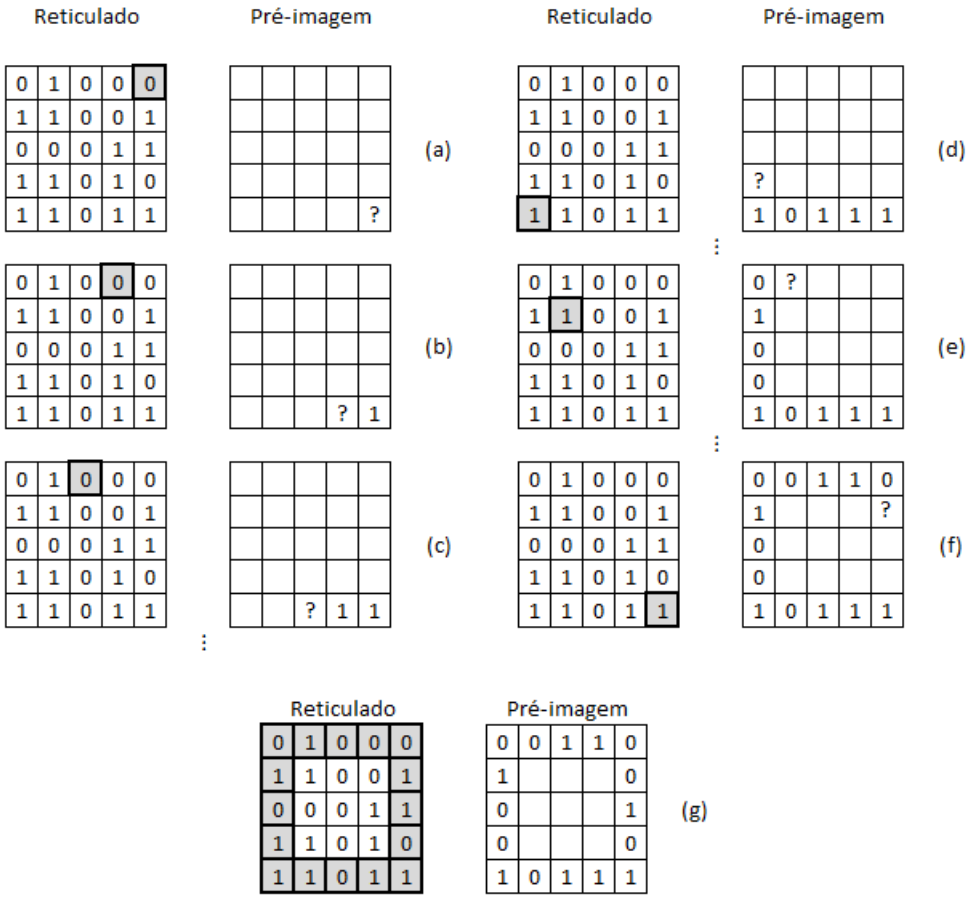


Figura 5.7: Cálculo da borda da pré-imagem

Após calcular a borda da pré-imagem já é possível iniciar o cálculo dos demais bits sendo que, a regra principal será utilizada para obtê-los. Para calcular o bit representado na figura 5.8 (a), é necessário procurar qual a vizinhança ({?1111}) da regra principal que resulte no bit de saída 1. A única vizinhança da regra principal que atende os requisitos é a {$\underline{1}$1111}, portanto o valor do bit da pré-imagem é 1. A figura 5.8 (b) exibe as células utilizadas para o cálculo da próxima célula da pré-imagem. Todas as células da penúltima linha podem ser calculadas de forma similar, sendo que elas podem ser calculadas em paralelo, uma vez que só dependem dos valores atuais das células da última e primeira linhas (que foram calculadas anteriormente pela regra de contorno). Finalizado o cálculo da penúltima linha da pré-imagem já é possível iniciar o cálculo das células da antepenúltima linha, como pode ser visto na figura 5.8 (c). A figura 5.8 (d) exibe a pré-imagem calculada por completo. Devido à regra utilizada ser sensível ao bit do norte, os cálculos das células numa mesma linha podem ser paralelizados, reduzindo assim o tempo final de cifragem.

As figuras 5.7 e 5.8 apresentam com detalhes o cálculo de uma única pré-imagem a

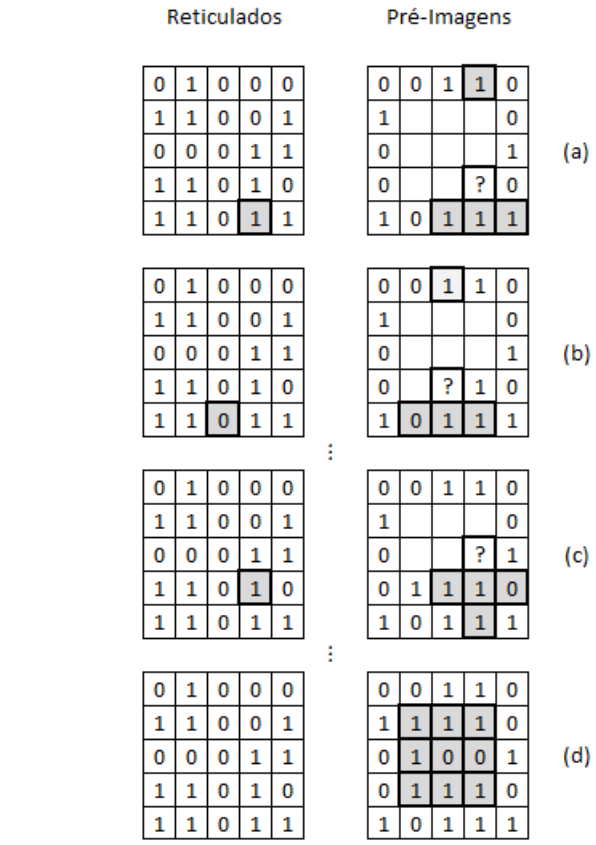


Figura 5.8: Cálculo das demais células utilizando a regra principal

partir do reticulado inicial da figura 5.5 e das regras apresentadas na figura 5.6. A figura 5.9 apresenta o resultado do cálculo consecutivo de 5 pré-imagens a partir do mesmo reticulado inicial e das mesmas regras de transição sensíveis ao bit do norte, onde nesse exemplo, a quinta pré-imagem corresponde à imagem cifrada (texto cifrado).

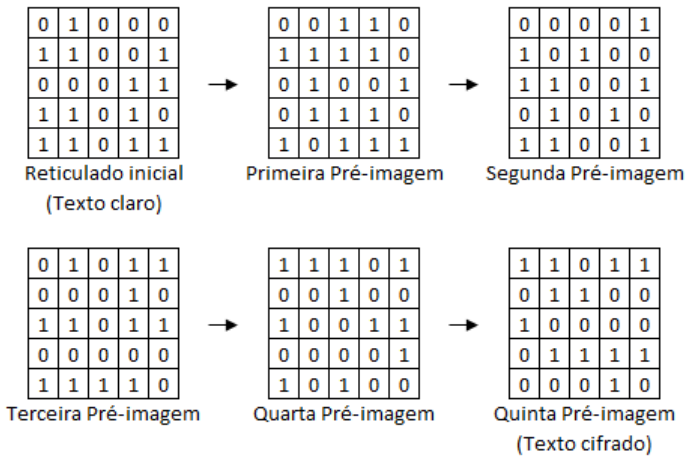


Figura 5.9: Cálculo consecutivo de 5 pré-imagens

5.1.2 Análise do Paralelismo no Modelo Básico

Uma grande vantagem em se investigar a utilização de ACs em métodos de cifragem é a possibilidade de se paralelizar o processo. Utilizando-se o modelo básico bidimensional, a etapa de decifragem é realizada pela simples evolução para frente do reticulado pelo mesmo número de passos realizados na cifragem, ou seja, a mesma quantidade de pré-imagens consecutivas calculadas na obtenção do texto cifrado. Assim, utilizando-se o texto cifrado da figura 5.9 e as regras da 5.6, a obtenção do texto claro ou reticulado inicial é feita pela simples aplicação das regras em todas as células do reticulado, de forma simultânea, por 5 passos de tempo, conforme ilustrado na figura 5.10.

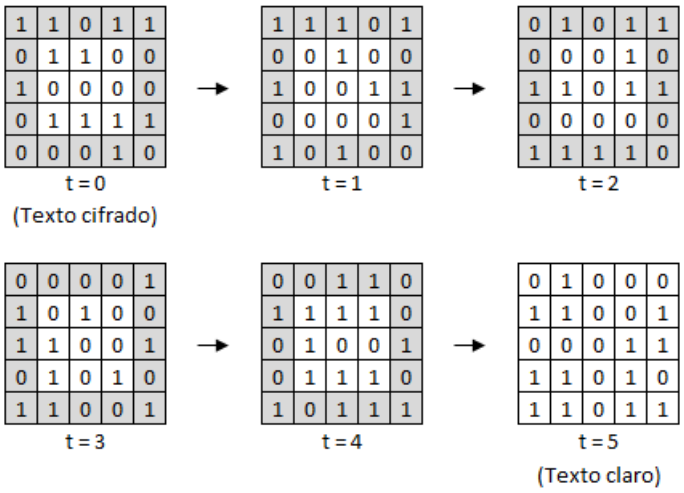


Figura 5.10: Evolução para frente de 5 passos de tempo

Na decifragem, o cálculo das 25 células do reticulado (16 na região da borda) pode ser totalmente paralelizado. Portanto, se esse processo fosse implementado em hardware paralelo, o cálculo do texto claro seria executado em exatamente 5 ciclos de relógio de processamento.

Por outro lado, a etapa de cifragem não é possível de ser realizada de forma totalmente simultânea, mas possui um certo nível de paralelismo. No cálculo de uma única pré-imagem do exemplo, o primeiro passo é realizar o cálculo das 16 células da borda, que podem ser calculadas de forma simultânea (1 ciclo de relógio de processamento). Posteriormente, cada linha interna do reticulado pode ser calculada de forma simultânea para todas as células , mas o cálculo de uma linha depende do cálculo da anterior. Assim, no exemplo, são 3 ciclos de relógio de processamento para as 3 linhas internas do reticulado. No total, no caso de uma arquitetura paralela, são 4 ciclos de relógio para cada pré-imagem. Como no modelo básico, o cálculo de uma pré-imagem só pode ser iniciado após a conclusão da última célula da pré-imagem anterior, para as 5 pré-imagens de exemplo da figura 5.9, seriam necessários 20 ciclos de relógio de processamento (para o cálculo de 125 células, 25 por pré-imagem). Por outro lado, na decifragem, utilizando hardware paralelo, são necessários apenas 5 ciclos de relógio.

De forma genérica, suponha que uma regra com vizinhança von Neumann de raio r é utilizada para cifrar um reticulado $m \times n$ (m linhas e n colunas), utilizando-se P passos de pré-imagem. O número de linhas de contorno é $2r$, assim como o número de colunas. Assim, na cifragem, será utilizado 1 ciclo de relógio para o cálculo das células de contorno e mais 1 ciclo de relógio para cada uma das $(n - 2r)$ linhas restantes. Seja NC_{cif} o número de ciclos de relógio necessário para o cálculo de todas as células do texto cifrado, P o número de passos de pré-imagem, $m \times n$ o tamanho do reticulado e r o raio da regra, então NC_{cif} é dado por:

$$NC_{cif} = P \times (1 + m - 2r) \tag{5.2}$$

Por outro lado, o número de ciclos de relógio necessário para o cálculo de todas as células do texto claro na decifragem (NC_{dec}) é dado por:

$$NC_{dec} = P \tag{5.3}$$

Suponha um exemplo, onde uma regra de raio 2 é usada para cifrar um texto de 512×512 bits por 50 passos de pré-imagem em uma arquitetura totalmente paralela. Nesse caso, serão necessários 50 ciclos de relógio na decifragem e 25.550 ciclos de relógio na cifragem para um total de 13.107.200 células calculadas.

5.2 Deslocamento Linear da Borda

Após concluída a primeira versão e validada a funcionalidade do algoritmo, o próximo passo foi buscar aumentar o desempenho do modelo, especialmente em relação à velocidade de cifragem, utilizando-se uma arquitetura paralela.

A alteração para deslocar a borda do reticulado visa alterar o início do cálculo de pré-imagem de um passo para outro, de forma a permitir que o cálculo das próximas pré-imagens possam ser iniciados mesmo antes do término do cálculo de uma pré-imagem anterior.

A figura 5.11 mostra o cálculo de duas pré-imagens realizado de forma serial. Nesse caso, o cálculo da segunda pré-imagem só foi iniciado após a conclusão da primeira. As células que estão em destaque representam as que estão sendo calculadas no instante t. As células sinalizadas com um "X" representam o valor obtido no cálculo da primeira pré-imagem, enquanto que as células sinalizadas com "O" representam o valor obtido a partir do cálculo da segunda pré-imagem. Essa sequência de cálculo é realizada quando a versão básica do modelo (seção 5.1) é utilizada.

Na figura 5.12 é mostrado como ocorre o deslocamento da borda ao longo de 5 cálculos de pré-imagem, quando a segunda versão do modelo é utilizada. As células em destaque pertencem à borda do reticulado. A cada passo de pré-imagem, a borda do reticulado é

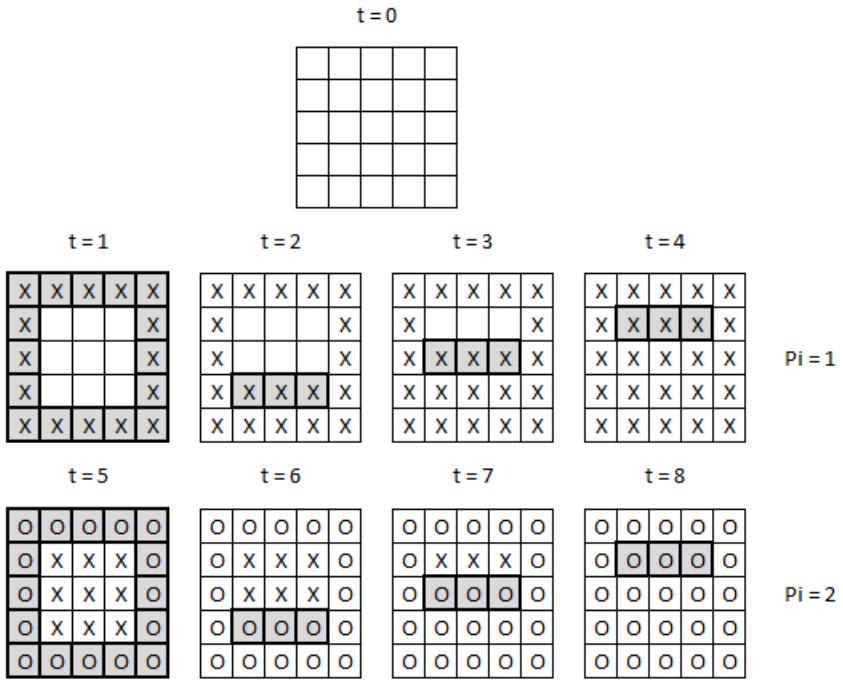


Figura 5.11: Cálculo de duas pré-imagens de forma serial

deslocada em $2r$ células, onde r é o raio da regra. Caso a sensitividade da regra seja ao bit do norte ou sul, o deslocamento deverá ser realizado no eixo y, em contrapartida, caso a regra seja sensível ao leste ou oeste, o deslocamento deverá ser realizado no eixo x. A direção do deslocamento deve obedecer à sensitividade da regra, de maneira a garantir o paralelismo.

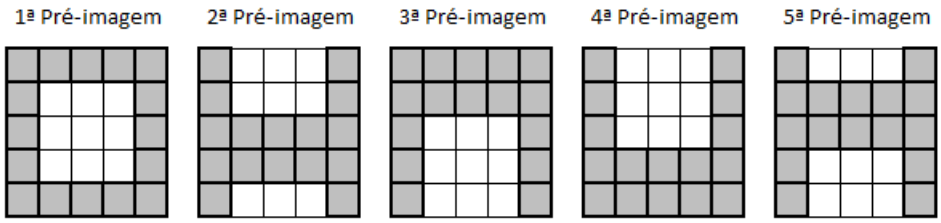


Figura 5.12: Deslocamento da borda

A figura 5.14 exemplifica o cálculo de 5 pré-imagens consecutivas em paralelo para o reticulado representado na figura 5.13, utilizando-se do recurso de deslocamento da borda do reticulado e a regra de transição {1001010110101110} sensível ao bit do norte. As células em destaque representam as células que compõem a borda do reticulado. Como pode ser visto, o cálculo da segunda pré-imagem iniciou no momento em que já haviam células suficientes calculadas na primeira pré-imagem, ou seja, após a obtenção da primeira linha fora da região da borda. Da mesma maneira, o cálculo da terceira pré-imagem iniciou no passo seguinte após o cálculo da primeira linha interna da segunda pré-imagem. O mesmo ocorreu com os cálculos da quarta e quinta pré-imagens. Como é possível observar, o cálculo das 5 pré-imagens foi realizado em apenas 12 passos de tempo, sendo que para cada pré-imagem são necessários 4 passos de tempo (1 para borda e 1 para cada linha

interna).

0	1	0	0	0
1	1	0	0	1
0	0	0	1	1
1	1	0	1	0
1	1	0	1	1

Figura 5.13: Reticulado inicial para o exemplo

Dado um AC bidimensional qualquer de raio r e um reticulado $m \times n$ (m número de linhas e n número de colunas), sendo P o número de pré-imagens utilizada na cifragem, o número de ciclos de relógio (NC_{cif}) que serão gastos na cifragem é dado por:

$$NC_{cif} = 2P + m - 2r + 1 \tag{5.4}$$

Assim, é possível notar que, quanto maior o número de pré-imagens, maior será a diferença em passos entre os modelos (equações 5.2 e 5.4), justificando assim esta alteração para utilização de um arquitetura paralela.

Suponha, por exemplo, uma regra principal de raio 2, uma imagem 512×512 bits e 50 passos de cálculo de pré-imagem. Na versão com deslocamento da borda serão necessários 611 ciclos de relógio, enquanto na versão básica são necessários 25.550 ciclos de relógio. A figura 5.15 exibe um gráfico comparando o modelo básico com o modelo que possui deslocamento da borda, contrastando o número de pré-imagens com a quantidade de ciclos de relógio utilizadas para o processo de decifragem.

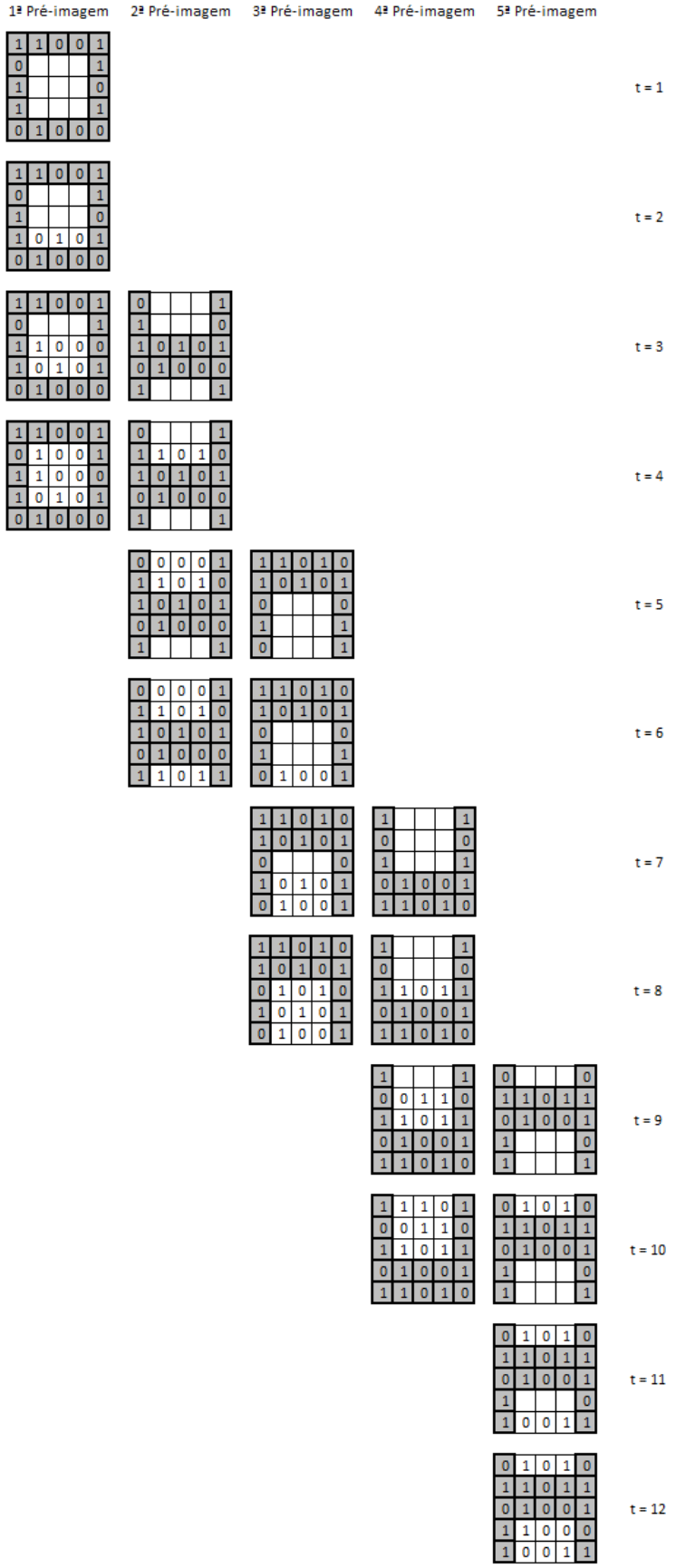


Figura 5.14: Cálculo em paralelo de 5 pré-imagens consecutivas

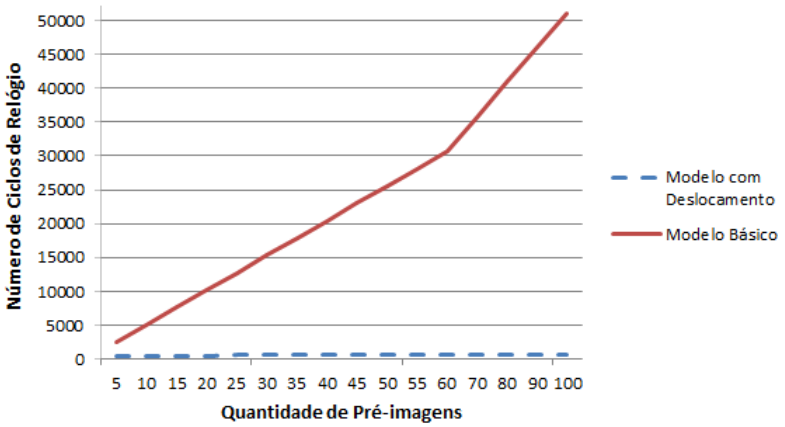


Figura 5.15: Comparação entre os modelos básico e o com deslocamento para a decifragem

5.3 Deslocamento Espacial do Reticulado

O deslocamento espacial do reticulado tem como objetivo aumentar a segurança do método. Devido à borda da pré-imagem utilizar a regra de contorno, que por sua vez não produz uma saída de alta aleatoriedade, o deslocamento espacial (deslocamento em duas direções) do reticulado força o método propagar as perturbações realizadas no interior para as extremidades.

Além do deslocamento no próprio eixo da sensitividade visto na seção anterior, a cada cálculo de uma nova pré-imagem os bits também são rotacionados $2r$ posições, onde r é o raio da regra utilizada. Quando a regra de transição for sensível ao bit norte ou sul, a rotação deverá ser realizada no eixo x. Em contrapartida, quando a regra de transição for sensível ao bit do leste ou oeste, a rotação deverá ser realizada no eixo y.

A figura 5.16 mostra o deslocamento espacial realizado ao longo do cálculo de 5 pré-imagens consecutivas. Para este exemplo, a regra do AC é de raio 1 e sensível ao bit do norte. É importante frisar que esta rotação não prejudica o tempo de cifragem.

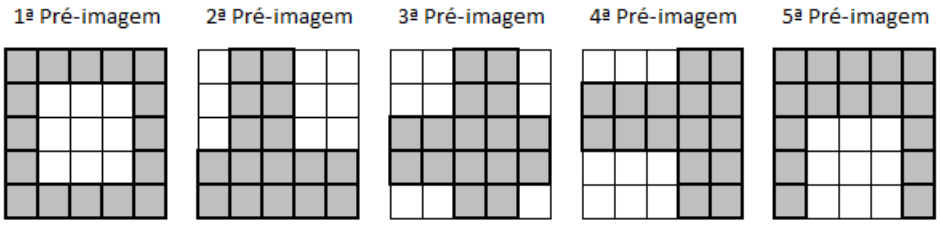


Figura 5.16: Deslocamento espacial do reticulado para uma regra de raio 1 sensível ao bit do norte

5.4 Modelo com Deslocamento Espacial da Borda e Rotação do Núcleo da Regra

A rotação do núcleo da regra foi outra alteração adicionada ao método a fim de melhorar o resultado final da cifragem, consequentemente aumentando a segurança do método. Esta rotação do núcleo é semelhante ao realizado no método proposto em [de Macedo 2007]. Testes aplicados no modelo com esta alteração, mostram-se mais sensíveis a propagação de perturbações no texto claro (reticulado inicial), característica desejada em modelos criptográficos.

A cada novo cálculo de pré-imagem o núcleo da regra utilizada é rotacionada para direita em uma posição, gerando assim uma nova regra principal e uma nova regra de contorno. Seja {0100010111010110} o núcleo de uma regra principal, logo os 32 bits da regra são dados por {01000101110101101011101000101001}. Após a rotação para direita do núcleo da regra, o novo núcleo e a nova regra gerados são {0010001011101011} e {00100010111010111011101000010100}. Dependendo da aleatoriedade do núcleo da regra

utilizada, o processo de cifragem poderá utilizar até $2^{(4\times raio)}$ regras diferentes (tamanho do núcleo) no processo de cifragem geradas a partir de uma única chave.

A figura 5.17 demonstra a rotação do núcleo da regra ao longo de 5 pré-imagens consecutivas. A cada pré-imagem o núcleo é deslocado para direita em 1 bit, dando origem a um novo núcleo, consequentemente à uma nova regra. Foi comprovado experimentalmente que a alternância aumenta a propagação da perturbação melhorando a cifragem.

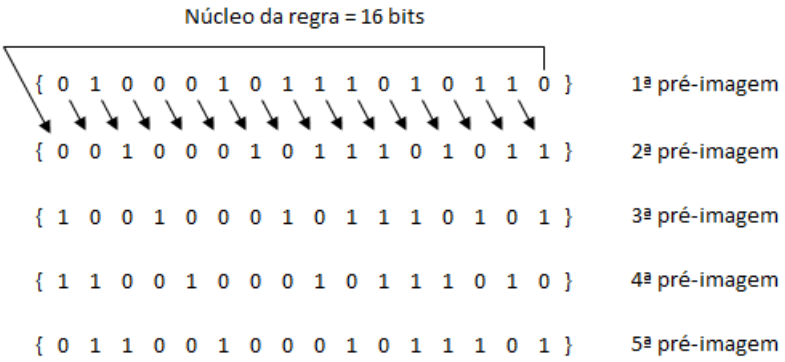


Figura 5.17: Rotação do núcleo da regra

5.5 Modelo Final e Variações

O modelo final proposto nesse trabalho utiliza o deslocamento da borda e a rotação do núcleo discutidas na últimas seções. Duas variações desse modelo foram utilizadas em nossas análises e testes que serão apresentados no próximo capítulo. Na primeira, adota-se uma direção única para a sensitividade da regra em todo o processo de cifragem, enquanto que na segunda, a cada pré-imagem, utiliza-se uma sensitividade diferente.

5.5.1 Variação com Sensitividade Fixa

Nessa variação do modelo, adota-se uma direção única para a sensitividade da regra, como a direção norte. Os exemplos anteriores apresentaram apenas cálculos de pré-imagens utilizando regras sensíveis ao bit do norte, porém o método também pode ser utilizado para regras sensíveis ao bit do leste, oeste ou sul. Para demonstrar que é simples a modificação do modelo para atender às demais sensitividades, suponha que seja realizada uma cifragem na imagem da figura 5.18 utilizando-se de uma regra sensível ao bit do norte. Portanto, o processo do cálculo da pré-imagem deverá ser iniciado do sul para o norte, como já foi explicado anteriormente. Agora suponha a cifragem para a mesma imagem, porém utilizando-se de uma regra sensível ao bit do leste, logo o processo do cálculo da pré-imagem deve iniciar do oeste para o leste. Os procedimentos a serem realizados são idênticos aos do cálculo da pré-imagem sensível ao bit do norte, porém com uma rotação em 90 graus da imagem como pode ser visto na figura 5.19 (a). As figuras 5.19 (b) e 5.19

(c) representam as rotações necessárias para o cálculo da pré-imagem com sensitividade ao bit do sul e do oeste, respectivamente.

Figura 5.18: Imagem de exemplo

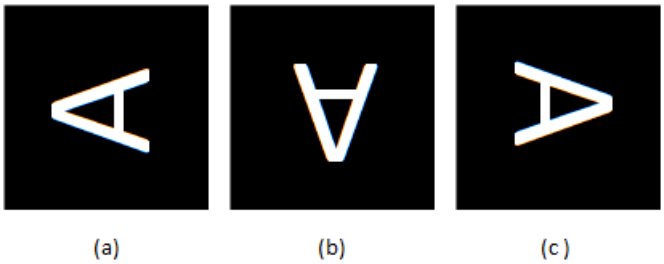


Figura 5.19: (a) Rotação em 90 graus (b) Rotação em 180 graus (c) Rotação em 270 graus

A rotação não precisa ser efetivamente realizada, bastando apenas realizar transposições das coordenadas das células, logo este processo não afetaria o desempenho do método.

A grande vantagem dessa variação é que, independentemente da direção escolhida para a sensitividade da regra a ser gerada a partir do núcleo, ela provê o maior paralelismo ao modelo, dado pela equação (5.4) da seção 5.2.

5.5.2 Variação com Rotação da Sensitividade

A modificação da sensitividade da regra a cada passo de cálculo de pré-imagem foi uma alteração realizada visando melhorar ainda mais a segurança do método. Esta alteração consiste em cada cálculo de pré-imagem gerar uma regra a partir do núcleo com uma sensitividade diferente do passo anterior. Como já foi apresentado na seção anterior, a utilização de regras com sensitividades diferentes é muito simples e não prejudica o desempenho do método no caso de implementação sequencial (não paralela).

A ordem sugerida para a rotação das sensitividades é primeiramente ao bit do norte, em seguida ao bit do oeste, depois ao sul e finalmente ao bit do leste, retornando ao bit do norte, iniciando um novo ciclo.

No próximo capítulo serão apresentados os testes para as duas variações do modelo final. A variação com rotação da sensitividade, apesar de prejudicar o paralelismo, necessita de um número menor de pré-imagens para uma boa cifragem, diferentemente da variação anterior. Portanto, cada variação possui uma vantagem e manteremos as duas como possibilidades de aplicação do modelo.

5.6 Aplicação em Imagens

Nas seções anteriores foram apresentados os modelos de cifragem, porém utilizando apenas matrizes binárias como texto claro. Nessa seção, apresentamos efetivamente como o método pode ser utilizado em imagens. Para imagens em preto e branco binarizadas não é difícil propor uma solução, pois a relação é direta, ou seja, se o valor do reticulado é 1, então a cor é preta, do contrário a cor é branca. A figura 5.20 exemplifica uma imagem em preto e branco, representada por 0s e 1s, bem como a imagem de sua cifragem.

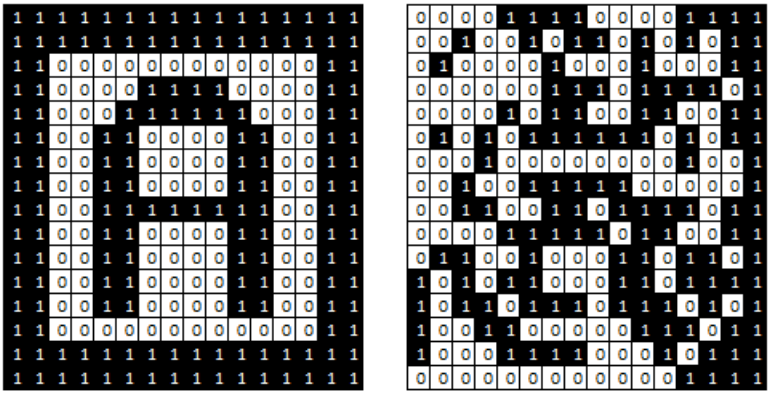


Figura 5.20: Exemplo de representação de uma imagem em preto e branco

Para imagens com mais de duas cores é preciso realizar uma adaptação no método. A adaptação do método consiste em distribuir os bits dos pixels da imagem em linhas, ou colunas, ou em ambas. Suponha uma imagem de tamanho 100×100 em escala de cinza que utiliza 8 bits para cada pixel. Os bits de cada pixel podem ser distribuídos em colunas, para cada pixel será necessário adicionar 8 células no reticulado. Uma vez que cada pixel da imagem representa 8 células dispostas sequencialmente no reticulado, a quantidade de colunas do reticulado será aumentada em 8 vezes, logo o tamanho reticulado para este tipo de representação seria de 800×100. A forma mais usual para representação do tamanho de imagens é largura $\times$ altura, porém nesse trabalho será adotado o padrão altura $\times$ largura para facilitar a comparação com matrizes binárias (linhas $\times$ colunas). A figura 5.21 demonstra a distribuição do pixel (0, 0) em colunas do reticulado para uma imagem de tamanho 128×128. Consequentemente, esse aumento do reticulado leva a pensar em uma redução no desempenho do modelo, pois haverá mais células para serem processadas. Porém se o aumento ocorrer em número de colunas e, para cifragem for utilizada regras sensíveis ao bit do norte ou ao bit do sul, como já foi explicado anteriormente, os cálculos das células que estão dispostas em uma mesma linha são processados de forma paralela. Portanto, se foi realizada uma implementação em uma arquitetura paralela, o aumento em colunas pode não significar uma degradação do desempenho do método. Analogamente, acontece com a distribuição do valor do pixel em linhas quando são utilizadas regras sensíveis ao bit do oeste ou do leste. Na seção 6.7 será apresentada uma abordagem para distribuição não linear dos pixels para imagens de 256 níveis de cinza. As figuras 5.22(a)

e 5.22(b) exibem duas formas de representação não linear. Na figura 5.22(a) cada pixel é formado por uma matriz binária de 2×4, enquanto a figura 5.22(b) exibe a distribuição dos pixels na forma 4×2.

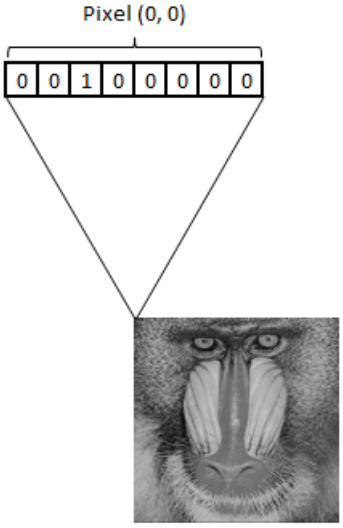


Figura 5.21: Distribuição do pixel (escala de cinza) distribuído em colunas do reticulado

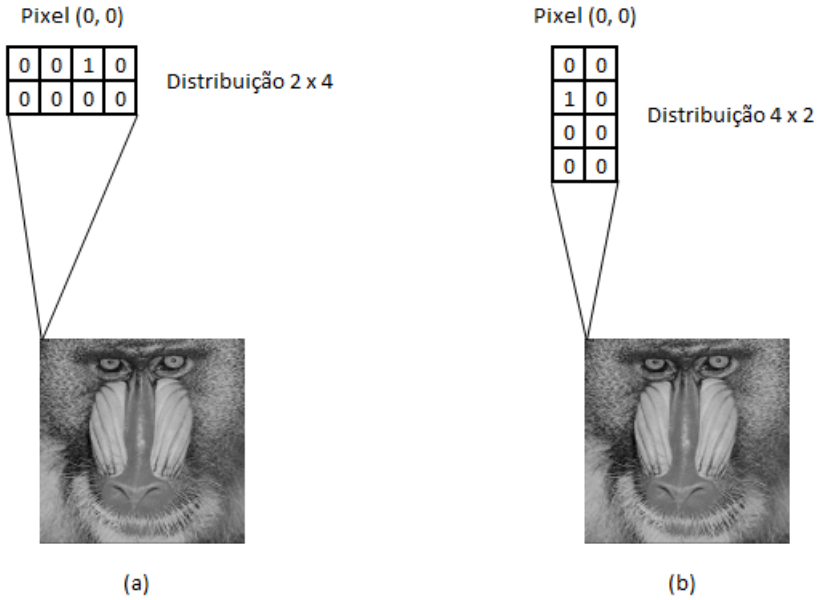


Figura 5.22: (a) Distribuição 2×4 do pixel (b) Distribuição 4×2 do pixel

Capítulo 6

Experimentos e Resultados

Neste capítulo serão apresentados os testes realizados e os resultados obtidos para a validação do modelo proposto. Como já foi dito no capítulo anterior, duas variações do modelo bidimensional foram analisadas, a primeira utiliza sempre a mesma direção para a sensitividade da regra e será denominada *"modelo com sensitividade fixa"*, enquanto a segunda realiza a rotação da sensitividade a cada passo do cálculo da pré-imagem e será denominada por *"modelo com rotação da sensitividade"*. A não ser quando especificado, para os testes com o modelo de sensitividade fixa foram utilizadas regras sensíveis ao bit do norte.

6.1 Experimentos Iniciais

Antes de iniciar a validação dos métodos bidimensionais, testes mais simples foram realizados a fim de validar características herdadas do modelo proposto em [de Macedo 2007]. Estas variações foram testadas em um número elevado de casos e comprovaram que realizam uma significativa melhoria na qualidade de cifragem e podem ser encontradas em [de Macedo 2007].

6.1.1 Modelo unidimensional proposto em [de Macedo 2007]

A primeira etapa, consistiu em reproduzir as variações dos modelos unidimensionais e os testes realizados em [de Macedo 2007]. Essa etapa teve como finalidade a compreensão das melhorias no modelo unidimensional em cada uma das variações, para que a criação do novo modelo bidimensional partisse de um estágio mais avançado. Além disso, os mesmos testes no modelo unidimensional realizados em [de Macedo 2007] foram reproduzidos e resultados similares foram obtidos. Isso nos deu a garantia de termos reproduzido o modelo com sucesso e nos auxiliou na compreensão do método.

Posteriormente, testes com imagens foram realizados para verificar a adequabilidade do modelo unidimensional proposto em [de Macedo 2007] à cifragem de imagens. Utilizando-

se das configurações - tamanho da chave 256 bits, tamanho do bloco 128 bits e 128 passos de pré-imagem - propostas em [de Macedo 2007], a imagem da figura 6.1 de 512×512 bits foi cifrada. Como a imagem é em preto e branco binarizada é possível representá-la por uma matriz de 512×512 bits. Devido ao modelo ser unidimensional, há a necessidade de quebrar a imagem em blocos. Dessa forma, a imagem foi particionada em 2048 blocos de 128 bits, onde cada bloco é equivalente a 1/4 de uma linha da imagem.

Figura 6.1: Imagem 512×512 em preto e branco binarizada para o exemplo

Existem diversos modos de operação que os métodos de criptografia por blocos podem utilizar. Modo de operação é a forma pelo o qual os blocos do texto claro ou cifrado são cifrados/decifrados. Em [de Macedo 2007] afirma-se que o modelo unidimensional proposto pode ser utilizado em qualquer modo de operação. A seguir serão apresentados os resultados das cifragens para os modos de operação: ECB (*Electronic Codebook*), CBC (*Cipher-block Chaining*), CFB (*Cipher Feedback*), OFB (*Output Feedback*) e CTR (*Counter*) [Stallings 2003].

No modo de operação ECB, os blocos são cifrados individualmente e em seguida concatenados gerando o texto cifrado. O processo de cifragem dos blocos pode ser visualizado na figura 6.2. O processo da decifragem é semelhante ao processo da cifragem, onde os blocos são decifrados individualmente e ao final são concatenados gerando o texto claro. O processo de decifragem dos blocos pode ser visualizado na figura 6.3. Note que os blocos podem ser cifrados em paralelo e não existe dependência entre os blocos. A figura 6.4 exibe a imagem do exemplo cifrada pelo método de AC unidimensional, utilizando o modo de operação ECB. Já é sabido que este modo de operação não produz um texto cifrado de boa qualidade quando o texto claro possui uma alta redundância. Portanto, apesar do processo de cifragem/decifragem dos blocos poder ser realizado em paralelo, este modo de operação inviabiliza a utilização em imagens devido a formação de zonas de textura na imagem cifrada.

Para melhorar a qualidade do texto cifrado, os modos de operação CBC, CFB e OFB utilizam informações da etapa de cifragem do bloco anterior para a cifragem do bloco atual. Dessa forma, o paralelismo no processo de cifragem/decifragem dos blocos é perdido, enquanto a qualidade da cifragem é melhorada. As figuras 6.5, 6.6 e 6.7 apresentam os esquemas de cifragem dos blocos para o modos de operação CBC, CFB e OFB, respectivamente. Note que a cifragem do bloco i utiliza uma informação do bloco

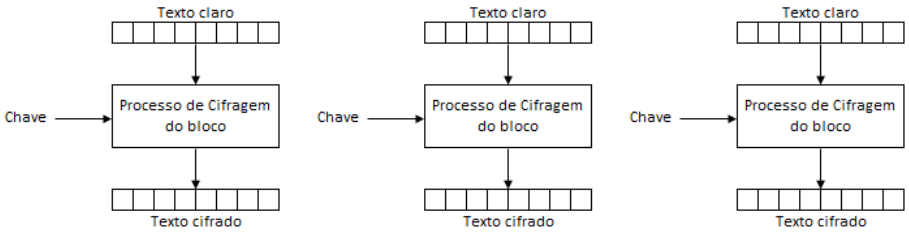


Figura 6.2: Esquema de cifragem dos blocos utilizando o modo de operação ECB

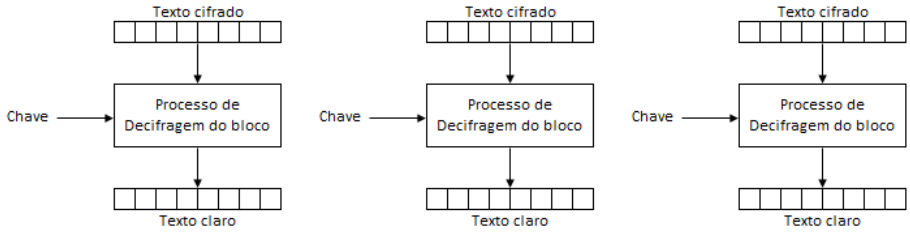


Figura 6.3: Esquema de decifragem dos blocos utilizando o modo de operação ECB

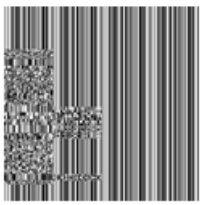


Figura 6.4: Imagem exemplo cifrada utilizando o modo de operação ECB

$i-1$, exceto para o primeiro bloco que utiliza um informação extra denominada por vetor de inicialização (*IV - Initialization Vector*).

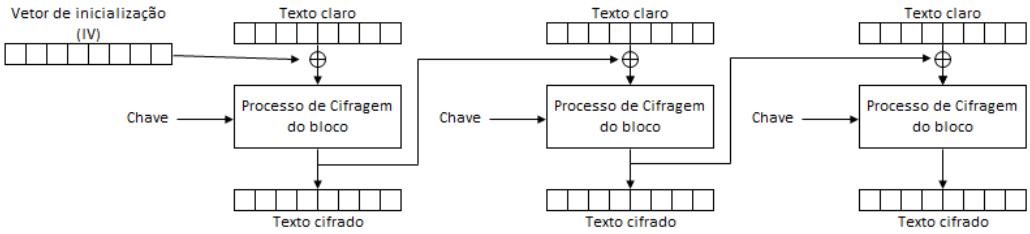


Figura 6.5: Esquema de cifragem dos blocos utilizando o modo de operação CBC

A figura 6.8 exibe as imagens cifradas para os modos de operação CBC, CFB e OFB. Visivelmente é possível identificar que as zonas de textura desapareceram, gerando uma imagem sem qualquer característica da imagem original.

As figuras 6.9, 6.10 e 6.11 apresentam os esquemas para o processo de decifragem dos blocos utilizando os métodos de operação CBC, CFB e OFB, respectivamente. É importante salientar que, o esquema de decifragem para os modos de operação CFB e OFB, não utiliza o processo de decifragem do modelo, sendo que a decifragem é realizada pela operação XOR inversa à realizada na cifragem. Dessa forma, o tempo gasto para a decifragem será igual ao tempo gasto para a cifragem, contudo já foi demonstrado que a decifragem é totalmente paralelizável, logo o processo como um todo sofreria uma

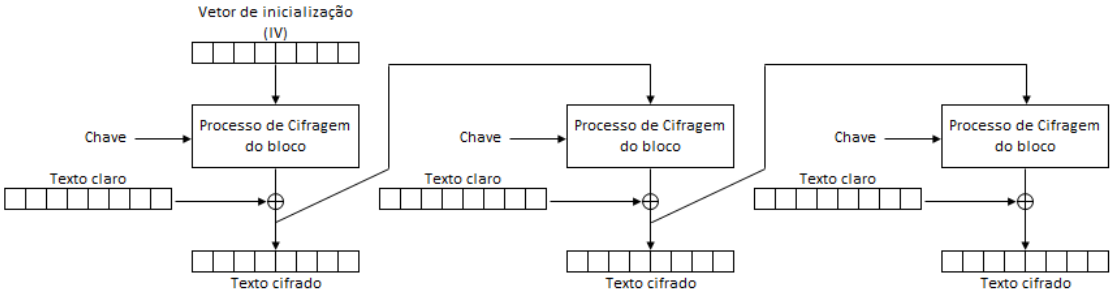


Figura 6.6: Esquema de cifragem dos blocos utilizando o modo de operação CFB

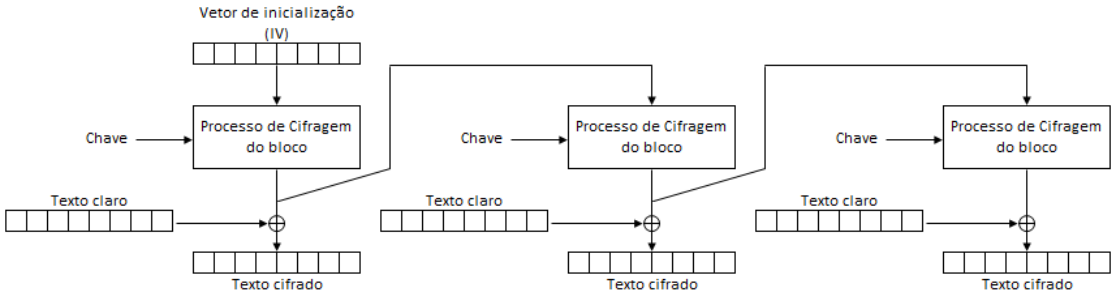


Figura 6.7: Esquema de cifragem dos blocos utilizando o modo de operação OFB

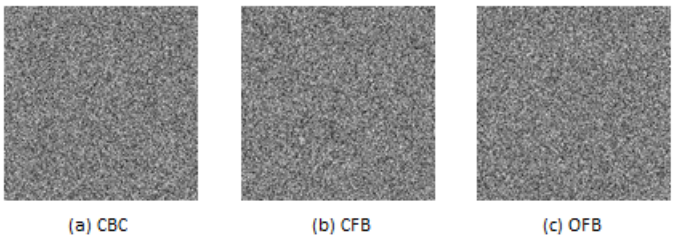


Figura 6.8: Imagens cifradas para os modos de operação CBC, CFB e OFB

degradação do desempenho.

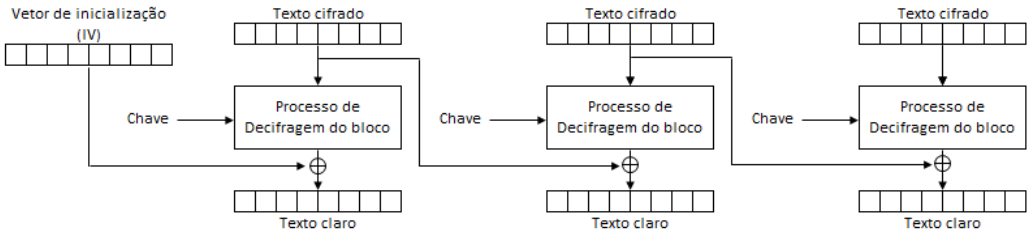


Figura 6.9: Esquema de decifragem dos blocos utilizando o modo de operação CBC

O modo de operação CTR utiliza um contador que serve como entrada para cifragem de cada bloco e essa entrada independe do bloco anterior. O contador de entrada é cifrado e em seguida é realizada uma operação XOR entre o bloco de texto claro e a cifragem do contador, gerando assim o bloco cifrado. Note, que dessa forma o paralelismo é mantido, assim como no modo de operação ECB. Como cada bloco cifrado possui um contador diferente, o resultado da cifragem de dois blocos de texto claro idênticos, resulta em blocos cifrados distintos. A figura 6.12 exibe o esquema de cifragem para o modo

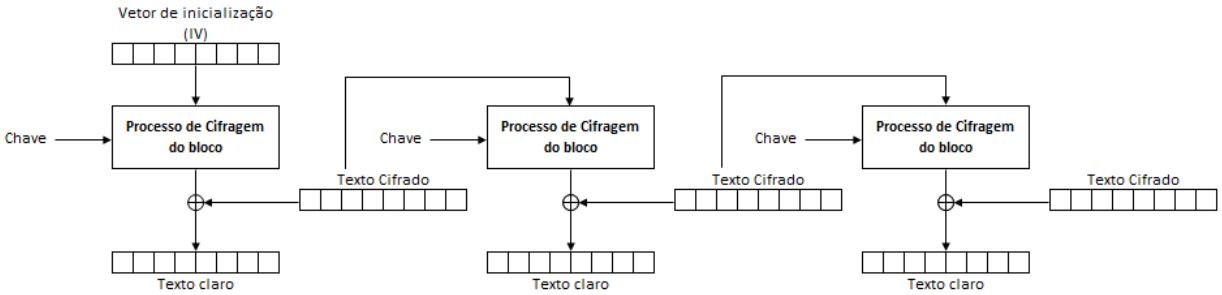


Figura 6.10: Esquema de decifragem dos blocos utilizando o modo de operação CFB

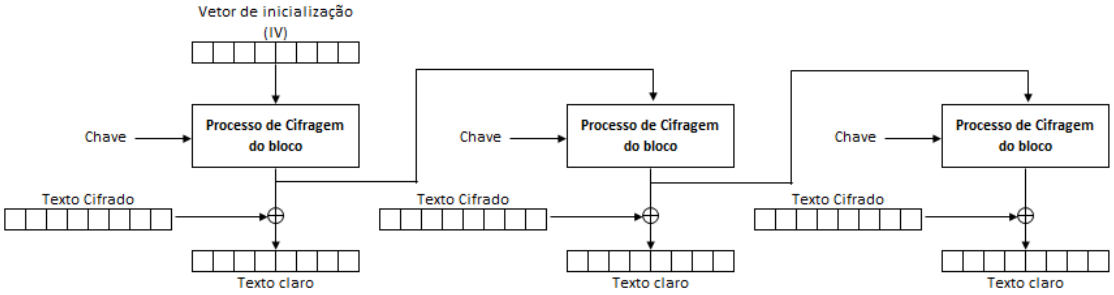


Figura 6.11: Esquema de decifragem dos blocos utilizando o modo de operação OFB

de operação CTR. Um ponto a ser considerado neste modo de operação é a decifragem, semelhante ao que ocorre nos modos de operação CFB e OFB, ela é realizada utilizando-se da operação XOR e o processo de cifragem. Logo, a decifragem do método é inutilizada. O esquema de decifragem para o modo de operação CTR pode ser visualizado na figura 6.13. A imagem cifrada a partir da figura 6.1, pode ser vista na figura 6.14.

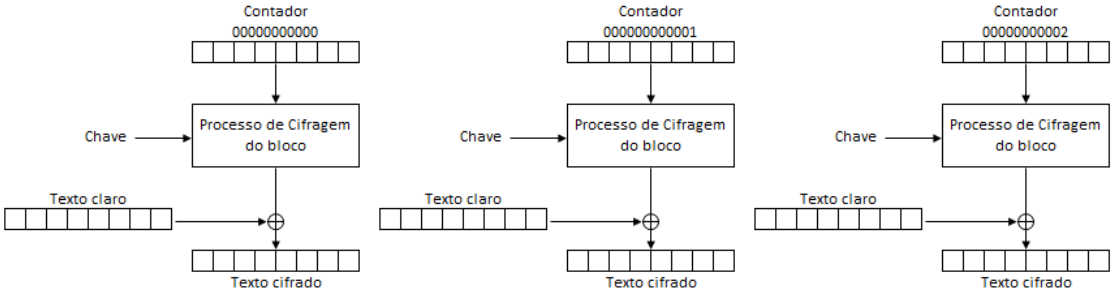


Figura 6.12: Esquema de cifragem dos blocos utilizando o modo de operação CTR

Portanto, é possível observar que o modelo unidimensional proposto em [de Macedo 2007], por ser baseado na cifragem de blocos lineares, não apresenta um bom comportamento quando utilizado em imagens, semelhante o que ocorre em modelos tradicionais. Quando utilizado o modo de operação ECB, foi visível a formação de zonas de texturas na imagem cifrada. Os modos de operação CBC, CFB, e OFB, apresentaram bons resultados na imagem cifrada, porém degradaram o desempenho do tempo de cifragem e decifragem em n vezes, considerando que n é quantidade de blocos necessária para o processo de cifragem ou decifragem. Outro ponto a ser considerado, para os modos de operação CFB, OFB e CTR, é a utilização apenas do processo de cifragem, o que acarreta

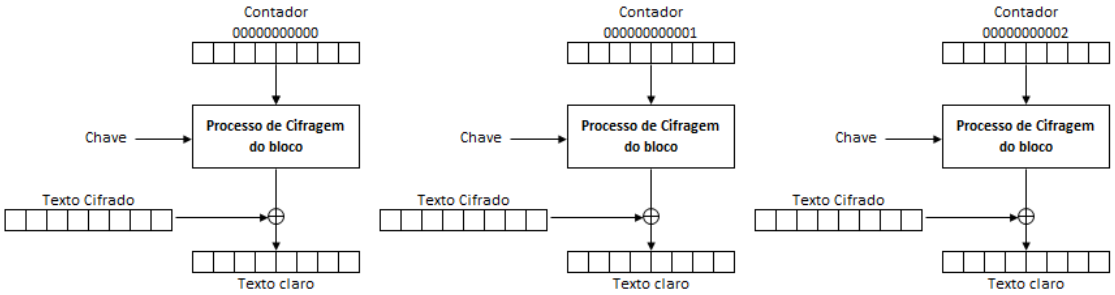


Figura 6.13: Esquema de decifragem dos blocos utilizando o modo de operação CTR

Figura 6.14: Imagem da figura 6.1 cifrada com o modo de operação CTR

ainda mais a degradação do desempenho geral do modelo. É preciso deixar claro que os modos de operação são esquemas propostos para cifragem de blocos para qualquer sistema criptográfico de blocos, não se restringindo apenas ao método unidimensional proposto em [de Macedo 2007]. Ou seja, as conclusões aqui apresentadas se aplicam a qualquer método de criptografia baseado em blocos lineares aplicados na cifragem de imagens.

6.1.2 Testes iniciais com variações no modelo bidimensional

• Análise visual da imagem cifrada

Testes visuais foram realizados nas variações do modelo bidimensional proposto com a finalidade de verificar a adequabilidade de cada variação. A análise visual realizada neste teste considera uma cifragem de boa qualidade quando a imagem cifrada não possui qualquer tipo de padrão e é totalmente diferente da imagem original. A seguir serão apresentados alguns exemplos de imagens cifradas que mostram visualmente as melhorias obtidas a cada variação implementada. Análises visuais isoladas mostraram que 30 passos de pré-imagens poderiam produzir bons resultados, ou seja, gerar imagens cifradas sem qualquer característica da imagem original. Logo, para os exemplos apresentados a seguir, foram utilizados os mesmos 30 passos nos cálculos de pré-imagens e uma regra sensível ao bit do norte obtida a partir do núcleo {0000100101100001}.

Na figura 6.15 é apresentada a cifragem da imagem da figura 6.1, utilizando-se a versão inicial do modelo proposto, ou seja, o autômato celular utiliza, no cálculo das pré-imagens, uma borda fixa e não existe rotação do núcleo do reticulado. É notável que a qualidade da cifragem é ruim, pois fornece informações da imagem original.

Como já foi mencionado na seção 5.2 o deslocamento espacial da borda visa aumen-

Figura 6.15: Imagem cifrada com borda fixa e sem rotação do núcleo da regra

tar o desempenho no tempo de cifragem. Porém, esta alteração também proporcionou uma melhoria na qualidade da imagem cifrada, como pode ser visto na figura 6.16, onde apresenta-se a imagem da figura 6.1 cifrada com essa variação, utilizando-se o mesmo número de pré-imagens. Devido à borda do reticulado utilizar a regra de contorno, a aleatoriedade aplicada no interior da imagem não é propagada para as extremidades se a borda for mantida fixa. Logo, o deslocamento aplicado no cálculo da pré-imagem força a borda a percorrer toda a imagem, ocasionando assim uma melhoria na qualidade da imagem cifrada.

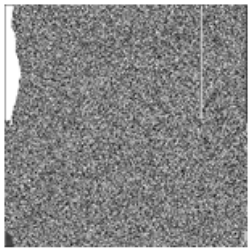


Figura 6.16: Imagem cifrada com o deslocamento da borda

A última variação que caracteriza o modelo bidimensional de sensitividade fixa é aquela que adota, além do deslocamento da borda, a rotação do núcleo da regra. O resultado da cifragem obtida com essa alteração pode ser exemplificado pela imagem da figura 6.17, que também é o resultado da cifragem da figura 6.1, com 30 passos de pré-imagem. A qualidade da imagem cifrada é visivelmente superior às imagens apresentadas anteriormente. Esta melhoria ocorre pelo fato de não se usar a mesma regra nos cálculos consecutivos de pré-imagens, mas várias regras diferentes, aumentando assim o grau de aleatoriedade do modelo. É importante lembrar que as regras utilizadas são originadas a partir de um único núcleo.

A rotação da sensitividade a cada cálculo da pré-imagem foi a última variação implementada e ela caracteriza o modelo com rotação da sensitividade. Esta variação tem por objetivo melhorar a qualidade da cifragem com um número menor de passos de pré-imagem. A figura 6.18 demonstra uma imagem cifrada com o modelo com rotação da sensitividade. Como pode ser visto, a cifragem não fornece características da imagem original, semelhante à imagem da figura 6.17 que utiliza o modelo sem a rotação da sensitividade. A diferença da qualidade da cifragem entre os dois modelos será esclarecida

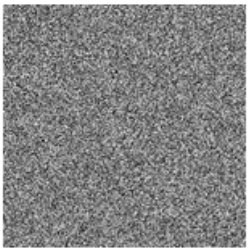


Figura 6.17: Imagem cifrada pelo modelo de sensitividade fixa

no próximo tópico dessa seção.

Figura 6.18: Imagem cifrada pelo modelo com rotação da sensitividade

Embora analisando-se visualmente as figuras 6.15 e 6.16 fique evidente que as variações originais não se adequam à criptografia, deve-se ter claro que esse resultado também depende do número de passos de pré-imagens, isto é, seria possível obter bons resultados caso utiliza-se um número maior de pré-imagens. A figura 6.19 apresenta as imagens obtidas a partir da figura 6.1, utilizando-se as quatro variações do modelo bidimensional, cifrados com 30, 100, 200 e 250 passos de pré-imagem (que estão simbolizados pelo símbolo Pi). O modelo básico também se mostrou capaz de produzir uma imagem cifrada de boa qualidade, porém precisou de um número maior de pré-imagens em relação às outras variações. As variações implementadas no modelo demonstram que reduzem o número de pré-imagens necessárias para uma boa cifragem. As duas variações finais demonstraram que realmente possuem maior potencial em realizar boas cifragens com o menor número de pré-imagens, logo terão uma análise mais detalhada.

• Análise da propagação de uma perturbação na imagem original

Como já foi discutido anteriormente, o modelo com a rotação da sensitividade sofre uma degradação do desempenho em uma implementação em hardware paralelo, pois interfere no paralelismo. O tempo gasto no processo de cifragem/decifragem está diretamente relacionado com o número de pré-imagens escolhido, então é desejado que o método produza boas cifragens utilizando-se do menor número de pré-imagens possível, consequentente no menor tempo. Os testes posteriores no modelo com a rotação da sensitividade são justificados, pois apesar de diminuir o paralelismo, para gerar uma cifragem de boa qualidade é necessário um número menor de pré-imagens. Para exemplificar esta

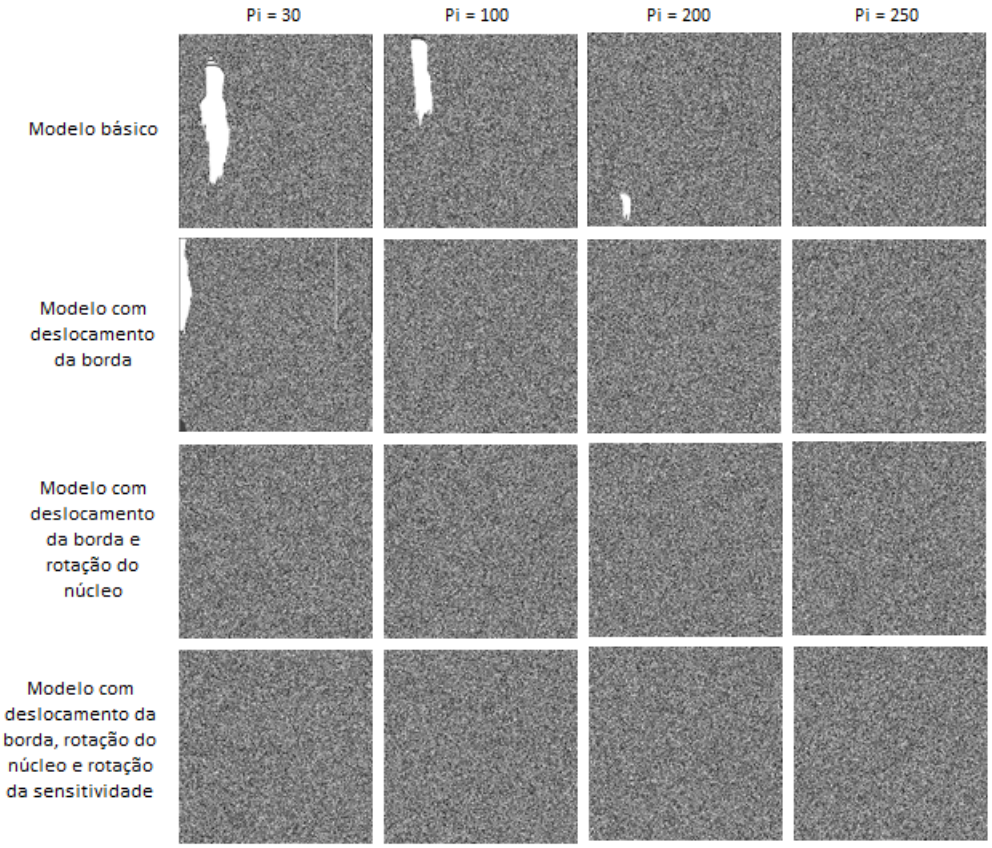


Figura 6.19: Evolução das variações do modelo

melhoria será realizada a cifragem da imagem original da figura 6.1 e de uma segunda imagem que sofreu uma pequena alteração em relação à imagem da figura 6.1. Esta alteração será feita no pixel central da imagem, correspondente a um bit, e pode ser vista na figura 6.20. Após a cifragem das imagens original e a perturbada, será gerada um nova imagem a partir da operação XOR entre elas. Esta nova imagem tem como objetivo mostrar a propagação de uma perturbação, ou seja, qual a diferença obtida entre a imagem cifrada a partir da imagem original e a imagem cifrada a partir da perturbada. Como a operação XOR é aplicada entre as duas imagens cifradas, a imagem resultado do XOR terá um bit preto sempre que o bit equivalente das duas imagens cifradas for diferente, ou branco caso sejam iguais. Para visualizar essa diferença será utilizado inicialmente 5 passos de pré-imagem.

Figura 6.20: Imagem original e a alterada em 1 pixel

A figura 6.21 (a) mostra a perturbação utilizando o modelo com sensitividade fixa,

enquanto que a figura 6.21 (b) exibe a perturbação para o modelo com rotação da sensitividade. A perturbação representada na figura 6.21 (b) é maior que a da figura 6.21 (a), logo é possível concluir que, com a mesma quantidade de pré-imagens, o modelo com rotação da sensitividade obteve uma melhor cifragem que o modelo com sensitividade fixa, sendo assim o modelo com sensitividade fixa precisaria de um número maior de pré-imagens para obter um resultado parecido com o do modelo com rotação da sensitividade. Neste exemplo, podemos comprovar sistematicamente o mesmo resultado contabilizando o percentual de 0s das imagens geradas a partir da operação XOR. Para boas cifragens é desejável que pequenas perturbações propaguem por toda a imagem. Portanto, as diferenças encontradas pela operação XOR devem conter 50% de 0s e 50% de 1s. Para imagens das figuras 6.21 (a) e 6.21 (b) temos os percentuais de zeros de 78% e 64%, respectivamente.

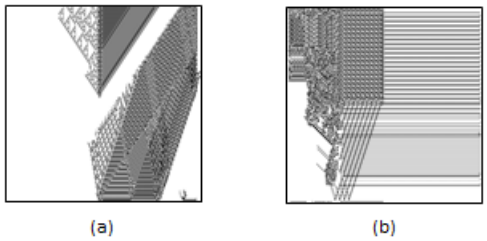


Figura 6.21: Diferenças entre imagens cifradas com 5 passos de pré-imagem: (a) Modelo sensitividade fixa (b) Modelo com rotação da sensitividade

A figura 6.22 apresenta a mesma análise das diferenças entre as imagens cifradas a partir da original e da perturbada para diferentes passos de pré-imagem: 10, 15, 20 e 30.

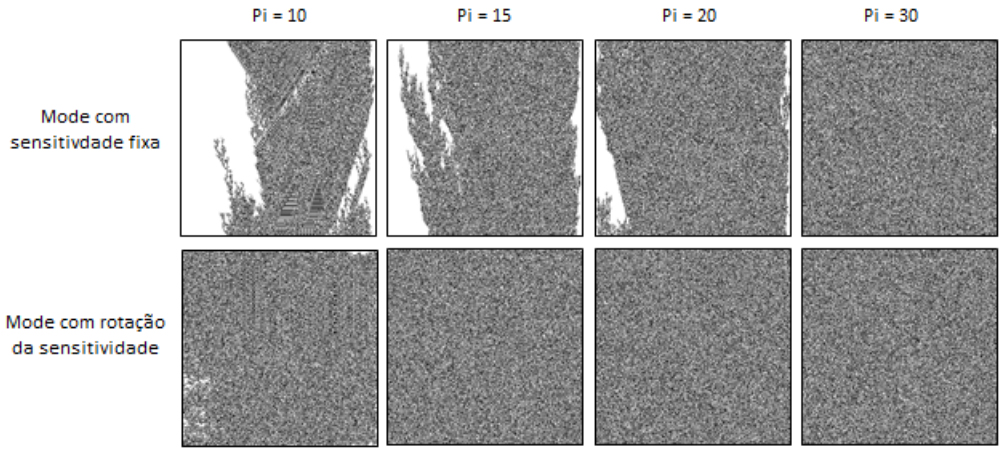


Figura 6.22: Diferenças entre imagens cifradas com diferentes passos de pré-imagem

Como é possível observar, no modelo com sensitividade rotacionada 15 pré-imagens são suficientes para propagar a perturbação por toda a imagem, enquanto que para o modelo com sensitividade fixa são necessários mais que 20 passos. A partir deste ponto é possível enumerar a vantagem e a desvantagem de cada modelo, abaixo é apresentada a vantagem e a desvantagem para cada modelo:

Modelo com sensitividade fixa: possui como vantagem um maior paralelismo no processo de cifragem, porém sua desvantagem é precisar de um maior número de pré-imagens para obter uma cifragem de qualidade.

Modelo com rotação da sensitividade: sua desvantagem é a perda de parte do paralelismo e a maior complexidade do modelo, contudo sua vantagem é que necessita de um menor número de pré-imagens para obter uma boa cifragem.

Como acreditamos que esse *trade-off* entre paralelismo e o número de passos de pré-imagem possa fazer com que uma variação seja a mais adequada dependendo da situação (por exemplo, se o hardware utilizado é sequencial ou paralelo), optamos por manter as duas variações nas análises desse capítulo.

6.2 Entropia

Para entender os resultados dos testes que serão apresentados, é necessário compreender a medida de entropia. A entropia é uma medida capaz de identificar a aleatoriedade em uma sequência de eventos, [Shannon 1948]. A entropia de uma sequência de k eventos é definida pela equação (6.1), onde p_i é a probabilidade de ocorrência do evento i:

$$S = -\sum_{i=1}^{k} p_i \times \log_2 p_i \tag{6.1}$$

Entretanto é necessário adaptar esta medida ao propósito deste trabalho, logo a entropia espacial de uma palavra binária de N bits é definida como sendo a entropia da ocorrência de N janelas de tamanho j, tendo $j < N$. O tamanho das janelas pode assumir qualquer valor, porém será definido pela equação (6.2), para que seja possível normalizar o valor da entropia (entre 0 e 1) para qualquer tamanho de palavra binária. Dessa forma a fórmula da entropia normalizada (s) é dada pela equação (6.3).

$$j = \log_2 N \tag{6.2}$$

$$s = \frac{-\sum_{i=1}^{k} p_i \times \log_2 p_i}{j} \tag{6.3}$$

Para exemplificar, suponha a sequência binária {1101001110100111} de 16 bits. A figura 6.23 demonstra como serão obtidas as 16 janelas de tamanho 4 ($j = 4$) para a sequência binária, note que para a obtenção das janelas será utilizado um contorno periódico. A partir das ocorrências apresentadas na tabela 6.1, é possível aplicar os dados na equação (6.1), pois a probabilidade p_i de um evento ocorrer é dado pelo número de ocorrências de uma janela i observada na sequência binária pelo total de janelas possíveis ($k = 16$). Assim para o exemplo da sequência {1101001110100111} teremos:

$$S = -[0 + 0 + 0 + (\frac{2}{16} \times \log_2 \frac{2}{16}) + (\frac{2}{16} \times \log_2 \frac{2}{16}) + 0 + 0 + (\frac{2}{16} \times \log_2 \frac{2}{16}) + 0 + (\frac{2}{16} \times \log_2 \frac{2}{16}) + (\frac{2}{16} \times \log_2 \frac{2}{16}) + 0 + 0 + (\frac{2}{16} \times \log_2 \frac{2}{16}) + (\frac{2}{16} \times \log_2 \frac{2}{16}) + (\frac{2}{16} \times \log_2 \frac{2}{16})] \quad (6.4)$$

Portanto $S = 3$ pela equação (6.3) e o valor normalizado é $s = \frac{3}{4} = 0,75$.

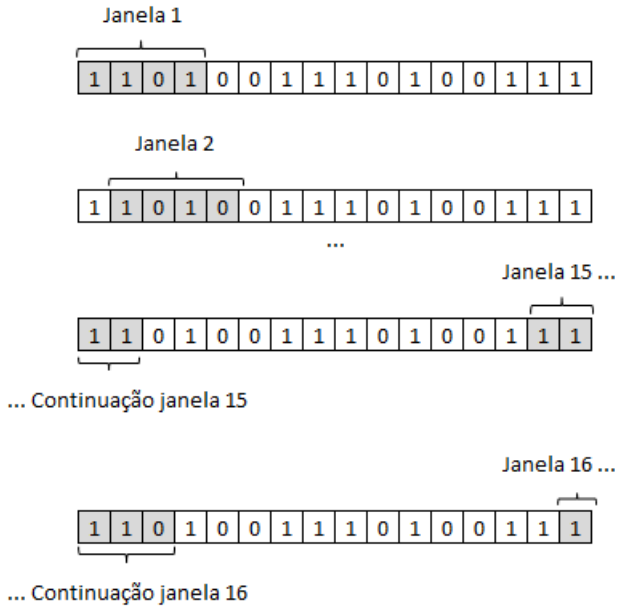


Figura 6.23: Janelas da sequência binária {1101001110100111}

Janelas	Ocorrências	Janelas	Ocorrências
0000	0	1000	0
0001	0	1001	2
0010	0	1010	2
0011	2	1011	0
0100	2	1100	0
0101	0	1101	2
0110	0	1110	2
0111	2	1111	2

Tabela 6.1: Ocorrência das janelas para a sequência binária {1101001110100111}

Para a entropia normalizada, quanto mais próximo o valor é de 1, significa que a sequência binária possui uma distribuição aleatória. Por outro lado, quanto mais próximo de 0, significa que a sequência é uniforme e/ou possui padrões ordenados. Sequências que possuem entropia acima de 0,8 possuem característica aleatória. Valor que foi obtido a

partir de experimentos realizados em [de Macedo 2007] e reproduzidos neste trabalho. A tabela 6.2 exibe algumas sequências binárias e sua respectivas entropias normalizadas.

Sequência binária	Entropia normalizada (s)
0000000000000000	0,000000
0101010101010101	0,250000
0000000010000000	0,327820
0011000000000000	0,405410
0000000100000100	0,5,0000
0010000010010000	0,607509
0110101100110101	0,714615
1010100111011110	0,800705
1110011010100000	0,906250
1110100101100001	1,000000

Tabela 6.2: Exemplo de entropias

A entropia descrita foi utilizada em [de Macedo 2007] e nos trabalhos [Oliveira et al. 2010a], [Oliveira et al. 2010b] e [Oliveira et al. 2010c], aplicada à cadeias de bits unidimensionais. Porém com este formato quando aplicado em cadeias bidimensionais, o valor resultante não fornece muita informação. Logo foi necessário realizar uma adaptação para que fosse possível medir corretamente a aleatoriedade das imagens cifradas. A adaptação, proposta neste trabalho, consiste em utilizar uma janela bidimensional ao invés de uma unidimensional. Assim, a informação extraída do valor da entropia será semelhante à obtida no modelo unidimensional, utilizando o número de ocorrências de cada janela possível para obter o p_i a ser aplicado na equação (6.1). Para uma janela de ordem $m \times n$ de j bits, tem-se que existem 2^j janelas possíveis. A normalização da equação (6.1) é obtida escolhendo-se uma janela $m \times n$ tal que $j = m \times n$ e $2^j = N$, sendo N o número de bits da imagem.

Por exemplo, a figura 6.24 apresenta um reticulado de ordem 16×16, logo $N = 256$. Portanto, a quantidade de bits da janela para a normalização de S deve ser dada por $j = \log_2 256 = 8$, sendo que a ordem da janela poderá ser qualquer combinação que resulte em 8 e que não seja unidimensional. Neste caso, poderá ser as ordens 2×4 ou 4×2. Na figura 6.25 pode-se visualizar a análise das 256 janelas 2×4 existentes na imagem para a contabilização das ocorrências das 256 janelas possíveis de ordem 2×4, apresentadas na figura 6.26.

No exemplo da figura 6.24, a contabilização das ocorrências das janelas resulta em uma entropia absoluta $S = 3,840490$ e uma entropia normalizada $s = 0,480061$. A figura 6.27 apresenta exemplos de figuras 16×16 com diferentes entropias.

Tanto o cálculo da entropia unidimensional, quanto o cálculo da entropia bidimensional foram usados nos testes que serão discutidos a seguir.

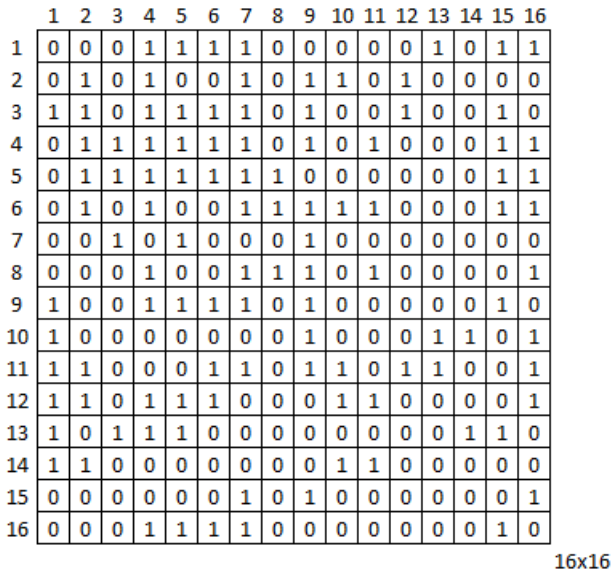


Figura 6.24: Construção das janelas de um reticulado de ordem 16×16

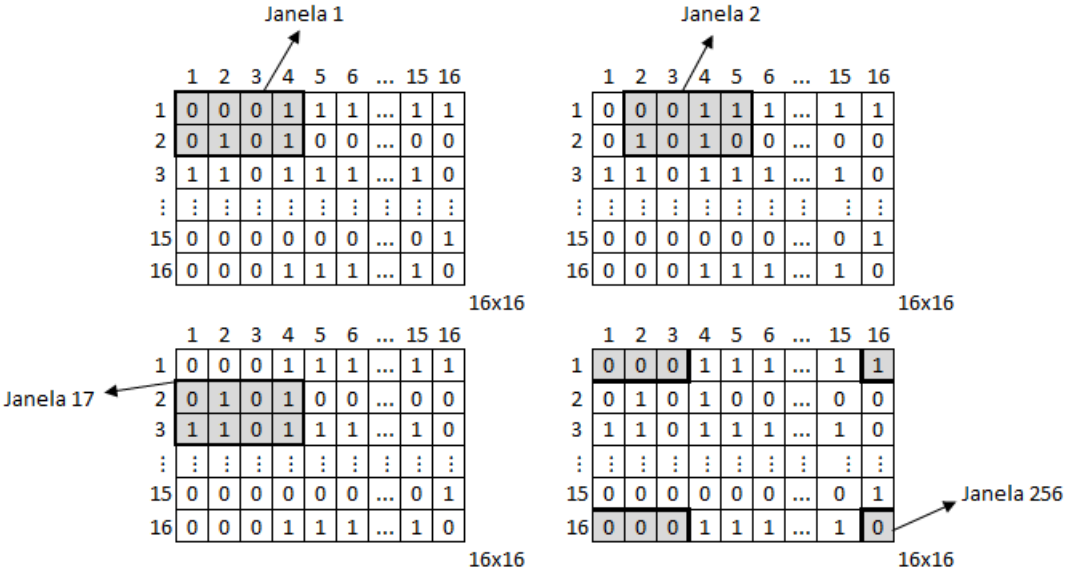


Figura 6.25: Construção das janelas de um reticulado de ordem 16×16

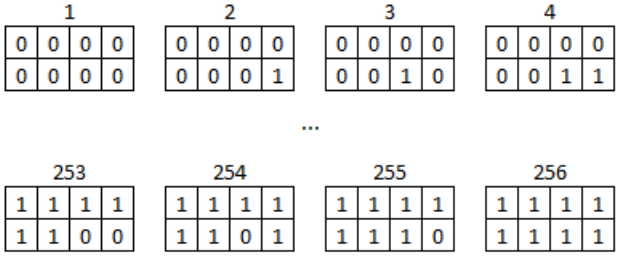


Figura 6.26: Janelas 2×4 possíveis

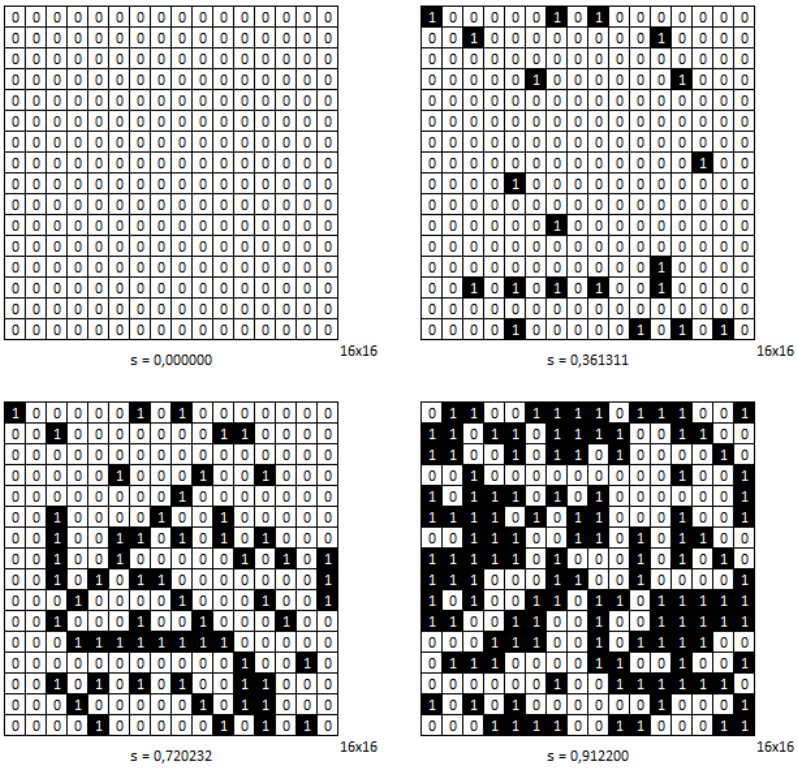


Figura 6.27: Exemplos de reticulados bidimensionais e suas entropias

6.3 Perturbação de 1 Bit na Imagem Original

Este teste tem por objetivo verificar se o método proposto consegue propagar a perturbação a partir da alteração em um único bit. Uma imagem original é cifrada e em seguida, uma imagem com uma alteração em um único pixel em relação à original também é cifrada. Ao final, uma nova imagem será gerada a partir da operação XOR entre as imagens cifradas, denominada "imagem da diferença". Esta imagem da diferença fornecerá a informação se a alteração de um único bit da imagem original foi propagada e ampliada na imagem cifrada. Na criptografia é desejável que esta diferença seja a maior possível, ou seja, dois textos claros semelhantes cifrados a partir da mesma chave devem gerar textos cifrados totalmente diferentes, de forma que a diferença entre os dois se aproxime de um texto aleatório [de Macedo 2007].

O AC bidimensional utilizado nos testes é de raio 1 resultando em uma regra de 32 bits, gerada a partir de um núcleo de 16 bits. O banco de imagens utilizadas nesse teste contém apenas imagens em preto e branco binarizadas obtidas em `http://www.cis.temple.edu/~latecki/TestData/mpeg7shapeB.tar.gz`.

Para este teste foram utilizados dois conjuntos: o conjunto das regras e o conjunto das imagens. O teste consiste em aplicar cada regra em todas as imagens, cifrando as mesmas por 30 passos de pré-imagem, e ao término da execução, registrar os seguintes dados para cada regra:

- Entropia unidimensional do núcleo da regra utilizada.
- Média das entropias bidimensionais geradas pelas imagens da diferença.
- Desvio padrão das entropias bidimensionais geradas pelas imagens da diferença.
- Menor entropia bidimensional encontrada nas imagens da diferença.
- Maior entropia bidimensional encontrada nas imagens da diferença.
- Média do percentual de zeros das imagens da diferença.
- Desvio padrão do percentual de zeros das imagens da diferença.
- Menor percentual de zeros encontrado nas imagens da diferença.
- Maior percentual de zeros encontrado nas imagens da diferença.

A razão de calcularmos a entropia do núcleo é que no modelo unidimensional foi identificado [de Macedo 2007] que núcleos com baixa entropia (abaixo de 0,70) não retornam cifragens seguras contra criptoanálises diferenciais. Isso se deve ao fato dessas regras não apresentarem um comportamento caótico, como seria desejável. Portanto, desejávamos investigar essa questão no modelo bidimensional. A entropia espacial da imagem da diferença foi calculada para verificarmos se existia algum tipo de padrão na diferença entre as imagens cifradas, o que denuncia uma cifragem de baixa qualidade. Foi constatado

que numa amostra de 10.000 imagens de 512×512 geradas de forma aleatória a entropia espacial média obtida foi de 0,954. Além disso, o percentual de zeros existente na imagem da diferença é uma das medidas mais utilizadas para avaliar a difusão de métodos criptográficos aplicados em textos binários. É esperado que uma imagem aleatória, gerada a partir de um pseudo gerador de números aleatórios de distribuição gaussiana, possua em torno de 50% de 0s, associado a um pequeno desvio padrão.

Além dessas estatísticas por regra, no momento em que os testes eram realizados, buscou-se identificar situações em que as regras não produziam uma cifragem de qualidade - baseado na propagação de uma perturbação simples - em pelo menos uma das imagens cifradas. Assim, uma regra era identificada com uma possível falha, se uma das situações abaixo ocorresse, em pelo menos uma das imagens cifradas:

- O percentual de zeros da imagem da diferença foi abaixo de 49%.
- O percentual de zeros da imagem da diferença foi superior à 51%.
- A entropia da imagem da diferença foi inferior à 0,94.
- Calculada a entropia unidimensional de cada linha da imagem da diferença e verificado se alguma é inferior à 0,8.
- Calculada a entropia unidimensional de cada coluna da imagem da diferença e verificado se alguma é inferior à 0,8.

Os valores adotados para as situações identificadas como falhas, foram definidos tomando-se como base os resultados de testes lineares executados em [de Macedo 2007] e valores próximos aos considerados ideais.

Neste teste, os modelos foram submetidos a um conjunto reduzido de 500 regras de raio 1 (32 bits), sendo que as 10 primeiras regras foram adicionadas manualmente e possuem baixa entropia, e as 490 regras restantes foram geradas aleatoriamente. Os núcleos de 16 bits das regras utilizadas podem ser encontrados no apêndice A. Para o modelo com sensitividade fixa foram utilizadas regras sensíveis ao bit do norte. Essas regras foram aplicadas na cifragem de um conjunto de 1000 imagens em preto e branco binarizadas de 512×512 pixels (bits), utilizando-se 30 passos de pré-imagens.

Para o modelo de sensitividade fixa, 48 regras registraram algum tipo de falha, sendo que 5 pertencem ao grupo das regras que foram adicionadas manualmente (em [de Macedo 2007] regras de baixa entropia mostraram que produzem resultados ruins). Regras que tiveram a média da entropia das imagens da diferença acima de 0,953 caracterizaram boas cifragens, isto é, resultados próximos aos aleatórios. Grande parte das regras que possuem baixa entropia no núcleo apresentaram resultados ruins, porém algumas ainda conseguiram resultados satisfatórios (não caracterizaram falhas). A tabela B.2 com os resultados para o modelo com sensitividade fixa pode ser vista no apêndice B. A tabela

6.3 resume os resultados obtidos para cada grupo de regras: (A) 452 regras que não apresentaram falhas; (B) 48 regras que apresentaram falhas.

Grupo	Nº regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	452	0,8225880	0,9540420	0,953704	49,9999008	0,0974069
B	48	0,6071659	0,7608850	0,430588	68,7463076	4,1769097

Tabela 6.3: Resumo dos resultados para sensitividade fixa

O modelo com rotação da sensitividade retornou um número menor de regras com falha do que o de sensitividade fixa. Para o conjunto das 500 regras, 26 apresentaram alguma falha na cifragem, sendo que 5 pertencem ao grupo das regras adicionadas manualmente e são as mesmas encontradas no modelo com sensitividade fixa. Análogo ao que ocorre com o método de sensitividade fixa, a entropia média das imagens da diferença que estiveram abaixo de 0,953 apresentaram problemas. No apêndice B pode ser encontrada a tabela B.3 com os resultados detalhados. A tabela 6.4 resume os resultados da tabela B.3.

Grupo	Nº regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	474	0,8166430	0,9540420	0,9537030	50,0001090	0,0976310
B	26	0,5332670	0,6019290	0,4028720	70,0713530	4,1044990

Tabela 6.4: Resumo dos resultados para rotação da sensitividade

Métodos criptográficos submetidos a este tipo de teste são caracterizados como bons, quando o desvio padrão do percentual de zeros resultar abaixo de 10% [Sen et al. 2002]. Neste caso, em ambas as variações do modelo bidimensional, os resultados encontrados estiveram abaixo de 10%. O mesmo pode ser dito em relação ao percentual de zeros, ambas as variações resultaram em um valor próximo de 50%, o que evidencia uma distribuição gaussiana.

Outro ponto que destaca a qualidade dos resultados é a aleatoriedade. A média da entropia para reticulados de tamanho 512×512, gerados a partir de um gerador de números aleatórios, é 0,9540 tendo um desvio padrão de 0,000103, enquanto que a média do percentual de zeros é dada por 49,999, com desvio padrão de 0,0973. Se analisarmos os valores obtidos, em ambos os métodos, para as regras que não apresentaram falhas, veremos que os resultados obtidos estão muito próximos dos valores obtidos para reticulados gerados a partir de um pseudo gerador de número aleatórios de distribuição gaussiana. Comparando-se os dois modelos é possível perceber que, o modelo com rotação da sensitividade retorna um número menor de regras que apresentam pelo menos uma falha. Porém, se analisarmos apenas os grupos de regras sem falhas nos dois modelos, eles se equivalem.

Uma característica que se sobressai nos grupos de regras que apresentaram falhas é o fato de os mesmos apresentarem uma média de entropia do núcleo baixa.

Como já era esperado, este teste mostrou que o método com rotação da sensitividade é melhor que o de sensitividade fixa quando utilizado o mesmo número de pré-imagens,

pois o conjunto de regras com falhas foi menor. Além disso, utilizamos os resultados desse teste para detectar as imagens que geraram os piores resultados, e estas foram utilizadas no teste fechado discutido na seção 6.5, pois consideramos elas as mais difíceis de cifrar do nosso conjunto de 1000 imagens.

6.4 Perturbação de 1 Bit na Chave

Os testes apresentados na seção 6.3 verificaram o comportamento dos modelos em relação a perturbações provocadas nas imagens originais. Esses testes verificaram a propriedade de difusão do método. Nessa seção, apresentaremos os testes que verificam o comportamento dos modelos quando a perturbação é provocada na chave. O teste consiste em cifrar uma imagem com uma chave qualquer e em seguida cifrar a mesma imagem com a chave alterada em apenas um bit.

As 500 regras utilizadas foram as mesmas utilizadas nos testes da seção 6.3 e podem ser vistas no apêndice A. As 1000 imagens utilizadas são as mesmas utilizada nos testes anteriores e podem ser encontradas em `http://www.cis.temple.edu/~latecki/TestData/mpeg7shapeB.tar.gz`. O AC utilizado é de raio 1 e foram utilizados 30 passos de pré-imagem para a cifragem. Para o modelo com sensitividade fixa foi utilizada a sensitividade ao bit do norte.

Cada regra foi aplicada na cifragem de cada uma das 1000 imagens e comparada à cifragem realizada por uma regra similar (complemento de 1 bit do núcleo/chave). A metodologia para apuração dos resultados foi semelhante à aplicada no teste da seção anterior.

Neste caso, a entropia espacial da imagem da diferença foi calculada a fim de investigar se o modelo atende o princípio da confusão, ou seja, a cifragem de uma mesma imagem a partir de chaves similares deve gerar imagens cifradas totalmente diferentes.

Os modelos se mostraram bastante eficientes a este tipo de teste: para o modelo com sensitividade fixa 9 regras apresentaram falhas, enquanto que no modelo com rotação da sensitividade apenas 4. No conjunto das regras com falha dos dois modelos, 2 regras pertencem ao grupo das regras que foram adicionadas manualmente e possuem baixa entropia no núcleo da regra.

As tabelas com os resultados completos para o modelo de sensitividade fixa e com rotação da sensitividade podem ser visualizadas no apêndice C, nas tabelas C.2 e C.3 respectivamente. As tabelas 6.5 e 6.6 apresentam os resultados médios obtidos com os modelos.

Ambos os modelos, para os resultados bons (linha A das tabelas), retornaram o desvio padrão do percentual de zeros bem abaixo de 10%, logo é possível concluir que os modelos distribuíram uniformemente os percentual de zeros na imagem da diferença.

O grau de aleatoriedade dos modelos foi bastante alto. Esta qualidade pode ser obser-

Grupo	N° regras	Média entropia núcleo	Média entropia diferença	Média mínima	Média desvio % 0s	Média desvio padrão % 0s
A	474	0,809034	0,954042	0,953703	50,000113	0,097605
B	9	0,413127	0,883892	0,647917	54,133690	1,841429

Tabela 6.5: Resumo dos resultados para sensitividade fixa

Grupo	N° regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	496	0,806705	0,954041	0,953682	49,999721	0,097678
B	4	0,206955	0,859577	0,668458	53,917051	1,788947

Tabela 6.6: Resumo dos resultados para rotação da sensitividade

vada e comparada com os valores dos reticulados gerados aleatoriamente. No conjunto das regras que não falharam, em ambos os métodos, os valores médios da entropia estiveram bem próximos de 0,9540 (valor obtido a partir de reticulados gerados aleatoriamente). É possível também verificar que o percentual de 0s foi adequado, pois a média se aproximou de 50%, tendo um desvio padrão semelhante ao de reticulados gerados aleatoriamente (0,0973).

Analisando-se as regras que apresentaram falhas no teste descrito nessa seção, foi constatado que pertencem ao conjunto de regras que apresentaram falhas no teste anterior. Neste teste, o grupo de regras com falhas também apresenta uma média baixa na entropia do núcleo. O próximo teste tentará identificar todas as regras que possuem algum tipo de falha, a partir da análise de um teste fechado para regras de raio 1.

6.5 Teste Fechado com as 20 Piores Imagens

Nos testes da seção 6.3, aproximadamente 10% e 5% das imagens cifradas com os modelos de sensitividade fixa e com rotação da sensitividade, respectivamente, apresentaram pelo menos uma falha em uma das 1000 imagens. Entretanto, esse conjunto é apenas uma amostra das possíveis chaves. Interessados em investigar qual seria o percentual de regras que apresentaram pelo menos uma falha considerando-se o espaço completo de chaves, novos testes foram realizados utilizando-se as 20 imagens de 512×512 mais difíceis do teste anterior. O número de passos de pré-imagem em cada cifragem foi mantido em 30. O espaço total de chaves testado é de 65536 chaves de raio 1 (2^{16} núcleos das regras com 16 bits). No modelo com sensitividade fixa, foram testadas todas as sensitividades possíveis (norte, leste, sul e oeste). A metodologia para obtenção dos resultados, foi a mesma utilizada na seção 6.3. Os dados detalhados obtidos por este teste não foram adicionados neste trabalho, pois geraram um volume muito grande de informação. A seguir, apresentamos um resumo e as principais análises desses dados.

Para o teste utilizando a sensitividade ao bit do norte foi detectado que 4771 regras apresentaram alguma falha na cifragem, o que corresponde à 7,27% do total de regras. As sensitividades à leste e ao oeste apresentaram 7,18% e 7,20%, que correspondem à 4710

e 4722 regras respectivamente. Quando realizado o teste com as regras sensíveis ao bit do sul o percentual de regras que apresentaram falhas foi de 7,22%, que representa 4734 regras. A pequena variação entre as sensitividades ocorre pelo fato das imagens não serem simétricas em todas direções, logo, a rotação de uma imagem pode ser mais prejudicial à uma sensitividade do que a outra.

O modelo que rotaciona a sensitividade apresentou melhores resultados, apenas 1790 regras apresentaram algum tipo de problema na cifragem. Esta quantidade representa 2,73% do total de regras. O modelo com a rotação da sensitividade mostrou-se novamente ser melhor que o de sensitividade fixa, mantido o número de pré-imagens fixo e igual à 30 para os dois modelos.

As tabelas 6.7, 6.8, 6.9 e 6.10 apresentam os resumos dos resultados obtidos com o modelo de sensitividade fixa com regras sensíveis ao bit do norte, leste, oeste e sul, respectivamente. Enquanto a tabela 6.11 apresenta o resumo dos resultados para o modelo com rotação da sensitividade.

Grupo	Nº regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	60765	0,8208795	0,9540420	0,9538467	50,0000814	0,0940979
B	4771	0,5332670	0,6019290	0,4028720	70,0713530	4,1044990

Tabela 6.7: Resumo dos resultados para sensitividade fixa com regras sensíveis ao bit do norte

Grupo	Nº regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	60826	0,8207863	0,9540421	0,9538467	50,0000093	0,0939452
B	4710	0,6662707	0,7342670	0,5505822	63,0632681	5,2197824

Tabela 6.8: Resumo dos resultados para sensitividade fixa com regras sensíveis ao bit do leste

Grupo	Nº regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	60814	0,8205244	0,9540131	0,9536585	50,0000108	0,0939266
B	4722	0,6643955	0,7361378	0,5519849	63,2239388	5,2330812

Tabela 6.9: Resumo dos resultados para sensitividade fixa com regras sensíveis ao bit do oeste

Grupo	Nº regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	60802	0,8208287	0,9540420	0,9538463	50,0000901	0,093970366
B	4734	0,6665098	0,7365420	0,5382759	62,9704316	5,908693644

Tabela 6.10: Resumo dos resultados para sensitividade fixa com regras sensíveis ao bit do sul

Em todos os conjuntos de regras que não apresentaram falhas, os resultados foram bastante satisfatórios, tendo como referência os valores de reticulados gerados aleatoriamente. Todas as médias das entropias espaciais estiveram sempre próximas à 0,9540

Grupo	N° regras	Média entropia núcleo	Média entropia diferença	Média entropia mínima	Média % 0s	Média desvio padrão % 0s
A	63746	0,8156089	0,9540419	0,9538455	50,0001155	0,0940720
B	1790	0,5985923	0,7558333	0,5032633	61,9547693	6,7854155

Tabela 6.11: Resumo dos resultados para rotação da sensitividade

(média da entropia para reticulados 512×512 gerados aleatoriamente), o mesmo ocorreu com os resultados para o percentual de 0s, em todos os casos sempre estiveram muito próximos à 0,0973.

Caso fossem analisados apenas os resultados para as regras que não geraram falhas (linha A das tabelas), ou mesmo as médias gerais (considerando-se todas as 65536 regras), levaria a uma conclusão errada de que o modelo de sensitividade fixa e o modelo com rotação da sensitividade possuem desempenho similar, Entretanto, o que evidencia que o modelo com rotação da sensitividade realiza uma melhor cifragem quando utilizado o mesmo número de pré-imagens é o número total de regras que falharam. Nos testes com o modelo de sensitividade fixa (em todas a sensitividades: norte, leste, oeste e sul) o número de regras que falharam é superior à quantidade retornada pelo modelo com rotação da sensitividade.

O desvio padrão indica que ambos os modelos realizam um boa cifragem, mesmo nos resultados para as regras que falharam (linha B das tabelas), o resultado esteve bem abaixo de 10%, caracterizando ambos os modelos como bons métodos criptográficos.

A fim de verificar se as piores regras do modelo com rotação da sensitividade estão contidas no conjunto das piores regras dos modelos de sensitividade fixa, foi realizada uma intersecção entre os conjuntos das piores regras a partir dos modelos com sensitividade fixa, e em seguida foi realizada a intersecção com o conjunto das piores regras do modelo com rotação da sensitividade. O conjunto da intersecção das piores regras dos modelos com a sensitividade fixa resultou em 4485 regras. Ou seja, a maior parte das regras que apresentaram alguma falha no modelo de sensitividade fixa é comum à aplicação ao norte, ao sul, a leste ou a oeste. Além disso, foi possível observar que todas as 1790 regras que apresentaram falhas no modelo com rotação da sensitividade está contido no conjunto de 4485 regras do modelo com sensitividade fixa. Uma análise posterior dessas regras permitiu comprovar que a entropia do núcleo está diretamente relacionada à elas como será apresentado na seção 6.7.1.

6.6 Análise de Histogramas

Nessa seção, apresentaremos resultados do teste realizado com o objetivo de verificar como a distribuição das cores na imagem é alterada pelo processo de cifragem. Em uma imagem em preto e branco binarizada é desejável que exista 50% de zeros e 50% uns na imagem resultante da cifragem. Numa imagem colorida, é desejável que as cores

disponíveis estejam distribuídas uniformemente pela escala de cinza na imagem cifrada.

A figura 6.28 (a) exibe uma imagem de tamanho 515×512 em escala de cinza e a figura 6.28 (b) o gráfico do seu histograma. A figura 6.29 (a) apresenta a imagem da figura 6.28 (a) cifrada e a figura 6.29 (b) o histograma associado à imagem cifrada. Para a cifragem foi utilizado o modelo com rotação da sensitividade, 30 passos de pré-imagens e uma regra sensível ao bit do norte criada a partir do núcleo {1101010110011101}.

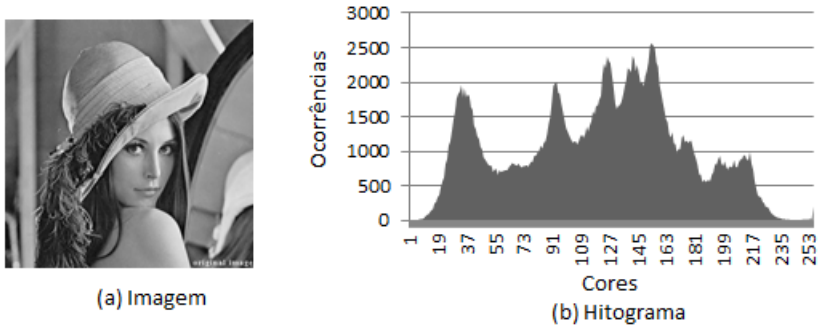


Figura 6.28: (a) Imagem original de 515×512 em escala de cinza (b) Histograma da imagem original

A imagem original possui o tamanho 515×512 e usa a escala de 256 níveis de cinza, sendo que a quantidade total de pixels é 262144. Logo, para que o histograma fosse totalmente uniforme seria necessário que cada pixel aparecesse 1024 vezes, pois a paleta total de cores é de 256. Note que as ocorrências de cores do histograma da imagem cifrada (ver figura 6.29 (b)) estão próximas de 1024, logo o processo de cifragem do modelo distribuiu uniformemente as cores na imagem cifrada. Dessa forma, percebe-se que o histograma da imagem cifrada não conserva qualquer informação a respeito da distribuição original do níveis de cinza da imagem que foi submetida à cifragem.

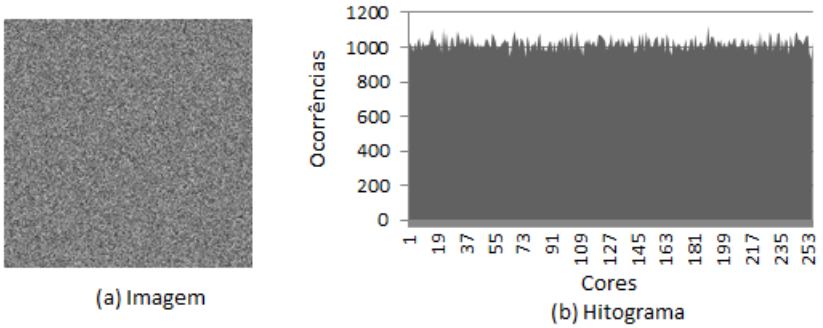


Figura 6.29: (a) Imagem cifrada (b) Histograma da imagem cifrada

Para realçarmos ainda mais essa característica, vamos analisar uma imagem com uma única cor cifrada numa escala de 256 níveis de cinza. Imagens com uma única cor, após a cifragem, também devem gerar histogramas uniformes. A figura 6.30 exibe uma imagem de uma única cor e o gráfico de seu histograma. Note que todos as ocorrências se concentram na última cor. Na figura 6.31 é apresentada a imagem cifrada gerada a partir da figura

6.30 (a) e também o gráfico do seu histograma. Para a cifragem foi utilizado um AC com as mesmas configurações do exemplo anterior. Dessa forma, é possível constatar que o método não preserva características referentes às cores das imagens, pois tanto na imagem com várias cores, quanto na imagem de um única cor, os histogramas foram semelhantes.

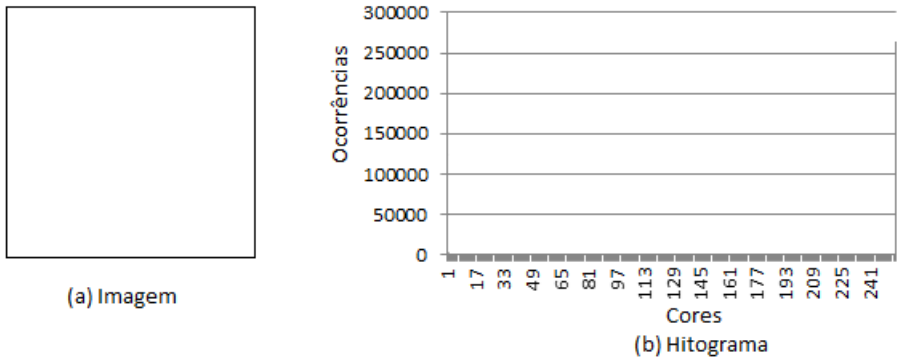


Figura 6.30: (a) Imagem original toda branca (b) Histograma da imagem toda branca

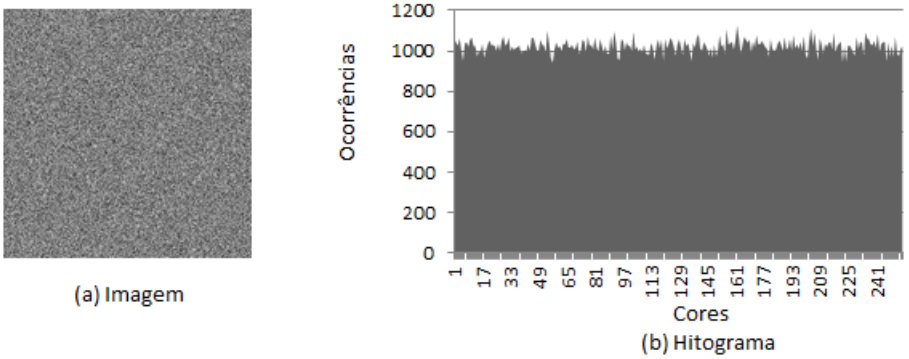


Figura 6.31: (a) Imagem cifrada (b) Histogram da imagem cifrada

Uma forma de verificar se os histogramas de diversas imagens estão próximos de uma distribuição gaussiana é através do cálculo do desvio padrão das ocorrências das cores. Como é esperada uma distribuição final em torno da média (no exemplo de 512×512 pixels e 256 níveis de cinza, a média é de 1024), o desvio padrão em torno dessa média deve ser baixo. Foi realizado um teste quantitativo que utilizou o desvio padrão para verificar se as imagens cifradas ficaram uniformes. Para o teste foram selecionadas 10 regras com entropias do núcleo diferentes que variam entre 0,756099 e 0,843750, e podem ser vistas na tabela 6.12. Quatro grupos de imagens de tamanho 128×128 pixels foram criados, com 100 imagens cada, são eles:

1. Imagens coloridas de 256 cores.
2. Imagens em escala de cinza (256 níveis de cinza).
3. Imagens preto e branca geradas em uma paleta de 256 cores.
4. Imagens preto e branca geradas em uma escala de 256 níveis de cinza.

Núcleo da Regra	Entropia do Núcleo
0001011111010000	0,843750
0000111111010100	0,820160
0000000010111101	0,818599
0000000101011101	0,812500
1110011101010111	0,800705
0000000010011101	0,787349
0000000100010111	0,781250
0000000101010111	0,769455
0000000001010011	0,757660
0000000010100011	0,756099

Tabela 6.12: Regras utilizadas para o teste de histograma

Foram utilizados 30 passos de pré-imagem a cada cifragem e ao final a média e o desvio padrão da distribuição de cores em cada imagem/chave foi computado. Ao final, para cada grupo de imagens foi calculado o desvio padrão médio obtido.

6.6.1 Resultados para o modelo com sensitividade fixa

A tabela 6.13 apresenta os resultados para os 4 grupos de imagens utilizando o modelo com sensitividade fixa. Pode-se observar que as médias dos desvios padrões ficaram muito próximas. É possível concluir que a quantidade de cores não interfere na qualidade de cifragem do método. E a média dos desvios padrões foram relativamente pequenas devido ao tamanho da imagens utilizas em relação à paleta de cores.

Grupo	Média do Desvio Padrão	
	Imagem Original	Imagem Cifrada
1	230,5122677	7,987783181
2	254,0782219	7,971262494
3	761,0842869	7,970302517
4	761,0842869	7,964790731

Tabela 6.13: Resultados histograma para o método com sensitividade fixa

6.6.2 Resultados para o modelo com rotação da sensitividade

A tabela 6.14 apresenta os resultados para os 4 grupos de imagens utilizando o modelo com rotação da sensitividade. Os resultados são muito parecidos com os apresentados na seção anterior, porém com um desvio padrão um pouco mais baixo. Da mesma forma que acontece no modelo com sensitividade fixa, a quantidade de cores utilizada na imagem, não interfere na qualidade da cifragem obtida.

Grupo	Média do Desvio Padrão	
	Imagem Original	Imagem Cifrada
1	230,5122677	7,969045071
2	254,0782219	7,969323919
3	761,0842869	7,956480221
4	761,0842869	7,964106386

Tabela 6.14: Resultados histograma para o método com rotação da sensitividade

6.7 Refinamento do Modelo e Ajuste da Especificação de Chaves

Após obtidos bons resultados médios nos testes das seções 6.3, 6.4, 6.5 e 6.6, sentiu-se a necessidade de novos testes a fim de obter a melhor configuração do AC bidimensional para a cifragem, buscando principalmente eliminar a existência de chaves com cifragem de baixa qualidade. A seguir serão apresentados os novos testes realizados com base no resultado dos testes anteriores.

6.7.1 Aumento da Quantidade de Pré-imagens

Este teste teve o objetivo de identificar qual a melhor quantidade de pré-imagens para a utilização dos modelos, ou mesmo se a quantidade utilizada nos testes anteriores (30) seria suficiente. Uma vez que no teste da seção 6.3 foi identificado que a direção da sensitividade fixa da regra não possui uma grande influência no resultado da cifragem, para este teste foram utilizadas apenas regras sensíveis ao bit do norte. Foi utilizado o conjunto das 20 imagens mais difíceis de cifrar encontradas pelo teste da seção 6.3. Neste teste foram utilizados dois conjuntos de regras: regras adequadas (não apresentaram falhas nos testes com 30 pré-imagens da seção 6.5) e regras que apresentaram algum tipo de falha no teste fechado. Para a cifragem foram avaliados 50 e 100 passos de pré-imagem. No modelo com sensitividade fixa ao norte, o conjunto das regras que apresentaram falhas é formado pelas 4771 regras obtidas no teste da seção 6.5. O conjunto das regras que apresentaram falhas para o modelo com rotação da sensitividade é formado pelas 1790 regras que geraram falha para este modelo no teste da seção 6.5. O conjunto das regras adequadas foi gerado a partir regras que não geraram falhas para ambos os modelos, elaborando-se uma amostra de 3000 regras para cada modelo.

A tabela 6.15 apresenta o resumo dos resultados para as regras adequadas em ambos os modelos. Como esperado, os resultados permaneceram bons, sendo que os dois modelos se comportaram de forma similar.

A tabela 6.16 apresenta os resultados para as amostras de regras que apresentaram falhas nos testes anteriores, para o modelo com sensitividade fixa e rotação da sensitividade. O que pode ser extraído desse resumo é que o modelo com sensitividade fixa realmente

SENSITIVIDADE FIXA						
Qtd. regras testadas	Qtd. regras falharam	Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
3000	0	30	0,9540420	0,9538467	50,0000814	0,0940979
3000	0	50	0,9540424	0,9538484	49,9996835	0,0940418
3000	0	100	0,9540426	0,9538471	50,0005505	0,0943461
ROTAÇÃO DA SENSITIVIDADE						
Qtd. regras testadas	Qtd. regras falharam	Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
3000	0	30	0,9540419	0,9538455	50,000115	0,0940720
3000	0	50	0,9540412	0,9538477	49,999964	0,0936551
3000	0	100	0,9540420	0,9538448	49,999646	0,0941941

Tabela 6.15: Resumo dos resultados para a amostra de regras adequadas para os modelos de sensitividade fixa e rotação da sensitividade

necessita de um número maior de pré-imagens para um bom resultado. Como pode ser visto, para 50 pré-imagens, o modelo com sensitividade fixa apresentou $2,5$ vezes mais regras com falhas que no modelo com rotação da sensitividade. Quando utilizado 100 passos de pré-imagens a diferença foi ainda maior, em torno de $3,3$ vezes. Entretanto, foi possível observar que em ambos os modelos, o número de regras que apresentaram falhas diminuiu com o aumento do número de pré-imagens. Assim, é possível perceber que algumas regras são mais lentas que outras na propagação de uma perturbação, necessitando de um número maior de pré-imagens para realizarem uma boa cifragem.

SENSITIVIDADE FIXA						
Qtd. regras testadas	Qtd. regras falharam	Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
4771	4771	30	0,6019290	0,4028720	70,0713530	4,1044990
4771	2550	50	0,7448467	0,5627248	62,6210029	5,5123728
4771	1092	100	0,7854670	0,6379857	60,1792532	4,5375466
ROTAÇÃO DA SENSITIVIDADE						
Qtd. regras testadas	Qtd. regras falharam	Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
1790	1790	30	0,7558333	0,5032633	61,9547693	6,7854155
1790	1010	50	0,7878464	0,5972448	59,9421392	5,2771091
1790	328	100	0,7737218	0,5244998	61,0497958	6,5379733

Tabela 6.16: Resumo dos resultados para regras que apresentaram falhas para sensitividade fixa e rotação da sensitividade

Além disso, analisando-se a entropia do núcleo dessas regras que apresentaram falhas, pudemos chegar a importantes observações:

- Considerando-se as 1790 regras que no modelo que rotaciona a sensitividade apresentaram falhas com 30 pré-imagens: 100% delas possuem entropia $\leq 0,7560$, sendo que apenas 52 delas têm entropia $\geq 0,75$. Considerando-se as 1010 regras que apresentaram alguma falha nesse modelo, obtidas com 50 pré-imagens, 100% delas possuem entropia abaixo de 0,70.
- Para o modelo com sensitividade fixa, considerando-se as 2550 detectadas com 50 passos de pré-imagens, 100% delas têm entropia $\leq 0,75766$, sendo que 112 delas têm entropia $\geq 0,75$ e apresentaram uma cifragem satisfatória quando analisadas

com detalhe. Para o cálculo de 100 pré-imagens, 1092 regras apresentaram falhas, contudo 100% delas possuem entropia abaixo de 0,70.

Realizando-se uma análise dos núcleos das regras, chegou-se aos dados da tabela 6.17. Se utilizarmos apenas regras com entropia do núcleo $\geq 0,70$, 90,1% do total do espaço de chaves seria utilizado, sendo que o modelo com sensitividade fixa deveria ser utilizado com 100 passos de pré-imagem, enquanto que no modelo com rotação da sensitividade seria necessário utilizar apenas 50 passos. Restringindo-se o espaço de chaves ainda mais para 82,7%, que compreende regras que possuem entropia $\geq 0,75$, poderiam ser utilizados valores menores de iterações: 50 e 30 passos de pré-imagens para os modelos com sensitividade fixa e rotação da sensitividade, respectivamente.

Entropia núcleo regra	Nº chaves restantes	% espaço de chaves	Modelos - Qtd. Pré-Imagens	
			Sensitividade fixa	Rotação da sensitividade
$\geq 0,70$	59584	90,92%	100	50
$\geq 0,75$	54208	82,71%	50	30

Tabela 6.17: Especificação para o número de pré-imagens

Dessa forma, com uma restrição no espaço de chaves de 16 bits poderíamos ter uma cifragem adequada para todas chaves restantes.

6.7.2 Aumento do Raio

O aumento do raio é uma das formas de aumentar o espaço de chaves, e assim aumentar a segurança do método. Este teste teve a finalidade de verificar o comportamento do método quando utilizadas regras de raio 2. Neste caso, o núcleo da regra possui 256 bits, logo o espaço de chaves potenciais é dado por 2^{256}.

Devido à inviabilidade de se realizar um teste fechado nesse espaço de chaves, foram utilizados 1000 núcleos de regras gerados aleatoriamente e 20 imagens 512×512, estas obtidas a partir do primeiro teste da seção 6.3, que detectou as imagens mais difíceis de serem cifradas. A metodologia utilizada nesse teste é a mesma explicada na seção 6.3. Como é esperado que o raio 2 produza uma maior aleatoriedade no método e uma propagação de perturbações mais rápida, para a cifragem foram utilizados 50 e 70 passos de pré-imagem.

Na tabela 6.18 é apresentado o resumo dos resultados obtidos. Nenhuma regra testada apresentou falha. Como pode ser visto, as entropias ficaram muito próximas de 0,9540 que foi o valor obtido para uma amostra de 10000 matrizes 512×512 geradas de forma aleatória (distribuição gaussiana). O percentual de zeros esteve sempre próximo de 50%, o que é confirmado pelo o desvio padrão muito baixo e próximo ao valor de referência obtido a partir de reticulados gerados aleatoriamente (desvio padrão igual à 0,0973).

Assim, concluímos que para a amostra de 1000 regras de raio 2 gerada de forma aleatória, o número de passos de pré-imagem igual a 50 seria suficiente.

SENSITIVIDADE FIXA				
Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
50	0,954040861	0,9538464	49,999638096	0,093542493
70	0,954041658	0,9538472	50,000360141	0,093762394
ROTAÇÃO DA SENSITIVIDADE				
Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
50	0,954042712	0,953847278	50,000650423	0,09373525
70	0,954041364	0,953846776	50,000410262	0,09498396

Tabela 6.18: Resumo dos resultados para sensitividade fixa e rotação da sensitividade para regras de raio 2

Ao analisarmos as 1000 regras geradas, verificamos que 100% delas tinha entropia do núcleo acima de 0,85. Assim, o método foi submetido a um novo teste utilizando as 20 imagens de 512×512 e três conjuntos de 1000 regras cada, com faixas de diferentes entropias. Para este teste foi utilizado apenas 50 passos de pré-imagem visto que na tabela 6.18 os resultados foram satisfatórios. A tabela 6.19 apresenta o resumo dos resultados obtidos para os modelos com sensitividade fixa e rotação da sensitividade.

SENSITIVIDADE FIXA					
Faixa entropia núcleo	Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
$\geq 0,70$ e $< 0,75$	50	0,954042074	0,9538478	50,000248814	0,093815987
$\geq 0,75$ e $< 0,80$	50	0,954042888	0,9538479	50,001261703	0,093521927
$\geq 0,80$ e $< 0,85$	50	0,954042070	0,9538481	49,999324309	0,094580499
ROTAÇÃO DA SENSITIVIDADE					
Faixa entropia núcleo	Número pré-imagens	Média entropia diferença	Média entropia diferença mínima	Média % 0s	Média desvio padrão % 0s
$\geq 0,70$ e $< 0,75$	50	0,95404280	0,953849855	50,0009098	0,09397085
$\geq 0,75$ e $< 0,80$	50	0,95404311	0,953846031	49,9998440	0,09442876
$\geq 0,80$ e $< 0,85$	50	0,95404223	0,953845238	50,0012135	0,09371169

Tabela 6.19: Resumo dos resultados para sensitividade fixa e rotação da sensitividade para regras de raio 2 testadas em 20 imagens e 1000 regras de diferentes entropias

Como pode ser visto na tabela 6.19 os resultados obtidos foram muito bons, mesmo com entropias de faixa diferentes os valores obtidos estiveram muito próximos, além de serem muito semelhantes aos valores obtidos com a geração de reticulados aleatórios (média da entropia 0,9540 e média do desvio padrão 0,0973). Também não encontramos diferenças significativas entre os modelos.

Pode-se concluir que o aumento do raio não interfere negativamente, contribuindo apenas para o aumento da segurança do método. Além disso, o modelo de sensitividade fixa se aproximou do desempenho do modelo com rotação, sendo possivelmente mais beneficiado pelo aumento da velocidade da propagação que o aumento do raio provocou.

6.7.3 Análise do Tamanho da Imagem

Para este teste foram utilizadas as mesmas 500 regras de raio 1 que podem ser vistas no apêndice A, exceto as que possuem entropia do núcleo abaixo de 0,7 resultando em 455 regras. O conjunto da imagens é formado pelas 20 imagens mais difíceis de serem cifradas

obtidas a partir do teste da seção 6.3. Entretanto, as imagens precisaram ser redimensionadas para os tamanhos adequados. Inicialmente as imagens de tamanhos diferentes foram cifradas com 30 passos de pré-imagem. A tabela 6.21 apresenta os resultados para os modelos com sensitividade fixa e rotação da sensitividade.

SENSITIVIDADE FIXA						
Tamanho imagem	Média entropia diferença	Média entropia diferença mínima	Média entropia aleatório	Média % 0s	Média desvio padrão % 0s	Media desvio padrão aleatório
16×16	0,8970423	0,8625775	0,89716499	49,9939694	3,1188706	3,09822455
32×32	0,9173590	0,9051041	0,91737412	50,0029367	1,5601708	1,55918281
64×64	0,9310789	0,9266132	0,93108402	50,0004802	0,7815171	0,77646818
128×128	0,9409148	0,9389436	0,94092020	50,0009696	0,3906178	0,39063443
256×256	0,9482631	0,9453027	0,94830163	50,0040861	0,2068404	0,19395876
ROTAÇÃO DA SENSITIVIDADE						
Tamanho imagem	Média entropia diferença	Média entropia diferença mínima	Média entropia aleatório	Média % 0s	Média desvio padrão % 0s	Media desvio padrão aleatório
16×16	0,8970380	0,8623609	0,89716499	50,1993407	3,1175409	3,09822455
32×32	0,9173596	0,9051416	0,91737412	50,0468987	1,5609464	1,55918281
64×64	0,9310762	0,9266299	0,93108402	50,0113580	0,7812736	0,77646818
128×128	0,9409135	0,9389423	0,94092020	50,0036728	0,3903309	0,39063443
256×256	0,9482982	0,9475424	0,94830163	50,0009564	0,1956016	0,19395876

Tabela 6.20: Resumo dos resultados para sensitividade fixa e rotação da sensitividade para regras de raio 1 testadas em 20 imagens de tamanhos diferentes

Como os valores esperados de entropia espacial e desvio do percentual de 0s se modificam em função do tamanho do reticulado, novas amostras de 10000 matrizes aleatórias de cada tamanho avaliado (16×16, 32×32, 64×64, 128×128 e 256×256) foram geradas e os valores obtidos são apresentados na tabela 6.21 (média entropia aleatório, média desvio padrão aleatório).

Como pode ser visto na tabela 6.21 não há diferença significativa entre os modelos com sensitividade fixa e com rotação da sensitividade. Ambos se mostraram bastante eficientes quando comparados com o valores obtidos a partir de uma geração de números aleatórios. Isso demonstra que o método possui um bom comportamento quando utilizando em imagens de tamanhos menores que 512×512, fixando-se o número de pré-imagens em 30.

• Análise da Quantidade de Pré-imagens Adequadas

Neste teste, buscou-se conseguir definir a quantidade de pré-imagens necessárias de acordo com o tamanho da imagem. Para este teste somente o modelo de sensitividade fixa foi utilizado. Foram utilizadas regras de raio 1 (455 regras do apêndice A com entropia $\geq 0,7$) e raio 2 (1000 regras utilizadas nos testes da tabela 6.19 entre 0,7 e 0,75) com entropias do núcleo $\geq 0,7$. A tabela 6.21 apresenta a quantidade de pré-imagens mínima necessárias para uma boa cifragem, considerando 20 imagens binarizadas quadradas. Para cada par (tamanho imagem, raio da regra), a quantidade de pré-imagens foi considerada satisfatória quando os valores de entropia espacial e desvio padrão do percentual de 0s de todas as regras se aproximaram dos valores médios obtidos pelas amostras aleatórias em cada tamanho analisado.

Tamanho imagem	Qtd. pré-imagens mínima	
	Raio 1	Raio 2
16×16	15	10
32×32	20	10
64×64	25	10
128×128	30	15
256×256	40	15
512×512	50	15
1024×1024	60	20
2048×2048	75	20

Tabela 6.21: Quantidade mínima de pré-imagens de acordo com o tamanho das imagens

Os valores apresentados na tabela são válidos para imagens quadradas binarizadas nos tamanhos avaliados. Para utilização do método na cifragem de imagens de tamanho arbitrário ou qualquer quantidade de cores é necessário considerar a quantidade total de bits. Na tabela 6.22 é apresentada a quantidade mínima de pré-imagens necessárias em relação à quantidade de bits da imagem se essa for quadrada. Na abordagem dos resultados apresentados na tabela, foi considerado número de células e o teto do valor mais próximo da tabela 6.21.

Número de bits	Qtd. pré-imagens mínima	
	Raio 1	Raio 2
≤ 256	15	10
≤ 1024	20	10
≤ 4096	25	10
$\leq 2^{14}$	30	15
$\leq 2^{16}$	40	15
$\leq 2^{18}$	50	15
$\leq 2^{20}$	60	20
$\leq 2^{22}$	75	20

Tabela 6.22: Quantidade mínima de pré-imagens de acordo com o tamanho das imagens quadradas

6.7.4 Análise da Geometria da Imagem (altura e largura)

Até o momento, foram apresentados apenas testes com imagens quadradas, ou seja, onde a largura da imagem é igual à altura. Nesta análise será verificado qual o grau de interferência da altura e da largura da imagem em relação ao número de pré-imagens, consequentemente à qualidade da imagem cifrada. A metodologia de apuração dos resultados é similar à utilizada nos testes anteriores. Devido à dificuldade de normalizar a entropia dos reticulados não quadrados gerados, neste teste não será apurado o valor da entropia da imagem da diferença, apenas o percentual de 0s e seu desvio padrão. Este teste também é importante para a utilização de imagens coloridas, pois a sugestão de utilização do método em imagens com mais de duas cores pode aumentar o reticulado a ser cifrado, tanto na largura, quanto na altura, ou ainda em ambos os lados, mas não de forma proporcional, transformando uma imagem quadrada em uma matriz binária retangular.

Para o teste foram utilizadas 20 imagens com tamanhos específicos e 500 regras geradas a partir dos núcleos do apêndice A, excluindo-se os núcleos que possuem entropia abaixo

de 0,7, totalizando um total de 445 regras. O bit do norte foi escolhido para a sensitividade das regras. A referência utilizada para o tamanho das imagens é altura × largura.

Inicialmente foi realizado um teste com imagens em preto e branco binarizadas de tamanhos 1024 e 4096 bits. Para o teste com imagens de 1024 bits serão utilizados os tamanhos 32×32, 4×256 e 256×4, enquanto que para as imagens de 4096 bits serão utilizados os tamanhos 64×64, 256×16 e 16×256. Em ambos os casos, a imagem quadrada serve como referência para o resultado das imagens retangulares. A tabela 6.23 apresenta os resultados para a imagens de 1024 bits retangulares, aplicando-se diferentes números de pré-imagens. Os valores médios com amostras aleatórias de 1024 bits são repetidos a cada linha para facilitar a comparação. Com esses resultados é possível constatar que a geometria da imagem interfere na qualidade de texto cifrado. Note que para uma boa cifragem a imagem quadrada 32×32 necessita apenas de 20 passos de pré-imagens, ao passo que a imagem 256×4 precisa de pelo menos 65 passos, enquanto a imagem 4×256 nem mesmo com 70 passos de pré-imagens conseguiu-se realizar uma boa cifragem. Logo, foi constado que a geometria da imagem interfere no resultado da cifragem. Essa interferência está associada com a propagação de uma perturbação de acordo com a sensitividade da regra. Ou seja, para uma regra com sensitividade ao bit do norte, a principal direção de propagação é do sul para o norte e a altura determina o número de pré-imagens necessárias, quando a imagem se aproxima de um quadrado. Por outro lado, se a largura se torna muito maior que altura, o AC tem muita dificuldade de propagar perturbações no eixo leste-oeste deteriorando bastante o desempenho do modelo.

Tamanho imagem	Qtd. Bits	PI	Média % 0s	Média desvio % 0s	Média %0s máximo	Média %0s mínimo	Média % 0s aleatório	Desvio %0s aleatório
32x32	1024	20	50,0085805	1,52042127	52,925079	47,05802317	50,01176758	1,559182818
4x256	1024	30	96,2927602	0,82981706	97,7747541	94,6063027	50,01176758	1,559182818
4x256	1024	40	95,0921041	0,98700141	96,8670997	93,1170997	50,01176758	1,559182818
4x256	1024	50	93,9017402	1,12827803	95,9601035	91,6171436	50,01176758	1,559182818
4x256	1024	60	92,7120896	1,27568027	95,0322595	90,1395716	50,01176758	1,559182818
4x256	1024	65	92,1129081	1,33515035	94,5670207	89,4695839	50,01176758	1,559182818
4x256	1024	70	91,5095461	1,38615810	94,0673279	88,7328827	50,01176758	1,559182818
256x4	1024	30	51,5739444	3,10571199	59,0201457	47,2553107	50,01176758	1,559182818
256x4	1024	40	50,4997257	2,10348451	55,1931179	47,0674596	50,01176758	1,559182818
256x4	1024	50	50,1818491	1,71226823	53,7320049	47,0722875	50,01176758	1,559182818
256x4	1024	60	50,0612162	1,58222049	53,2614993	47,1311008	50,01176758	1,559182818
256x4	1024	65	50,0255003	1,53089056	53,1008602	47,1073999	50,01176758	1,559182818
256x4	1024	70	50,0013277	1,52929009	53,0297577	47,0481478	50,01176758	1,559182818

Tabela 6.23: Resultado da análise da quantidade de pré-imagens necessárias para imagens retangulares de 1024 bits

A tabela 6.24 apresenta o resultado para imagens retangulares de 4096 bits. Como pode ser visto, existe o mesmo problema ocorrido nas imagens de retangulares de 1024 bits. Nenhum resultado de pré-imagem apresentado mostrou-se satisfatório para imagens de 16×256. Entretanto, esses resultados foram muito superiores aos obtidos com as imagens 4×256, o que mostra que quanto mais desbalanceada a proporção entre altura e largura, pior é o desempenho do método. A partir de 30 pré-imagens já foi possível obter bons resultados com as imagens 256×16, aproximando-se dos resultados obtidos

de matrizes geradas aleatoriamente.

Tamanho imagem	Qtd. Bits	PI	Média % 0s	Média desvio % 0s	Média %0s máximo	Média %0s mínimo	Média % 0s aleatório	Desvio %0s aleatório
64x64	4096	20	49,9937785	0,7418682	51,434998	48,5441537	50,006435	0,776468
256x16	4096	30	50,0049678	0,7441235	51,438838	48,5563334	50,006435	0,776468
256x16	4096	40	50,0114115	0,7371531	51,438344	48,5870567	50,006435	0,776468
256x16	4096	50	49,9978301	0,7576483	51,472853	48,5121137	50,006435	0,776468
256x16	4096	60	50,0067783	0,7535384	51,477571	48,5726277	50,006435	0,776468
256x16	4096	65	50,0074284	0,7578990	51,460674	48,5335103	50,006435	0,776468
256x16	4096	70	49,9904373	0,7485076	51,442349	48,5379542	50,006435	0,776468
16x256	4096	30	59,2428294	2,5877802	64,513254	54,6132702	50,006435	0,776468
16x256	4096	40	53,1325464	1,6769871	56,766919	50,2785946	50,006435	0,776468
16x256	4096	50	51,0422911	1,1115429	53,337155	49,0593728	50,006435	0,776468
16x256	4096	60	50,3333644	0,9002971	52,191285	48,6836705	50,006435	0,776468
16x256	4096	65	50,1879965	0,8312832	51,873683	48,6064782	50,006435	0,776468
16x256	4096	70	50,1100717	0,8030002	51,712879	48,5946278	50,006435	0,776468

Tabela 6.24: Resultado da análise da quantidade de pré-imagens necessárias para imagens retangulares de 4096 bits

Constatado que o problema com a geometria da imagem existe, foi elaborada uma estratégia para minimizar o esforço computacional e maximizar a qualidade de cifragem. Para imagens em que a altura for maior que a largura, regras sensíveis ao bit do norte ou sul deverão ser utilizadas, em contrapartida, imagens em que a largura for maior que altura, deverão ser utilizadas regras sensíveis ao bit do leste ou oeste. O número de pré-imagens a ser escolhido deverá obedecer o valor de referência mais próximo (não o menor) nas imagens quadradas, de acordo com o maior lado da imagem. Por exemplo, numa imagem 100×20 (altura $\times$ largura), deve-se escolher a sensitividade norte ou sul e usar o número de pré-imagens referente à imagem quadrada 128 (que necessita de 25 pré-imagens para o raio 1 e 15 pré-imagens para o raio 2). Dessa forma, o método já consegue obter bons resultados com número de pré-imagens um pouco maior que nas imagens quadradas. Com essa estratégia, pode até ser utilizado um número de pré-imagens maior que o necessário, porém o risco de retornar uma imagem cifrada de baixa qualidade é diminuído.

A tabela 6.25 apresenta alguns resultados para essa abordagem com tamanhos de imagens diferentes utilizando-se regras de raio 1 e 2 com sensitividade ao norte. Como pode ser visto a abordagem descrita anteriormente apresenta bons resultados.

6.7.5 Proposta para Cifragem de Imagens Quadradas com Várias Cores

Como a apresentado na seção anterior, existe uma dependência do número de pré-imagens necessário quanto à geometria da imagem. Então, este problema poderá ser evidenciado em imagens quadradas de várias cores a partir da estratégia citada na seção 5.6 (distribuição de 1 pixel em 8 colunas). De posse dos resultados obtidos anteriormente, uma estratégia para distribuição dos pixels foi elaborada a fim de garantir a segurança e o desempenho do método.

RAIO 1								
Tamanho imagem	Qtd. Bits	PI	Média % 0s	Média desvio % 0s	Média %0s máximo	Média %0s mínimo	Média % 0s aleatório	Desvio %0s aleatório
64x32	2048	25	49,9942503	1,05878464	52,0066713	47,9336376	49,992265	1,1173201
128x64	8192	30	50,0015677	0,52353006	51,0152409	48,9928513	50,000175	0,5535093
256x128	32768	30	49,9974310	0,26386763	50,5100275	49,4932573	49,9978421	0,2761566
512x256	131072	50	50,0005701	0,13270958	50,2629621	49,7430831	50,000048	0,1370385
RAIO 2								
Tamanho imagem	Qtd. Bits	PI	Média % 0s	Média desvio % 0s	Média %0s máximo	Média %0s mínimo	Média % 0s aleatório	Desvio %0s aleatório
64x32	2048	10	50,0080264	1,0750764	52,1128862	47,9698472	49,992265	1,1173201
128x64	8192	15	49,9982841	0,5366342	51,0634107	48,9576841	50,000175	0,5535093
256x128	32768	15	49,9958986	0,2665367	50,5199852	49,4876750	49,997842	0,2761566
512x256	131072	15	50,0011013	0,1312592	50,2588181	49,7440861	50,000048	0,1370385
1024x512	524288	20	49,9995790	0,0666408	50,1284314	49,8694833	49,999477	0,0695368

Tabela 6.25: Resultado da análise da quantidade de pré-imagens necessárias para imagens retangulares utilizando regras de raio 1 e 2

Suponha que deseja-se cifrar uma imagem quadrada de tamanho $Q \times Q$, e esta utiliza 256 cores. Logo, são necessários 8 bits para representação de cada cor. Nesta abordagem os bits não serão distribuídos consecutivamente em uma única direção, mas sim, poderão ser utilizadas as distribuições 2×4 ou 4×2 em linhas e colunas dependendo da implementação utilizada (sequencial ou paralela).

Em uma implementação sequencial, não importa se existem mais linhas ou colunas na imagem, pois o tempo de processamento é o mesmo. Então será escolhido o caso que necessite um número menor de pré-imagens. Foi constatado experimentalmente que, para imagens retangulares com altura que não ultrapasse duas vezes a largura, o número de pré-imagens a ser utilizado pode ser definido em função do menor lado (largura). Caso a geometria seja deformada em relação ao quadrado (por exemplo, altura oito vezes a largura) tal afirmação não pode ser feita. Portanto, no caso de implementação sequencial, a distribuição dos pixels a ser utilizada para transformar uma imagem com uma paleta de 256 cores (ou níveis de cinza) em uma matriz binária será 4×2. Nesse caso, o reticulado a ser cifrado será $4Q \times 2Q$ (com mais linhas) e basta utilizar uma quantidade de pré-imagens adequado para uma imagem quadrada binarizada $2Q \times 2Q$.

Por outro lado, em uma abordagem com uma implementação paralela, uma linha é cifrada em paralelo (para regras sensíveis ao bit do norte ou sul) independentemente do número de colunas. Logo, deverá ser escolhido o caso em que resulte em um menor número de linhas, que é transformar cada pixel em 2×4. Nessa distribuição, o número de linhas será inferior, reduzindo o tempo de cálculo de cada pré-imagem à metade (comparando à distribuição 4×2). Entretanto, o número de pré-imagens necessário será maior, visto que ele deverá ser dado pelo maior lado (largura). Contudo, nas dimensões analisadas, esse número nunca dobra, especialmente no raio 2. Nesse caso, o reticulado a ser cifrado será $2Q \times 4Q$ e basta utilizar a quantidade de pré-imagens para imagens binarizadas de tamanho $4Q \times 4Q$.

A tabela 6.26 apresenta alguns exemplos para as configurações a serem utilizadas quanto a utilização do método proposto para cifragem de imagens de 256 cores. A tabela

6.27 resume as características mais adequadas para cada tipo de implementação (sequencial/paralela).

RAIO 1								
Tamanho imagem	Qtd. Bits	PI	Média % 0s	Média desvio % 0s	Média %0s máximo	Média %0s mínimo	Média % 0s aleatório	Desvio %0s aleatório
64x32	2048	25	49,9942503	1,05878464	52,0066713	47,9336376	49,9922656	1,1173201
32x64	2048	20	50,0250834	1,07060350	52,1222129	47,9543758	49,9922656	1,1173201
64x128	8192	30	50,0038527	0,53399511	51,0516151	48,9855819	50,0001757	0,5535093
128x64	8192	25	50,0012165	0,53120484	51,0374056	48,9630332	50,0001757	0,5535093
128x256	32768	30	50,0245670	0,29545788	50,6434545	49,4967137	49,9978421	0,2761566
256x128	32768	25	50,0082874	0,27225316	50,5541854	49,4880110	49,9978421	0,2761566
256x512	131072	50	50,0035840	0,14490525	50,3102094	49,7390713	50,0000480	0,1370385
512x256	131072	40	50,0046021	0,13658402	50,2756371	49,7463543	50,0000480	0,1370385
512x1024	524288	60	50,0319002	0,11610977	50,2891617	49,8700825	49,9994777	0,0695368
1024x512	524288	50	50,0393059	0,08551714	50,2136689	49,8743584	49,9994777	0,0695368
RAIO 2								
Tamanho imagem	Qtd. Bits	PI	Média % 0s	Média desvio % 0s	Média %0s máximo	Média %0s mínimo	Média % 0s aleatório	Desvio %0s aleatório
32x64	2048	15	49,9877490	1,07634637	52,0637289	47,9182760	49,992265	1,1173201
64x32	2048	10	50,0080264	1,07507647	52,1128862	47,9698472	49,992265	1,1173201
64x128	8192	15	49,9932079	0,52912987	51,0249516	48,9708512	50,000175	0,5535093
128x64	8192	10	49,9982841	0,52663429	51,0634107	48,9576841	50,000175	0,5535093
128x256	32768	20	50,0000171	0,26398696	50,5185244	49,4823258	49,997842	0,2761566
256x128	32768	15	49,9958986	0,26653674	50,5199852	49,4876750	49,997842	0,2761566
256x512	131072	20	49,9987072	0,13223301	50,2594645	49,7436403	50,000048	0,1370385
512x256	131072	15	50,0011013	0,13125927	50,2588181	49,7440861	50,000048	0,1370385
512x1024	524288	20	50,0010572	0,06600770	50,1288051	49,8723053	49,999477	0,0695368
1024x512	524288	15	49,9995790	0,06664080	50,1284314	49,8694833	49,999477	0,0695368
1024x2048	2097152	25	49,9998865	0,03312090	50,0635863	49,9354974	50,000178	0,0347588
2048x1024	2097152	20	50,0001090	0,03287595	50,0634767	49,9377563	50,000178	0,0347588

Tabela 6.26: Exemplo de configurações para cifragem de imagens de 256 cores para regras de raio 1 e 2

RAIO 1					
Tamanho imagem	Qtd. Bits	Implementação	Matriz de bits	Referência nº pré-imagens	Nº pré-imagens mínimo
16x16	2048	SEQUENCIAL	64x32	32x32	20
16x16	2048	PARALELA	32x64	64x64	25
32x32	8192	SEQUENCIAL	128x64	64x64	25
32x32	8192	PARALELA	64x128	128x128	30
64x64	32768	SEQUENCIAL	256x128	128x128	30
64x64	32768	PARALELA	128x256	256x256	40
128x128	131072	SEQUENCIAL	512x256	256x256	40
128x128	131072	PARALELA	256x512	512x512	50
256x256	524288	SEQUENCIAL	1024x512	512x512	50
256x256	524288	PARALELA	512x1024	1024x1024	65
512x512	2097152	SEQUENCIAL	2048x1024	1024x1024	65
512x512	2097152	PARALELA	1024x2048	2048x2048	80
RAIO 2					
Tamanho imagem	Qtd. Bits	Implementação	Matriz bits	Referência nº pré-imagens	Nº pré-imagens mínimo
16x16	2048	SEQUENCIAL	64x32	32x32	10
16x16	2048	PARALELA	32x64	64x64	10
32x32	8192	SEQUENCIAL	128x64	64x64	10
32x32	8192	PARALELA	64x128	128x128	15
64x64	32768	SEQUENCIAL	256x128	128x128	15
64x64	32768	PARALELA	128x256	256x256	15
128x128	131072	SEQUENCIAL	512x256	256x256	15
128x128	131072	PARALELA	256x512	512x512	15
256x256	524288	SEQUENCIAL	1024x512	512x512	15
256x256	524288	PARALELA	512x1024	1024x1024	20
512x512	2097152	SEQUENCIAL	2048x1024	1024x1024	20
512x512	2097152	PARALELA	1024x2048	2048x2048	25

Tabela 6.27: Exemplos de números de pré-imagens para imagens de 256 cores para os raios 1 e 2

6.8 Análise do Tempo de Processamento

6.8.1 Análise de uma Implementação Sequencial

Este teste realizou um comparativo do tempo de cifragem entre o sistema criptográfico AES e o modelo com sensitividade fixa proposto nessa dissertação. A plataforma JAVA foi utilizada para implementação dos modelos, entretanto a implementação utilizada para o AES foi desenvolvida pela biblioteca JCE (Java Cryptography Extension) disponibilizada pela ORACLE (`http://www.oracle.com/technetwork/java/index.html`).

O teste consistiu em obter o tempo médio de cifragem a partir de 100 cifragens de imagens com tamanhos diferentes. Para evitar a utilização dos recursos de melhoria de desempenho implementados na JVM (Java Virtual Machine), cada execução foi realizada de maneira única, ou seja, não foi utilizada uma estrutura de repetição no programa de cifragem para realizar a 100 execuções.

O número de pré-imagens utilizado no modelo proposto tomou como base os resultados obtidos anteriormente. Para o AES foi utilizada uma chave de 128 bits e o modo de operação de blocos foi o CFB.

A tabela 6.28 apresenta os tempos médios de execução para cada modelo, bem como o número de vezes que o modelo proposto é mais lento que o AES.

Como pode ser visto, o AES mostrou-se menos suscetível à mudança do tamanho da imagem a ser cifrada. Isto é justificado pelo fato do AES utilizar a cifragem de blocos

Imagens de tamanho 16×16 bits		
Método de cifragem	Tempo médio (ms)	Nº × mais lento AES
AES CFB (Chave 128 bits)	439,07	-
Raio 1 - 15 Pré-imagens	11,6	0,0264
Raio 2 - 10 Pré-imagens	9,31	0,0212
Imagens de tamanho 32×32 bits		
Método de cifragem	Tempo médio (ms)	Nº × mais lento AES
AES CFB (Chave 128 bits)	443,41	-
Raio 1 - 20 Pré-imagens	44,62	0,1006
Raio 2 - 10 Pré-imagens	28,94	0,0652
Imagens de tamanho 64×64 bits		
Método de cifragem	Tempo médio (ms)	Nº × mais lento AES
AES CFB (Chave 128 bits)	444,06	-
Raio 1 - 25 Pré-imagens	63,94	0,1439
Raio 2 - 10 Pré-imagens	48,61	0,1094
Imagens de tamanho 128×128 bits		
Método de cifragem	Tempo médio (ms)	Nº × mais lento AES
AES CFB (Chave 128 bits)	448,72	-
Raio 1 - 30 Pré-imagens	119,97	0,2673
Raio 2 - 15 Pré-imagens	95,26	0,2122
Imagens de tamanho 256×256 bits		
Método de cifragem	Tempo médio (ms)	Nº × mais lento AES
AES CFB (Chave 128 bits)	449,48	-
Raio 1 - 40 Pré-imagens	367,18	0,8168
Raio 2 - 15 Pré-imagens	215,54	0,4795
Imagens de tamanho 512×512 bits		
Método de cifragem	Tempo médio (ms)	Nº × mais lento AES
AES CFB (Chave 128 bits)	456,54	-
Raio 1 - 50 Pré-imagens	1491,16	3,2662
Raio 2 - 15 Pré-imagens	588,7	1,2894

Tabela 6.28: Tempos médios modelos criptográficos em um implementação sequencial

de tamanho fixo (128 bits). Dessa forma, o tempo de cifragem de um bloco é aproximadamente constante e, à medida que as imagens são aumentadas, o número de blocos é aumentado, então o tempo de cifragem aumenta de forma aproximadamente proporcional com o aumento da imagem. Entretanto, é possível observar pela tabela 6.28, que o aumento do tempo é pequeno comparado ao aumento do número de bits. Por exemplo, uma imagem de 16×16 bits demorou em média 439 ms, enquanto uma imagem de 512×512 bits demorou em média 456 ms. Devido no AES o tamanho da imagem não interferir muito no tempo final, é possível que grande parte do processamento seja atribuído ao carregamento (leitura *S-Box*, tabelas de transposição, etc). Quando utilizadas imagens menores que 256×256, o tempo de cifragem para o modelo proposto de sensitividade fixa foi inferior ao AES. A partir do tamanho 512×512, o AES obteve melhores resultados, porém é importante ressaltar que a implementação para o modelo proposto não é ótima e poderia ser aperfeiçoada/otimizada em diversos pontos. Além disso, a principal motivação para estudo do modelo baseado em ACs está na sua possibilidade de paralelização, como será discutido na próxima seção.

6.8.2 Análise de uma Implementação Paralela

O estudo de ACs em criptografia é justificado devido à possibilidade de se paralelizar os processos de cifragem e decifragem conforme foi apresentado no capítulo 5, o modelo

de sensitividade fixa permite o paralelismo de grande parte do processo de cifragem. Para exemplificar o ganho de desempenho entre uma implementação sequencial e uma paralela, suponha que a obtenção do novo valor de cada célula, no cálculo da pré-imagem, leve 1 ciclo de relógio de processamento, e deseja-se cifrar um imagem de tamanho 512×512 binarizada através de um AC de raio 1 e 50 passo de pré-imagem. O número de ciclos de relógio necessário para a cifragem sequencial e paralela (teórica) é dado a seguir, onde m é o número de linhas da imagem, n o número de colunas, r o raio e P a quantidade pré-imagens utilizada.

$$\begin{aligned} NC_{seq} &= m \times n \times P \\ &= 512 \times 512 \times 50 \\ &= 13.107.200 \end{aligned} \tag{6.5}$$

$$\begin{aligned} NC_{par} &= 2P + m - 2r + 1 \\ &= 2 \times 50 + 512 - 2 \times 1 + 1 \\ &= 611 \end{aligned} \tag{6.6}$$

Assim é possível observar que o número de ciclos de relógio necessários para uma implementação paralela é extremamente menor que uma implementação sequencial. Em termos teóricos, é possível verificar que a cifragem de uma imagem 512×512 em um único bloco pode ser reduzida por um fator da ordem de 2×10^4. Além disso, quanto maior o tamanho da imagem, maior será o ganho com o paralelismo. Porém, é importante lembrar que esta análise é teórica e em uma implementação real existem diversas variáveis que dificultam o completo paralelismo suportado pelo método.

O AES também permite um certo paralelismo, porém não tão eficiente com o apresentado para o método baseado em ACs bidimensionais. Nas referências [Zambreno et al. 2004], [Zambreno et al. 2005] e [Good e Benaissa 2005], são apresentadas soluções para extrair o paralelismo para o método criptográfico do AES, utilizando-se placas FPGA (*Field Programmable Gate Array*). É importante destacar que AES não fornece uma implementação natural em uma arquitetura paralela e, portanto, o fator de paralelização obtido não é tão alto quanto o obtido pelo AC.

Capítulo 7

Sistema Criptográfico THCA (Two-Dimensional Hybrid Cellular Automata)

Neste capítulo será feita uma especificação completa do sistema criptográfico, fixando as configurações de entrada, tais como, possíveis tamanhos das imagens, tamanho do bloco no caso de cifragem de texto linear, quantidade de passos de pré-imagens, direção da sensitividade, dentre outras. Os parâmetros que serão propostos são baseados nos experimentos realizados no capítulo anterior. Com essa especificação, são sugeridos os valores para os parâmetros que seriam recomendáveis no estágio atual dos sistemas criptográficos e do *hardware* disponível. Além disso, essa especificação torna possível a realização de uma criptoanálise pela comunidade pesquisadora, para assim, poder identificar uma possível fraqueza não prevista no método proposto.

7.1 Tamanho do Bloco

7.1.1 Aplicação em Imagens

A sugestão é aplicar o método utilizando a imagem em um único bloco, embora seja possível quebrar em blocos menores. Para os tamanhos de imagens investigados nesse trabalho, sugerimos um bloco no máximo de 4.194.384 bits (512 Kbytes) com uma lateral máxima de 2048 bits. Tamanhos superiores a esse, podem ser tratados com a quebra de blocos de 2048×2048, desde que o modo de operação seja adequado (CBC, CFB, OFB, CTR, etc).

7.1.2 Aplicação em Cifragem de Textos

Apesar dos testes terem sido realizados com imagens, pois esse era o foco do trabalho, o método proposto também pode ser utilizado para cifragem de textos. A sugestão para cifragem de textos, é utilizar blocos de 1024 bits, que serão tratados no método como matrizes de ordem 32×32.

7.2 Tamanho da Chave

Para as duas aplicações (imagens e texto) definimos a utilização de regras de ACs binários com vizinhança von Neumann de raio 2. Isso resulta em chaves de 256 bits (núcleo da regra) e um espaço de chaves de 2^{256}, sem considerar o descarte da regras com entropia do núcleo abaixo de 0,7.

Realizando uma análise no espaço de chaves para o raio 1, temos que 5.952 regras possuem entropia do núcleo abaixo de 0,7, o que corresponde à 9,08% do total de chaves disponíveis (65.536). É sabido que ao aumentar o raio, a quantidade de regras descartadas é reduzida. Logo, mesmo com o descarte de regras com entropia do núcleo inferior à 0,7 para o raio 2, o espaço de chaves (núcleos das regras) ainda é suficientemente grande para inviabilizar um ataque de força bruta. Por exemplo, suponha hipoteticamente que para realizar a cifragem de uma imagem qualquer dure apenas 1 milisegundo, desta forma para que o criptoanalista teste todas as chaves possíveis seriam necessários 1,22391E+65 anos.

7.3 Número de Pré-imagens

7.3.1 Cifragem de Imagens

• Aplicação em Cifragem de Imagens Quadradas em Preto e Branco

A especificação da quantidade de pré-imagens a ser utiliza na cifragem de imagens quadradas binarizadas é baseada na tabela 6.22 apresentada na seção 6.7. Porém, como não é possível realizar um teste exaustivo de chaves para confirmar esses valores, para uma maior segurança do método sugere-se uma adição de 5 passos de pré-imagens. A tabela 7.1 apresenta a quantidade de pré-imagens necessárias de acordo com a quantidade de bits da imagem quadrada a ser cifrada.

Número de bits	Quantidade pré-imagens
$\leq 2^{12}$	15
$\leq 2^{18}$	20
$\leq 2^{22}$	25

Tabela 7.1: Quantidade de pré-imagens a ser utilizada em imagens quadradas binarizadas

• Aplicação em Cifragem de Imagens Retangulares e Quadradas em Escala de 256 Cores (ou níveis de cinza)

As imagens retangulares e coloridas necessitam de um tratamento especial, pois como já foi observado, o método não possui a mesma eficiência apresentada em imagens quadradas. As tabelas 7.2 e 7.3 apresentam os números de pré-imagens necessárias de acordo com cada lado da imagem. Caso seja realizada uma implementação sequencial do método, para um melhor desempenho, é desejável escolher a sensitividade da regra que está relacionada com o eixo do maior lado da imagem, consequentemente será necessário utilizar um número menor de pré-imagens. Se for adotada uma implementação paralela, deverá ser utilizada uma regra sensível ao eixo do menor lado da imagem, logo será necessário um número maior de pré-imagens, contudo no ambiente paralelo, o tempo geral do método será diminuído pelo paralelismo entre as pré-imagens.

Maior lado (em bits)	Quantidade pré-imagens
$\leq 2^6$	15
$\leq 2^9$	20
$\leq 2^{11}$	25

Tabela 7.2: Quantidade de pré-imagens a ser utilizada em imagens retangulares (caso geral)

Menor lado (em bits)	Quantidade pré-imagens
$\leq 2^6$	15
$\leq 2^9$	20
$\leq 2^{11}$	25

Tabela 7.3: Quantidade de pré-imagens a ser utilizada em imagens retangulares não degeneradas

• Especificação Única da Quantidade de Pré-Imagens

Para simplificação do processo de especificação do número de pré-imagens (P), uma vez que, com a utilização de regras de raio 2, a diferença entre o menor e o maior P (quantidade de pré-imagens) especificados nas tabelas anteriores não é significativo, pode-se fixar um valor único de P. Assim, pode-se adotar o valor 25 para qualquer imagem que não ultrapasse uma altura de 2048 bits e tenha uma largura igual ou menor à altura. Apenas deve-se ter em mente que em muitos casos o tempo de cifragem será maior que o necessário, mas não mais que o dobro do tempo mínimo, uma vez que o menor valor de P utilizado é 15. Para imagens com o maior lado acima de 2048, a imagem deve ser quebrada em blocos de 2048×2048 bits e cifrada por 25 pré-imagens, aplicando um dos modos de operação adequados (CFB, CBC, OFB, etc).

7.3.2 Aplicação em Cifragem de Texto

Conforme já foi especificado na seção 7.1, quando utilizado o sistema criptográfico proposto neste trabalho para cifragem de blocos de texto lineares, deverão ser utilizados blocos de 1024 bits. Logo, de acordo com os testes realizados na seção 6.7 o número de pré-imagens que deverá ser utilizado será 15.

7.4 Escolha entre os modelos: Sensitividade Fixa × Rotação da Sensitividade

De acordo com os testes realizados no capítulo 6, ambos os métodos possuem bons resultados na cifragem. Entretanto no modelo com rotação da sensitividade as regras apresentam uma maior velocidade de propagação de perturbações, especialmente quando utilizadas regras com entropia do núcleo abaixo de 0,7. Porém, como já foi especificado, a regras que possuem núcleo com entropia abaixo de 0,7 deverão ser filtradas do espaço de chaves, logo podemos afirmar que os métodos têm desempenho similar.

Devido ao método com sensitividade fixa permitir um melhor paralelismo e ter maior simplicidade de implementação, este deverá ser considerado como o modelo de utilização para o sistema criptográfico.

7.5 Descrição do Sistema Criptográfico THCA

O sistema criptográfico THCA pode ser empregado para cifrar tanto imagens em um único bloco, quanto para cifrar blocos de textos lineares. O THCA realiza o processo de cifragem de acordo com o fluxograma da figura 7.1.

Considerando a direção de sensitividade norte ($D = 00$), o número de pré-imagens igual à 25, a chave k' correspondente ao núcleo inicial (K), I imagem a ser cifrada, m a quantidade de linhas, n a quantidade de colunas, temos os principais processos do fluxograma:

- Gerar Φ (regra principal, seção 2.4):

$$\Phi[i] = K[i], 1 \leq i \leq 256 \quad (7.1)$$

$$\Phi[i] = \overline{K}[i], 257 \leq i \leq 512 \quad (7.2)$$

- Gerar τ (regra de contorno):

$$\tau = \overline{\Phi}[0] \quad (7.3)$$

- Cálculo da borda de S:

⋆ Cálculo da primeiro linha, para $j = 1$ e $1 \leq i \leq n$

$$S[i][j] = \tau \bigoplus I[i-1 \; mod \; m][j] \tag{7.4}$$

⋆ Cálculo da última linha, para $j = m$ e $1 \leq i \leq n$

$$S[i][j] = \tau \bigoplus I[i-1 \; mod \; m][j] \tag{7.5}$$

⋆ Cálculo da primeira coluna, para $i = 1$ e $2 \leq j \leq m-2$

$$S[i][j] = \tau \bigoplus I[i-1 \; mod \; m][j] \tag{7.6}$$

⋆ Cálculo da última coluna, para $i = n$ e $2 \leq j \leq m-2$

$$S[i][j] = \tau \bigoplus I[i-1 \; mod \; m][j] \tag{7.7}$$

• Cálculo de uma linha interna i de S:

$$\begin{aligned} S[i][j] = \; & \Phi(S[i-1][j], \\ & S[i][j-2], \\ & S[i][j-1], \\ & S[i][j+1], \\ & S[i][j+2], \\ & S[i][j-2], \\ & S[i+1][j], \\ & S[i+2][j], \\ & I[i][j]) \\ para \quad & 3 \leq j \leq n-3 \end{aligned} \tag{7.8}$$

• Rotacionar matriz S:

$$\begin{aligned} I[i][j] \leftarrow \; & S[i-2 \; mod \; m][j-2 \; mod \; n] \\ para \quad & 1 \leq i \leq m \\ para \quad & 1 \leq j \leq n \end{aligned} \tag{7.9}$$

• Rotacionar núcleo:

$$\begin{aligned} K[i+1] = \; & K[i] \\ para \quad & 1 \leq i \leq 256 \end{aligned} \tag{7.10}$$

A descrição do método foi feita de forma sequencial. No caso de uma implementação paralela, algumas partes do fluxo podem ser paralelizadas, conforme descrito a seguir.

Cálculo da borda de S: pode ser realizada em apenas 1 ciclo de relógio, visto que todas as células da borda (primeira linha, última linha, primeira coluna, última coluna) podem ser calculadas de forma independente, pois só dependem do valor da matriz I.

Cálculo de uma linha interna de S: pode ser realizada em apenas 1 ciclo de relógio, visto que todas a células de uma linha só dependem dos valores das células da mesma linha na matriz I e das últimas duas linhas calculadas em S.

Cálculo de pré-imagens consecutivas: embora o fluxograma da figura 7.1 apresente que o cálculo de uma nova pré-imagem (novo P), só possa ser iniciado após a conclusão da última linha interna da pré-imagem corrente, uma nova pré-imagem pode ser iniciada sempre que duas linhas da pré-imagem corrente já tiverem sido calculadas ($i = 5$).

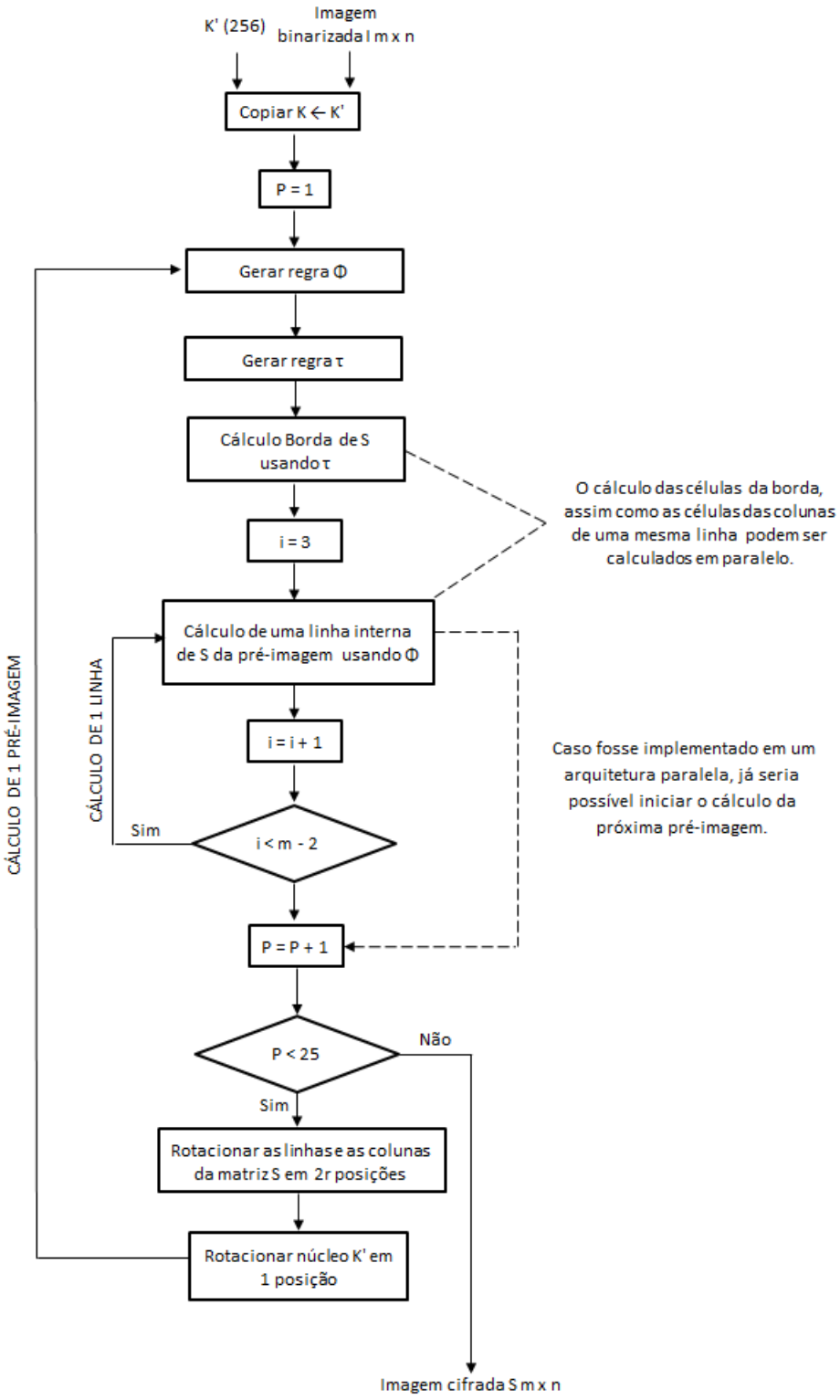


Figura 7.1: Fluxograma da cifragem do método T-HCA

7.6 Comparação com o Modelo da Patente PI0703188-2

Em [Oliveira e Macedo 2007] foi proposto o sistema HCA (unidimensional) para a cifragem de blocos lineares de 128 bits utilizando-se uma chave de 256 bits e 128 passos de pré-imagem. Para o sistema THCA (bidimensional) a chave também possui 256 bits, são utilizados blocos lineares de 1024 bits e 15 passos de pré-imagens.

Em uma arquitetura sequencial, considerando que o cálculo de uma única célula gaste 1 ciclo de relógio de processamento, o número de ciclos de relógio gastos para cifragem de um bloco, utilizando-se o sistema HCA é dado por $128 \times 128 = 16384$. Para o sistema THCA o número de ciclos de relógio para cifragem de um bloco é $1024 \times 15 = 15360$. Logo, é possível constatar que o *throughput* do sistema THCA é bem maior que o do HCA, uma vez que o THCA cifra uma quantidade de bits oito vezes superior ao HCA.

A equação (7.11) apresenta o número de ciclos de relógio necessário para a cifragem de um bloco para o HCA, enquanto que a equação (7.12) demonstra a quantidade de ciclos de relógio para o THCA, utilizando-se uma arquitetura paralela. Semelhante ao ocorrido em uma implementação sequencial, o *throughput* para o THCA é superior ao HCA, da ordem de seis vezes mais rápido para cifrar um bloco oito vezes maior.

$$\begin{aligned} NC_{hca} &= (N - 2r + 1) + [2 \times (P - 1)] \\ &= (128 - 2 \times 2 + 1) + [2 \times (128 - 1)] \\ &= 379 \end{aligned} \tag{7.11}$$

$$\begin{aligned} NC_{thca} &= 2P + m - 2r + 1 \\ &= 2 \times 15 + 32 - 2 \times 2 + 1 \\ &= 59 \end{aligned} \tag{7.12}$$

Capítulo 8

Conclusão e Trabalhos Futuros

Essa dissertação investigou um novo modelo criptográfico baseado em autômatos celulares bidimensionais heterogêneos e não-aditivos. Esse modelo se enquadra na classe dos métodos que utilizam o cálculo da pré-imagem (evolução para trás) na etapa de cifragem. O AC utiliza duas regras com vizinhança von Neumann na evolução temporal de suas células: uma chamada de regra principal, responsável por prover a caoticidade necessária à dinâmica, e outra chamada de regra de contorno, uma regra de dinâmica simples que efetua um deslocamento espacial no reticulado e é responsável por garantir que sempre exista uma pré-imagem de qualquer reticulado. Tanto a regra principal como a regra de contorno são sensíveis a uma das células nos extremos da vizinhança (ao norte, ao sul, à leste ou à oeste). Esse tipo de heterogeneidade já havia sido aplicada anteriormente no modelo criptográfico baseado em ACs investigado em [de Macedo 2007] e posteriormente registrado no INPI como solicitação de patente (PI0703188-2) [Oliveira e Macedo 2007]. Entretanto, nesse modelo prévio utilizado como base para o discutido na presente dissertação, os ACs utilizados são unidimensionais.

A principal motivação para se estudar um modelo baseado em uma estrutura bidimensional foi sua aplicabilidade na cifragem de imagens. A maioria dos métodos para cifragem de imagens pesquisados na literatura se baseia na aplicação de modelos convencionais para a cifragem de blocos de textos lineares, que são aplicados em uma versão linearizada da imagem. Dessa forma, perde-se a informação espacial da imagem, ou seja, a distribuição dos pixels nas duas dimensões. Qualquer que seja o modelo linear aplicado para cifrar os blocos, esse só será capaz de propagar a entropia em uma dimensão. Dessa forma, a eficácia do método fica atrelada ao modo de operação investigado, herdando suas vantagens e desvantagens. Por outro lado, a aplicação de um método que efetivamente propague a entropia em duas dimensões permite uma cifragem de maior qualidade na qual a imagem pode ser cifrada em um único bloco bidimensional.

A utilização de autômatos celulares em criptografia tem sido investigada por diversos pesquisadores [Wolfram 1986], [Kari 1992], [Nandi et al. 1994]; [Gutowitz 1995], [Tomassini e Perrenoud 2000], [Sen et al. 2002], [Guan e Tan 2003], [Oliveira et al.

2004], [Hameed e Eldin 2007] ; [Oliveira e Macedo 2007], [Seredynski et al. 2003], [Benkiniouar e Benmohamed 2004], [Oliveira et al. 2008], [Oliveira et al. 2010c], desde a proposição do primeiro método desse tipo por Wolfram (1986). A principal motivação para o estudo dessas estruturas na criptografia reside no fato das mesmas serem estruturas naturalmente paralelas e adequadas à implementação em *hardwares* com paralelização massiva. De fato, embora tenha sido implementado e testado de forma sequencial, foi possível mostrar que o modelo investigado na presente dissertação tem um forte potencial para implementação em uma plataforma paralela.

Embora a motivação original do estudo do método de criptografia bidimensional tenha sido sua aplicação em imagens, a sua aplicabilidade em cifragem de textos lineares também foi constatada. Nesse tipo de aplicação, o texto linear deve ser estruturado em matrizes binárias, resultando em blocos de 1024 bits. Dessa forma, o modelo mostrou ter um *throughput* maior que o modelo unidimensional no qual se baseia [Oliveira e Macedo 2007], tendo aproximadamente o mesmo tempo de processamento que o modelo anterior gasta para cifrar um bloco de 128 bits, na cifragem de um bloco de 1024 bits, quando a implementação é realizada em uma plataforma essencialmente sequencial. Essa diferença deve-se principalmente ao fato da difusão em dados acondicionados em duas dimensões ser muito mais rápida que a difusão quando eles são mantidos lineares. No caso de uma implementação paralela, tanto o método unidimensional quanto o bidimensional apresentam um bom potencial de paralelização, mas verificamos que o aumento do *throughput* no caso bidimensional é da ordem de 6 vezes maior.

Na comparação com o tempo de processamento em uma implementação sequencial do método mais convencional AES [National Institute of Standards and Technology 2001], o modelo baseado em ACs mostrou ter um tempo de processamento da mesma ordem de grandeza, até o tamanho investigado de 512×512 bits. Por outro lado, o método baseado em ACs tem um potencial muito maior para a paralelização e, teoricamente, deve retornar um *throughput* de uma ordem bem maior no caso de uma implementação em plataforma totalmente paralela.

Os testes realizados com o modelo mostraram que o mesmo possui as propriedades de confusão e difusão necessárias a um bom método criptográfico, além de ser robusto a ataques do tipo criptoanálise diferencial. A partir desses testes, o sistema criptográfico THCA (*Two-dimensional Hybrid Cellular Automata*) foi elaborado com chaves de 256 bits (regras de raio 2), tendo como principais características:

- Aplicado à cifragem de imagens: pode ser aplicado a uma imagem em um único bloco, desde que seu tamanho não supere 2048 bits na sua maior dimensão. Nesse caso, o número de pré-imagens a ser aplicado varia de 15 a 25, dependendo da dimensão da imagem (tabela 7.2) e a sensitividade deve ser escolhida no mesmo eixo da maior dimensão da imagem (no caso de matrizes binárias retangulares). No caso da imagem ser maior que 512 Kbytes ou ter pelo menos um lado maior que

2048 bits, a imagem deve ser quebrada em blocos de 2048×2048 bits e ser cifrada em 25 passos de pré-imagem, aplicando-se um modo de operação que não permita zonas de textura (p.e., CBC).

- Aplicado em cifragem de textos lineares: utilizando blocos bidimensionais de 1024 bits estruturados em matrizes de 32×32 bits com 20 passos de pré-imagem, aplicando-se um modo de operação seguro (p.e., CBC).
- Uma parte do espaço de chaves (2^{256}) deve ser descartado devido ao seu risco potencial de gerar cifragens de baixa qualidade. Para verificar a necessidade de descarte, basta realizar um cálculo de entropia sobre a chave de 256 bits (equação 6.3) e caso esse cálculo retorne um valor abaixo de 0,7, a chave deve ser descartada. Esse procedimento reduz o espaço em menos de 10%, pois mais de 90% das palavras binárias de 256 bits possuem entropia acima de 0,7.

Após elaborado, refinado e testado, o sistema criptográfico resultante pode ser descrito simplesmente por uma sequência de operações e funções binárias, em escalares, vetores e matrizes, como apresentado no fluxograma da figura 7.1. Descrito dessa forma, o sistema THCA pode até mesmo abstrair o modelo de autômato celular no qual o mesmo foi concebido. Entretanto, deve-se ter em mente que os estudos em autômatos celulares, tais como a dinâmica das regras, o cálculo de pré-imagens e o estudo de parâmetros dinâmicos (como a entropia do núcleo da regra), permitiu que fosse elaborado um modelo que atendesse às propriedades de difusão e confusão, necessários a qualquer método criptográfico, além de manter a natureza paralelizável dos ACs.

A partir da definição do sistema THCA e dos testes realizados nessa dissertação uma adicional da patente PI0703188-2 [Oliveira e Macedo 2007] está sendo elaborada e deve ser registrada no INPI em 2011.

Como continuidade dessa dissertação, várias investigações e desenvolvimentos podem ser conduzidas tanto com o objetivo de aperfeiçoá-lo, quanto de propor extensões do mesmo. A seguir apresentamos algumas idéias que surgiram durante o desenvolvimento da dissertação:

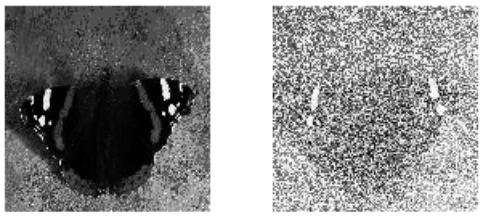
- Realizar testes com imagens de dimensão lateral maior que 2048 bits para definir o número de pré-imagens necessárias, de tal forma que não seja preciso quebrá-las em blocos menores. Nesses testes, podem ser utilizadas apenas regras de raio 2 que apresentam um crescimento menor com o aumento da largura, comparado às regras de raio 1. Por exemplo, poderiam ser avaliadas imagens de 4096×4096, 8192×8192, 16384×16384, 32768×32768, 65536×65536, atingindo imagens de até 512 Gbytes.
- Realizar testes sobre a geometria da imagem com o modelo que rotaciona a sensitividade como os que foram realizados com o modelo de sensitividade fixa na seção 6.7.4. Acreditamos que, nesse caso, a difusão será mais robusta à geometria, permitindo a utilização do menor lado da imagem como referência para a escolha do

número de pré-imagens a ser utilizado. Se confirmado, o modelo com rotação teria maior aplicabilidade no caso da implementação sequencial.

- Analisar uma terceira variação do modelo, que utilizasse a alteração da sensitividade apenas em dois extremos (de eixos diferentes), por exemplo, norte e oeste. Acreditamos que esse modelo manteria as vantagens do modelo com rotação da sensitividade (maior velocidade de difusão, menor número de pré-imagens, maior robustez à geometria) e permitiria extrair um modelo de paralelismo maior do que esse modelo (embora num nível menor que o da sensitividade fixa).
- Realizar testes com imagens coloridas em padrão RGB e HSI. Embora pudesse ser realizado um esquema similar ao que foi proposto para as imagens em escala de 256 cores ou níveis de cinza, como o fator de amplificação da dimensão da matriz binária é maior nesses padrões, seria interessante investigá-los com maior detalhamento. Nesses padrões, a composição dos pixels em 24 bits pode ser feita de diferentes formas para gerar a matriz binária: 24×1, 12×2, 8×3, 6×4, 4×6, 3×8, 2×12 e 1×24. Seria interessante investigar, por exemplo, se a composição 3×8 resultaria em uma geometria que também não comprometesse o desempenho do algoritmo em relação às matrizes quadradas e se o valor de P poderia ser associado à menor dimensão sem diminuir a qualidade da cifragem.
- Investigar modelos de ACs de maior dimensão (acima de 2) para lidar com as imagens coloridas. Uma possibilidade para decomposição dos pixels de uma imagem $m \times n$ de 256 cores, por exemplo, em uma matriz binária, seria a utilização de 8 matrizes $m \times n$, cifrando cada uma em separado e recompondo as 8 matrizes cifradas para gerar uma nova imagem $m \times n$. Nessa possível abordagem, cada matriz é tratada como um bloco e depois os blocos devem ser recombinados. Entretanto, essa abordagem sofre a mesma dependência do modo de operação de blocos, podendo gerar zonas de texturas. A figura 8.1 apresenta uma figura cifrada utilizando-se essa abordagem e a simples concatenação das matrizes cifradas para recomposição da imagem (similar ao modo de operação ECB). É possível perceber claramente as zonas de textura. Por outro lado, a utilização de uma única matriz bidimensional como a abordagem apresentada nessa dissertação acarreta um aumento da dimensão da matriz binária em oito vezes, aumentando o número de passos necessários e degradando o desempenho do mesmo. Se o padrão utilizado fosse o RGB, por exemplo, a dimensão seria aumentada em 24 vezes. Assim, propomos que uma melhor abordagem para tratar as imagens coloridas em 256 níveis seria a utilização de um AC 3D que fosse capaz de propagar perturbações não só em relação ao plano da imagem, mas também na dimensão dos bits do pixel. Acreditamos que um esquema similar aos modelos unidimensional (HCA) e bidimensional (THCA) pode ser elaborado, obtendo-se um paralelismo ainda mais forte. Nesse caso, uma imagem

colorida $m \times n$ seria representada por uma matriz 3D binária de dimensão $m \times n \times 8$, sendo que cada pré-imagem seria um cubo que poderia ser parcialmente paralelizado em relação à pré-imagem anterior. De forma similar, para tratar padrões de maior dimensão, como o RGB, uma matriz 4D poderia ser utilizada para propagar perturbações também entre os diferentes canais de cores R, G e B. Uma imagem colorida em RGB de dimensão $m \times n$ seria representada por uma matriz 4D de dimensão $m \times n \times 8 \times 3$, sendo que cada pré-imagem também seria de dimensão 4, podendo ser cifrada com paralelismo em relação a sua pré-imagem anterior. Em ambos os casos - 3D e 4D - as regras escolhidas devem ter vizinhanças que reflitam as dimensões utilizadas e terem a característica de serem sensíveis aos bits dos extremos dessas vizinhanças n-dimensionais.

- Implementar efetivamente o método em uma arquitetura paralela, para assim descobrir o *throughput* real do método e compará-lo a outras propostas de paralelização de métodos criptográficos existentes na literatura. Pesquisas apontam que a utilização de placas FPGA [Donthi e Haggard 2003] seria muito interessante.



(a) Imagem original (b) Imagem cifrada

Figura 8.1: (a) Imagem original (b) Imagem cifrada com zonas de texturas

Referências Bibliográficas

[Anderson 2008] Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems (2nd edition)*.

[Benkiniouar e Benmohamed 2004] Benkiniouar, M. e Benmohamed, M. (2004). Cellular Automata for Cryptosystem. In *Proceedings of IEEE Conference Information and Communication Technologies: From Theory to Applications*, pp. 423–424.

[Blundo et al. 2000] Blundo, C., De Santis, A., e Naor, M. (2000). Visual cryptography for grey level images. *Inf. Process. Lett.*, 75(6):255–259.

[Chen et al. 2004] Chen, G., Mao, Y., e Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, 21(3):749–761.

[Chen e Lai 2007] Chen, R.-J. e Lai, J.-L. (2007). Image security system using recursive cellular automata substitution. *Pattern Recogn.*, 40(5):1621–1631.

[Conrad 2007] Conrad, E. (2007). Types of Cryptographic Attacks.

[de Macedo 2007] de Macedo, H. B. (2007). Um novo método criptográfico baseado no cálculo de pré-imagens de autômatos celulares caóticos, não-homogêneos e não-aditivos. Master's thesis, Universidade Federal de Uberlândia.

[de Oliveira 2003] de Oliveira, G. M. B. (2003). *Autômatos Celulares: aspectos dinâmicos e computacionais*, chapter 8, pp. 297–345. Sociedade Brasileira de Computação.

[de Oliveira et al. 2003] de Oliveira, G. M. B., A. R. Coelho, e L. H.A. Monteiro (2003). Criptografia Baseada em Autômatos Celulares com Sensitividade Bidirecional. *Anais do XXIII Congresso da Sociedade Brasileira de Computação (IV Encontro Nacional de Inteligência Artificial)*, 7:235–243.

[Donthi e Haggard 2003] Donthi, S. e Haggard, R. (2003). A survey of dynamically reconfigurable FPGA devices. In *Proceedings of the 35th Southeastern Symposium*, pp. 422 – 426.

[Encinas et al. 2002] Encinas, L. H., Rey, A. M. D., e Encinas, A. H. (2002). Encryption of Images with 2-dimensional Cellular Automata. *SCI/ISAS*.

[Ganguly et al. 2003] Ganguly, N., Sikdar, B. K., Deutsch, A., Canright, G., e Chaudhuri, P. P. (2003). A Survey on Cellular Automata. Technical report.

[Gardner 1970] Gardner, M. (1970). The fantastic combinations of John Conway's new solitaire game of life. In *Scientific American 223*.

[Good e Benaissa 2005] Good, T. e Benaissa, M. (2005). AES on FPGA from the Fastest to the Smallest. In *Cryptographic Hardware and Embedded Systems - CHES 2005, 7th International Workshop*, pp. 427–440. Springer.

[Guan e Tan 2003] Guan, S.-U. e Tan, S. (2003). Pseudorandom Number Generator - The Self Programmable Cellular Automata. In *Knowledge-Based Intelligent Information and Engineering Systems*, volume 2773 de *Lecture Notes in Computer Science*, pp. 1230–1235. Springer Berlin / Heidelberg. 10.1007/978-3-540-45224-9166.

[Gutowitz 1995] Gutowitz, H. (1995). Cryptography with Dynamical Systems. In Goles, E. e N. Boccara, K. A. P. (editores), *Cellular Automata and Cooperative Phenomena*.

[Hameed e Eldin 2007] Hameed, A. e Eldin, B. (2007). A cellular automata random number generator for cryptographic applications. In *International Conference Computer Engineering & Systems*, pp. 101–105. 10.1109/ICCES.2007.4447033.

[Harris 2007] Harris, S. (2007). *CISSP All-in-One Exam Guide*.

[Hou 2003] Hou, Y.-C. (2003). Visual cryptography for color images. *Pattern Recognition*, 36(7):1619–1629.

[J.C. Yen 2000] J.C. Yen, J. G. (2000). A new chaotic key based design for image encryption and decryption. *Proceedings of the IEEE International Symposium Circuits and Systems*, 4:49–52.

[Jun 2009] Jun, J. (2009). Image encryption method based on Elementary Cellular Automata. *Southeastcon, 2009. SOUTHEASTCON '09. IEEE*, pp. 345 – 349.

[Kari 1992] Kari, J. (1992). Cryptosystem based on reversible cellular automata. *Apud in (Seredynski, Bouvry and Zomaya, 2003)*.

[Machhout et al. 2009] Machhout, M., Zied, G., Medien, Z., e Tourki, R. (2009). Design of Reconfigurable Image Encryption Processor Using 2-D Cellular Automata Generator. *IJCSA*, 6(4):43–62.

[Maleki et al. 2008] Maleki, F., Mohades, A., Hashemi, S. M., e Shiri, M. E. (2008). An Image Encryption System by Cellular Automata with Memory. *Availability, Reliability and Security, International Conference on*, 0:1266–1271.

[Mao 2003] Mao, W. (2003). *Modern Cryptography: Theory and Practice*. Prentice Hall, New Jersey.

[Matsui 1994] Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology*, pp. 386–397.

[Mihir Bellare 2005] Mihir Bellare, P. R. (2005). Introduction to Modern Cryptopraphy.

[Mitchell 1996] Mitchell, M. (1996). Computation in Cellular Automata: A Selected Review. In Verlagsgesellschaft, W. V. (editor), *Nonstandard Computation*.

[Nandi et al. 1994] Nandi, S., Kar, B. K., e Chaudhuri, P. P. (1994). Theory and Applications of Cellular Automata in Cryptography. *IEEE Trans. Comput.*, 43(12):1346–1357.

[Natarajan 2002] Natarajan, R. (2002). Differential CryptAnalysis.

[National Institute of Standards and Technology 2001] National Institute of Standards and Technology (2001). *Advanced Encryption Standard (AES)*. U.S. Department of Commerce, Washington D.C.

[Oliveira et al. 2008] Oliveira, G., Macêdo, H., Branquinho, A., e Lima, M. (2008). A cryptographic model based on the pre-image computation of cellular automata. In Adamatzky et al, L. P. (editor), *Theory and Applications of Cellular Automata*, pp. 139–155.

[Oliveira et al. 2004] Oliveira, G. M. B., Coelho, A. R., e Monteiro, L. H. A. (2004). Cellular Automata Cryptographic Model Based on Bi-Directional Toggle Rules. *International Journal of Modern Physics C*, 15:1061–1068.

[Oliveira e Macedo 2007] Oliveira, G. M. B. e Macedo, H. (2007). *Sistema criptográfico baseado no cálculo de pré-imagem em autômatos celulares não-homogêneos, não-aditivos e com dinâmica caótica*. Patente registrada no INPI, PI0703188-2, Depósito em 4/7/2007.

[Oliveira et al. 2010a] Oliveira, G. M. B., Martins, L. G. A., Alt, L., e Ferreira, G. (2010a). A Cellular Automata-Based Cryptographic Model with a Variable-Length Ciphertext. *International Conference on Scientific Computing (CSC 2010)*, 1.

[Oliveira et al. 2010b] Oliveira, G. M. B., Martins, L. G. A., Alt, L., e Ferreira, G. (2010b). Exhaustive Evaluation of Radius 2 Toggle Rules for a Variable-Length Cellular Automata Cryptographic Model. *International Conference on Cellular Automata for Research and Industry*, 6350:1–10.

[Oliveira et al. 2010c] Oliveira, G. M. B., Martins, L. G. A., Alt, L., e Ferreira, G. (2010c). Secret Key Specification for a Variable-Length Cryptographic Cellular Automata-Based Model. *11th International Conference on Parallel Problem Solving From Nature (PPSN2010)*, 6239:1–10.

[RSA Laboratories 2000] RSA Laboratories (2000). RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1.

[Sen et al. 2002] Sen, S., Shaw, C., Chowdhuri, D., Ganguly, N., e Chaudhuri, P. (2002). Cellular Automata Based Cryptosystem (CAC). In Deng, R., Bao, F., Zhou, J., e Qing, S. (editores), *Information and Communications Security*, volume 2513 de *Lecture Notes in Computer Science*, pp. 303–314. Springer Berlin / Heidelberg. 10.1007/3-540-36159-626.

[Seredynski et al. 2003] Seredynski, F., Bouvry, P., e Zomaya, A. (2003). Secret key cryptography with cellular automata. In *Proc. of Workshop on Nature Inspired Distributed Computing (in IPDPS2003)*, pp. 149–155.

[Shannon 1948] Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423; 623–656.

[Socek et al. 2005] Socek, D., Li, S., Magliveras, S. S., e Furht, B. (2005). Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption.

[Stallings 2003] Stallings, W. (2003). *Cryptograph and Network Security: Principles and Practice*. Prentice Hall, New Jersey.

[Tomassini e Perrenoud 2000] Tomassini, M. e Perrenoud, M. (2000). Stream Ciphers with One and Two-Dimensional Cellular Automata. In *Proc . of Parallel Problem Solving from Nature VI*, pp. 1917:722–731. LNCS (Springer-Verlag).

[Wolfram 1984] Wolfram, S. (1984). Universality and Complexity in Cellular Automata. *Physica D*, 10:1–35.

[Wolfram 1986] Wolfram, S. (1986). Cryptography with cellular automata. In (Springer-Verlag), L. (editor), *Proceedings of International Cryptology Conference (Crypto'85)*, pp. 429–432.

[Wolfram 2002] Wolfram, S. (2002). *A New Kind of Science*. Wolfram Media Inc.

[Yu et al. 2008] Yu, L., Li, Y., e Xia, X. (2008). Image Encryption Algorithm Based on Self-Adaptive Symmetrical-Coupled Toggle Cellular Automata. In *CISP '08: Proceedings of the 2008 Congress on Image and Signal Processing, Vol. 3*, pp. 32–36, Washington, DC, USA. IEEE Computer Society.

[Zambreno et al. 2005] Zambreno, J., Honbo, D., e Choudhary, A. (2005). Exploiting Multi-Grained Parallelism in Reconfigurable SBC Architectures. In *Proceedings of the 13th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, pp. 333–334, Washington, DC, USA. IEEE Computer Society.

[Zambreno et al. 2004] Zambreno, J., Nguyen, D., e Choudhary, A. (2004). Exploring Area/Delay Tradeoffs in an AES FPGA Implementation. In Becker, J., Platzner, M., e Vernalde, S. (editores), *Field Programmable Logic and Application*, volume 3203 de *Lecture Notes in Computer Science*, pp. 575–585. Springer Berlin / Heidelberg. 10.1007/978-3-540-30117-259.

[Zeghid et al. 2007] Zeghid, M., Machhout, M., Khriji, L., Baganne, A., e Tourki, R. (2007). A Modified AES Based Algorithm for Image Encryption. *International Journal of Computer Science and Engineering*, 1(1):70–75.

Apêndice A

Conjunto dos 500 núcleos da regras utilizadas

Índice	Núcleo	Índice	Núcleo	Índice	Núcleo
1	0000000000000000	201	0101100110101110	200	0000010000110010
2	1111111111111111	202	0010111000001111	401	0111001011001001
3	1111111100000000	203	1110111011111110	402	1001010010101110
4	0000000011111111	204	1001010110101111	403	0001100111011011
5	1010101010101010	205	0010100011011101	404	1101000001110011
6	0101010101010101	206	0110110010011111	405	0100101001110001
7	1100110011001100	207	1110111110000010	406	1010110101110010
8	1110001110001100	208	1111011001011100	407	0010111110011111
9	1111000011110000	209	0001000100110100	408	1101001011111011
10	0110110011010111	210	0001011001001111	409	0001010110110010
11	1111010010010101	211	0100100100011100	410	1100111110011111
12	0011001011111000	212	0100000000001101	411	1110110011100000
13	0001001010011000	213	0110111000100110	412	1010101001111111
14	1100001010000111	214	0000000000010000	413	1110101100000010
15	1100101001101001	215	0000110010011000	414	1111000011111000
16	1111011011000110	216	0101011111011000	415	1000000101000101
17	1110111010111001	217	0000110101111010	416	1011011101100010
18	0110000110100010	218	0111001100101001	417	1001101011100101
19	1110001010100000	219	1011000101110011	418	0111001101000001
20	0110111110110011	220	0000000110010100	419	1101011111011110
21	1001010011011110	221	0001100010110101	420	1110010100100110
22	1100010010001110	222	0101100011011110	421	1110111001101010
23	0110101101001011	223	1011000001100101	422	1001111101110101
24	1011010100100110	224	1111011001100010	423	0010101001010111
25	1111101011101101	225	0100111100111000	424	1001011101010111
26	0011101100000101	226	1011010011111011	425	1110001111010000
27	0111100010001110	227	1101000101100101	426	1011110101100101
28	0001101010011110	228	0101010001010100	427	0010000000101010
29	1011101100101001	229	0110100011110110	428	0011000010100000
30	0010110101101000	230	0001111010000010	429	0001100011100110
31	0000101000011000	231	0010100011101010	430	1100011111110001
32	1011111111000001	232	1001011011111000	431	0001011001110011
33	1101001011110011	233	0011101110000001	432	0110101100011011
34	1110100100100011	234	1010100011101000	433	0101101010000010
35	0001100011110001	235	0101000111111101	434	1100001011100100
36	1111001010001111	236	1100000001110001	435	0100111011110010
37	0000101110010100	237	1111100110111001	436	0100000000111111
38	0010001000001110	238	1111101001110000	437	0110011010010001
39	0001001000101001	239	0010011101101010	438	0001010010001100
40	0101001010100011	240	0000111001100000	439	1011110000011001
41	1100011011010101	241	0000001111001011	440	1111011101010111
42	1011110000110110	242	0000101100110000	441	1101011111101111
43	1010010011101110	243	1011110011110111	442	0011101111100000
44	0111101101000111	244	0110110110001111	443	1011100100111101
45	1011110100011011	245	0101110111100011	444	0000110010001101
46	1011001101001100	246	1010111110101001	445	0101000010110110
47	0001000000111011	247	1011010101111010	446	0100001110100100
48	0100000011011111	248	0011101001001010	447	1110010101101010
49	0001111101100001	249	0110101010100111	448	0001110110111100
50	0001010001100110	250	0110100000100110	449	1110110001111110
51	1101000111111000	251	1100001011011011	450	0011001001010100
52	1101010111101111	252	1011100010110110	451	0011010010100111

53	0111110111111111	253	1011000001000011	452	0010000110111000
54	0011001000010010	254	0110101101110110	453	0100010001101010
55	1001001001001011	255	0111000001011100	454	0101101101100110
56	1111111001011000	256	1110110100000111	455	0100000100000000
57	1101000100100001	257	1000001100000011	456	0111101000010010
58	0110011010000010	258	0110111100000001	457	0011011010111101
59	0100111111110110	259	1000100100101101	458	1101010110010001
60	0000100010101000	260	1110101011110010	459	0010011001101101
61	1011111100101100	261	0000111000011110	460	0010011101011001
62	1101011101101111	262	0000111001001101	461	0010110010010110
63	1010001100000010	263	0001010110110010	462	0101101011011000
64	0001101011111110	264	1101011101111010	463	0110111010101011
65	1111100110101110	265	1001001110000011	464	0001110100001001
66	0010000000001101	266	1010110010101101	465	1011000010010001
67	1000011011111011	267	0000011110110101	466	0110101100011100
68	1110010111010101	268	1110110100001001	467	0101000001111000
69	0000110010000110	269	0111000001101000	468	1010100110100001
70	1011101101101111	270	0011110100101000	469	0011100111010100
71	1011100001111101	271	1110100110011101	470	0101011100000111
72	1101101110110000	272	0011011000010111	471	1111010101111001
73	1001110010101010	273	0111110101101010	472	1001010111011110
74	1100011110110101	274	1110100110101101	473	1111111110001101
75	0011100011101010	275	0011100011001101	474	1101110001111100
76	1111001010000000	276	1000001111101101	475	1001110110010110
77	1011110010101000	277	0110111100100101	476	1000001001000000
78	1010010010010110	278	1101000111010000	477	0101001011000001
79	0110011100110010	279	1011110010001100	478	0101001101101100
80	0001011101010110	280	1000000011000110	479	1110100110000010
81	0110110010011100	281	1010000101101010	480	0100000011110000
82	1110100101010111	282	0000011111101100	481	1101111110110011
83	0000001011001101	283	1110011110100110	482	1010001101011101
84	0001110111100100	284	1011101011101010	483	1110101011000100
85	1101011100111100	285	1101010000011111	484	0010011110001000
86	1001001101010000	286	1110101011001101	485	1010000010000010
87	1111011100001101	287	0110111000110110	486	1111100001100010
88	1100000000101110	288	1010100000101100	487	0111010100111110
89	1011111100111000	289	1011010110000011	488	1101110000010011
90	1010010010111000	290	1000111101111101	489	1101110000110000
91	1100101001101101	291	0011010100001010	490	1100001001110000
92	0001001001000010	292	1010011111011101	491	1001110000100000
93	0110011010110101	293	0011100111001000	492	1110011100101111
94	1101100010111110	294	1000111011101101	493	0011101111100010
95	1000011101001111	295	1100010011001010	494	1010000000100110
96	0101111000110001	296	1011100010111001	495	1010010000101011
97	0100110011111110	297	0111110010100001	496	1000010100101110
98	0100111011001011	298	0001010111000000	497	1100001110001001
99	0111010110001111	299	1100000000101110	498	0100110110010001
100	1100010001011010	300	1111000010111010	499	1101010110011001
101	0011010110111111	301	0111101010101101	500	0101010110011001
102	0100001110101011	302	1111101011100010		
103	1101000110001110	303	1111100101101110		
104	0100110101110011	304	1001010000111101		
105	0011010101001001	305	0001011010110110		
106	0111011001101110	306	0101101111001100		
107	1001111010000000	307	0011111010011011		
108	1111001001010101	308	1101001011110010		
109	1111111111111100	309	0001110101000011		
110	0010011010110110	310	1011001111111111		
111	0111111001001000	311	1010010110100101		
112	1111110001000100	312	1111010000111001		
113	1100110110111000	313	0110101100001011		
114	0011011001110010	314	1001010000111110		
115	0000110001001100	315	1001001101100001		
116	0111001101011011	316	1001010111011001		
117	1010100011100100	317	0000011010010111		
118	1000110000001101	318	1000101111011100		
119	1101001011011001	319	0001001001111001		
120	0011101111001000	320	0011101001001011		
121	1111110101100110	321	1111101100011111		
122	0001100111001100	322	1111111111110110		
123	1111001111010000	323	1100101001100010		
124	0110011010110001	324	1011101010001001		
125	1010100000110111	325	0011011001001011		
126	1101010010101011	326	1010101110001101		
127	1100000110101001	327	0100110000100110		
128	1000010001011001	328	0001111110101011		
129	0111001001000001	329	1001010110001101		
130	1011100001100101	330	1110101100101101		
131	1100011101011001	331	1011010001101101		
132	1101000011111110	332	0011100001101001		

133	0000111101111010	333	0011011110001101		
134	1101110010101011	334	0101000001101001		
135	0111100100000100	335	0100001011001010		
136	0101111000101111	336	1111001000101110		
137	1110101000010110	337	1100000000000110		
138	0110100101001010	338	0010100100111111		
139	0000001101010100	339	1000000111010110		
140	1110111100000101	340	0101000111011000		
141	0001011000101010	341	1100001011111111		
142	1100111011011100	342	1000111011001001		
143	0110110000011010	343	1101000000001101		
144	1011101000111101	344	1110001100100100		
145	0010100110001011	345	0101001001000100		
146	1100111001110000	346	1101100111110010		
147	0010111101100101	347	1011101111010111		
148	0010111001010001	348	1101010101100000		
149	0111111110011111	349	1000000011000000		
150	0000100010110000	350	0111001010001110		
151	1100000001100111	351	0011001110111010		
152	1111100011001101	352	0000000010110110		
153	0100111010111011	353	0101011000011000		
154	1001011100111000	354	0000110110100010		
155	1100111111100010	355	1001010000011100		
156	1101000010001110	356	0010110010010111		
157	1111011111000010	357	1111001000011100		
158	1100111111110001	358	1000011111100111		
159	0000001100110000	359	1010110000111100		
160	1010110001110000	360	0110111010111011		
161	0000010011101011	361	0101010111000010		
162	0100101110110100	362	1111010001010001		
163	0000110000101101	363	1111010110111100		
164	0011110010110000	364	1111000001001000		
165	0110100011001011	365	1011011010010100		
166	0111011111100110	366	1101011101101010		
167	0010101011011011	367	0111001011111001		
168	1001010100110111	368	1110001110100000		
169	1011000010010001	369	1010000110001101		
170	0000110111010101	370	1011001110100010		
171	0101010101001001	371	0110011111000000		
172	1110110011111100	372	0101110101000011		
173	0111001101010110	373	0000101101111000		
174	0010001001111111	374	0001100101010111		
175	1110000110111011	375	0100000110111111		
176	0111111101110010	376	1110010100011100		
177	1101100000011100	377	0110011011101010		
178	0001000011101001	378	0000011001000001		
179	1110100111101111	379	0011110100111111		
180	0110001111011101	380	1101010100111111		
181	1100111110101111	381	1010010001011011		
182	1101001010110111	382	0011011010110101		
183	1100110001010110	383	1111111110111110		
184	1101011000100001	384	1111110111000000		
185	1101110011000101	385	0000101110000011		
186	0000110111011011	386	0000100111011111		
187	1000101011000001	387	0110111000111100		
188	1100000100000011	388	0100101000001100		
189	1011011010010111	389	1000001101111000		
190	0100110001101011	390	0000011101010000		
191	1101101100101100	391	1101110011011100		
192	1010111011001110	392	1011011101101111		
193	1110001110101001	393	0010011010010100		
194	0110011101100101	394	1100110110011110		
195	0010011100100111	395	1101000100101110		
196	0001100000110110	396	1011011100000000		
197	0111101111001111	397	1100011100011011		
198	1010000111101000	398	0111101100111111		
199	1100000011110101	399	0010100000110110		
200	1110110010001001	400	1001000000101111		

Apêndice B

Resultados dos testes da seção 6.3

Este apêndice possui os resultados obtidos dos testes realizados na seção 6.3. A tabela B.1 abaixo descreve as informação de cada uma das colunas das seções de resultados B.1 e B.2.

Coluna	Descrição da informação
A	Índice do núcleo da regra
B	Entropia do núcleo da regra
C	Entropia média da imagem da diferença)
D	Desvio padrão da entropia da imagem da diferença
E	Média do percentual de zeros da imagem da diferença
F	Desvio padrão do percentual de zeros da imagem da diferença
G	Entropia máxima da imagem da diferença
H	Entropia mínima da imagem da diferença
I	Percentual de zeros máximo da imagem da diferença
J	Percentual de zeros mínimo da imagem da diferença
K	Indica que regra apresentou alguma falha de segurança

Tabela B.1: Descrição das informações das colunas da tabela de resultado

B.1 Resultados dos testes com o modelo de sensitividade fixa

A	B	C	D	E	F	G	H	I	J	K
1	0,0000	0,0001	0,0000	99,9996	0,0000	0,0001	0,0001	99,9996	99,9996	Sim
2	0,0000	0,0001	0,0000	99,9996	0,0000	0,0001	0,0001	99,9996	99,9996	Sim
3	0,6372	0,9540	0,0001	49,9960	0,1008	0,9544	0,9537	50,3368	49,7147	Não
4	0,6372	0,9540	0,0001	50,0066	0,0945	0,9543	0,9537	50,2758	49,7105	Não
5	0,2500	0,0020	0,0000	99,9844	0,0000	0,0020	0,0020	99,9844	99,9844	Sim
6	0,2500	0,0020	0,0000	99,9844	0,0000	0,0020	0,0020	99,9844	99,9844	Sim
7	0,5000	0,5553	0,0000	74,9962	0,0000	0,5553	0,5553	74,9962	74,9962	Sim
8	0,7264	0,9540	0,0001	50,0055	0,1007	0,9544	0,9537	50,3490	49,6597	Não
9	0,7500	0,9540	0,0001	49,9983	0,0993	0,9543	0,9537	50,3746	49,6876	Não
10	0,7771	0,9540	0,0001	50,0020	0,0989	0,9543	0,9537	50,3025	49,7005	Não
11	0,8125	0,9540	0,0001	49,9966	0,0993	0,9544	0,9537	50,2926	49,7120	Não
12	0,9063	0,9540	0,0001	50,0008	0,0980	0,9544	0,9538	50,2911	49,6025	Não
13	0,8320	0,9540	0,0001	50,0019	0,0990	0,9544	0,9536	50,3330	49,7223	Não
14	0,8750	0,9540	0,0001	49,9972	0,0967	0,9544	0,9537	50,3490	49,7128	Não

15	0,8320	0,9540	0,0001	49,9988	0,0969	0,9544	0,9537	50,3059	49,7059	Não
16	0,7771	0,9540	0,0001	49,9972	0,1019	0,9544	0,9537	50,3307	49,6834	Não
17	0,7889	0,9540	0,0001	50,0036	0,0953	0,9544	0,9536	50,2975	49,7177	Não
18	0,8438	0,9540	0,0001	50,0012	0,0955	0,9543	0,9537	50,2781	49,6548	Não
19	0,8438	0,9540	0,0001	49,9975	0,0993	0,9544	0,9537	50,3288	49,7177	Não
20	0,7459	0,9540	0,0001	49,9957	0,0954	0,9544	0,9537	50,3132	49,6815	Não
21	0,8750	0,9540	0,0001	50,0052	0,0997	0,9544	0,9538	50,3078	49,7059	Não
22	0,8750	0,9540	0,0001	49,9985	0,0975	0,9544	0,9538	50,3162	49,6929	Não
23	0,7146	0,9540	0,0001	50,0042	0,1000	0,9544	0,9537	50,3628	49,6952	Não
24	0,7695	0,9540	0,0001	50,0020	0,0996	0,9544	0,9537	50,3071	49,6120	Não
25	0,7146	0,9540	0,0001	49,9969	0,0977	0,9544	0,9537	50,3796	49,6971	Não
26	0,9688	0,9540	0,0001	50,0027	0,0985	0,9544	0,9537	50,3006	49,6464	Não
27	0,8125	0,9540	0,0001	50,0015	0,0966	0,9544	0,9537	50,2861	49,6525	Não
28	0,9375	0,9540	0,0001	50,0003	0,0976	0,9544	0,9537	50,2827	49,6887	Não
29	0,8750	0,9540	0,0001	49,9999	0,0953	0,9544	0,9537	50,3120	49,7147	Não
30	0,8125	0,9540	0,0001	50,0034	0,0976	0,9544	0,9537	50,3017	49,6647	Não
31	0,7561	0,8506	0,1258	56,9326	7,6118	0,9543	0,4079	81,3660	49,7360	Sim
32	0,7873	0,9540	0,0001	50,0044	0,0981	0,9544	0,9537	50,3326	49,7402	Não
33	0,8750	0,9540	0,0001	50,0046	0,0938	0,9544	0,9537	50,3601	49,6616	Não
34	0,8320	0,9540	0,0001	49,9998	0,0967	0,9544	0,9537	50,3418	49,7242	Não
35	0,7889	0,9540	0,0001	49,9924	0,0967	0,9543	0,9538	50,3242	49,6693	Não
36	0,8186	0,9540	0,0001	50,0017	0,0965	0,9543	0,9537	50,3059	49,6876	Não
37	0,8632	0,9540	0,0001	49,9994	0,0950	0,9544	0,9537	50,3513	49,7429	Não
38	0,7577	0,9540	0,0001	49,9989	0,1001	0,9544	0,9538	50,2769	49,6296	Não
39	0,6563	0,9540	0,0001	50,0003	0,0951	0,9543	0,9536	50,3029	49,6979	Não
40	0,7695	0,9540	0,0001	49,9981	0,0972	0,9544	0,9537	50,3101	49,7158	Não
41	0,8438	0,9540	0,0001	50,0007	0,0978	0,9544	0,9537	50,2979	49,7284	Não
42	0,9063	0,9541	0,0001	49,9952	0,0975	0,9544	0,9537	50,2941	49,7036	Não
43	0,8125	0,9540	0,0001	49,9969	0,0980	0,9544	0,9537	50,3117	49,6700	Não
44	0,8320	0,9540	0,0001	50,0006	0,0987	0,9544	0,9537	50,3067	49,6284	Não
45	0,8320	0,9540	0,0001	49,9960	0,0957	0,9543	0,9536	50,3681	49,6922	Não
46	0,7889	0,9540	0,0001	50,0027	0,0962	0,9545	0,9537	50,3132	49,7128	Não
47	0,8632	0,9540	0,0001	50,0017	0,0971	0,9544	0,9537	50,3006	49,6098	Não
48	0,8632	0,9540	0,0001	50,0011	0,0987	0,9544	0,9536	50,3010	49,7177	Não
49	0,9063	0,9540	0,0001	49,9997	0,1000	0,9544	0,9536	50,3056	49,7013	Não
50	0,8438	0,9540	0,0001	49,9997	0,0940	0,9544	0,9537	50,3597	49,7402	Não
51	0,8320	0,9540	0,0001	49,9996	0,0982	0,9544	0,9536	50,3048	49,6265	Não
52	0,6875	0,8229	0,0664	58,7676	4,2040	0,9543	0,7204	65,0349	49,7726	Sim
53	0,5000	0,0585	0,0965	97,7739	4,2283	0,6303	0,0001	99,9992	71,8830	Sim
54	0,7577	0,9540	0,0001	50,0053	0,0977	0,9545	0,9537	50,3757	49,6937	Não
55	0,6757	0,9540	0,0001	50,0011	0,1002	0,9544	0,9537	50,3479	49,6758	Não
56	0,8438	0,9540	0,0001	50,0028	0,0945	0,9544	0,9537	50,3304	49,7059	Não
57	0,8320	0,9540	0,0001	50,0037	0,0957	0,9544	0,9537	50,3712	49,7448	Não
58	0,8438	0,9540	0,0001	50,0011	0,0974	0,9544	0,9537	50,3132	49,6998	Não
59	0,7873	0,9540	0,0001	49,9999	0,1023	0,9544	0,9537	50,3582	49,6555	Não
60	0,6875	0,5811	0,1973	72,0007	10,2658	0,9459	0,1372	94,1986	51,2096	Sim
61	0,7695	0,9540	0,0001	50,0039	0,0950	0,9544	0,9537	50,3731	49,7131	Não
62	0,7146	0,9540	0,0002	50,0036	0,0963	0,9544	0,9501	50,5333	49,7402	Sim
63	0,8007	0,9540	0,0001	49,9993	0,0962	0,9543	0,9537	50,3044	49,7330	Não
64	0,8750	0,9540	0,0001	49,9979	0,0965	0,9544	0,9537	50,3208	49,6540	Não
65	0,8438	0,9540	0,0001	49,9983	0,1010	0,9544	0,9537	50,2594	49,6593	Não
66	0,7264	0,9540	0,0002	50,0034	0,1028	0,9545	0,9505	50,8202	49,7147	Sim
67	0,8438	0,9540	0,0001	50,0045	0,0974	0,9544	0,9537	50,3071	49,6803	Não
68	0,8007	0,9540	0,0001	49,9958	0,0982	0,9544	0,9537	50,2777	49,7238	Não
69	0,7695	0,9540	0,0001	49,9955	0,1013	0,9544	0,9537	50,3113	49,6681	Não
70	0,6250	0,9540	0,0001	49,9956	0,1011	0,9544	0,9538	50,3365	49,6967	Não
71	0,8438	0,9540	0,0001	50,0025	0,0951	0,9544	0,9537	50,3166	49,6822	Não
72	0,7771	0,9540	0,0001	50,0049	0,0948	0,9544	0,9537	50,3494	49,7372	Não
73	0,7188	0,9540	0,0001	49,9961	0,0966	0,9544	0,9537	50,2720	49,6490	Não
74	0,8750	0,9540	0,0001	50,0026	0,0940	0,9543	0,9537	50,2674	49,7177	Não
75	0,8125	0,9540	0,0001	49,9984	0,0956	0,9544	0,9537	50,3277	49,6796	Não
76	0,8750	0,9540	0,0001	50,0020	0,0946	0,9543	0,9538	50,3727	49,7112	Não
77	0,8632	0,9540	0,0001	49,9981	0,1021	0,9544	0,9537	50,3273	49,6315	Não
78	0,7146	0,9540	0,0001	49,9952	0,0974	0,9544	0,9537	50,2907	49,6807	Não
79	0,6952	0,9540	0,0001	49,9977	0,0965	0,9544	0,9537	50,3483	49,6975	Não
80	0,8632	0,9540	0,0001	49,9970	0,0957	0,9543	0,9537	50,2518	49,6975	Não
81	0,8750	0,9540	0,0001	49,9959	0,0976	0,9544	0,9537	50,3048	49,7238	Não
82	0,7771	0,9540	0,0001	49,9959	0,0997	0,9543	0,9538	50,3723	49,6490	Não
83	0,8945	0,9540	0,0001	49,9981	0,0965	0,9543	0,9537	50,3170	49,6609	Não
84	0,9063	0,9540	0,0001	49,9991	0,0936	0,9544	0,9537	50,3105	49,7311	Não
85	0,8438	0,9540	0,0001	49,9988	0,0966	0,9544	0,9537	50,3044	49,6162	Não
86	0,8320	0,9540	0,0001	50,0035	0,0991	0,9544	0,9536	50,3376	49,6761	Não
87	0,8438	0,9540	0,0001	49,9915	0,0981	0,9544	0,9537	50,2872	49,7009	Não
88	0,7873	0,9540	0,0001	49,9963	0,0991	0,9543	0,9537	50,3162	49,6883	Não
89	0,8320	0,9540	0,0001	49,9973	0,0940	0,9544	0,9537	50,2728	49,7208	Não
90	0,8320	0,9540	0,0001	49,9966	0,0994	0,9544	0,9537	50,3551	49,7086	Não
91	0,8750	0,9540	0,0001	49,9998	0,0985	0,9544	0,9537	50,3567	49,6784	Não
92	0,6250	0,9540	0,0001	49,9987	0,0961	0,9544	0,9537	50,3975	49,7078	Não
93	0,7146	0,9540	0,0001	49,9972	0,0959	0,9544	0,9537	50,2674	49,7055	Não
94	0,8320	0,9540	0,0001	49,9956	0,0946	0,9544	0,9537	50,2892	49,6864	Não

95	0,8750	0,9540	0,0001	50,0093	0,0969	0,9544	0,9537	50,3262	49,6780	Não
96	0,8750	0,9540	0,0001	49,9989	0,0984	0,9543	0,9537	50,3170	49,7169	Não
97	0,7382	0,9540	0,0001	49,9953	0,0972	0,9544	0,9537	50,3242	49,6788	Não
98	0,8750	0,9540	0,0001	50,0053	0,0969	0,9544	0,9537	50,3010	49,7189	Não
99	0,8750	0,9540	0,0001	49,9991	0,0964	0,9544	0,9537	50,2941	49,6761	Não
100	0,8125	0,9540	0,0001	49,9979	0,1005	0,9544	0,9536	50,3166	49,6655	Não
101	0,8320	0,9540	0,0001	49,9966	0,0993	0,9543	0,9536	50,3288	49,6662	Não
102	0,8632	0,9540	0,0001	50,0037	0,0963	0,9544	0,9537	50,3017	49,7017	Não
103	0,8438	0,9540	0,0001	49,9990	0,0980	0,9544	0,9537	50,2842	49,6475	Não
104	0,8438	0,9540	0,0001	49,9998	0,0980	0,9544	0,9537	50,2785	49,7402	Não
105	0,7146	0,9540	0,0001	50,0012	0,0959	0,9544	0,9537	50,3674	49,6777	Não
106	0,7500	0,9540	0,0001	49,9970	0,0978	0,9544	0,9537	50,2651	49,7089	Não
107	0,8438	0,9540	0,0001	50,0016	0,1001	0,9544	0,9538	50,3086	49,7215	Não
108	0,8007	0,9540	0,0001	49,9958	0,0956	0,9543	0,9537	50,3258	49,6941	Não
109	0,4054	0,1771	0,1223	92,0359	6,0247	0,7690	0,0085	99,6880	61,3564	Sim
110	0,8632	0,9540	0,0001	49,9978	0,0988	0,9543	0,9538	50,3532	49,7051	Não
111	0,8320	0,9540	0,0001	50,0041	0,1012	0,9544	0,9537	50,2968	49,6368	Não
112	0,8007	0,9540	0,0001	50,0002	0,0940	0,9544	0,9536	50,2735	49,7082	Não
113	0,8007	0,9540	0,0001	49,9994	0,0944	0,9543	0,9537	50,2438	49,6559	Não
114	0,8750	0,9540	0,0001	49,9995	0,0953	0,9544	0,9537	50,3075	49,7166	Não
115	0,7695	0,9540	0,0001	49,9995	0,0916	0,9543	0,9537	50,3082	49,6685	Não
116	0,7771	0,9540	0,0001	49,9967	0,0992	0,9544	0,9537	50,2949	49,6838	Não
117	0,8438	0,9540	0,0001	49,9991	0,0968	0,9544	0,9537	50,3246	49,7181	Não
118	0,7264	0,9540	0,0001	50,0013	0,0981	0,9544	0,9537	50,3460	49,6834	Não
119	0,8750	0,9540	0,0001	49,9963	0,0966	0,9543	0,9537	50,3056	49,6883	Não
120	0,9063	0,9540	0,0001	50,0004	0,0985	0,9544	0,9537	50,3342	49,6948	Não
121	0,8320	0,9540	0,0001	49,9976	0,0976	0,9544	0,9537	50,2731	49,6792	Não
122	0,7577	0,9540	0,0001	49,9986	0,0975	0,9544	0,9537	50,3174	49,7036	Não
123	0,8750	0,9540	0,0001	50,0023	0,0946	0,9544	0,9538	50,3105	49,6964	Não
124	0,8320	0,9540	0,0001	50,0004	0,0965	0,9544	0,9536	50,3853	49,7093	Não
125	0,9063	0,9540	0,0001	50,0059	0,0931	0,9544	0,9537	50,2827	49,7116	Não
126	0,7500	0,9540	0,0001	50,0066	0,0982	0,9543	0,9537	50,3250	49,6166	Não
127	0,9063	0,9540	0,0001	49,9960	0,0944	0,9543	0,9537	50,2930	49,6700	Não
128	0,8438	0,9541	0,0001	49,9946	0,0986	0,9544	0,9537	50,4059	49,6758	Não
129	0,8320	0,9540	0,0001	49,9952	0,0963	0,9543	0,9537	50,2625	49,6407	Não
130	0,9063	0,9540	0,0001	49,9957	0,0962	0,9545	0,9537	50,2911	49,7028	Não
131	0,8750	0,9540	0,0001	49,9961	0,0962	0,9544	0,9537	50,3094	49,7437	Não
132	0,8438	0,9540	0,0001	50,0016	0,0983	0,9544	0,9537	50,3239	49,6849	Não
133	0,8438	0,9540	0,0001	50,0056	0,0984	0,9543	0,9537	50,3113	49,7211	Não
134	0,8007	0,9540	0,0001	49,9993	0,0911	0,9544	0,9537	50,2617	49,7089	Não
135	0,8438	0,9540	0,0001	49,9951	0,0977	0,9543	0,9537	50,3151	49,6498	Não
136	0,8438	0,9540	0,0001	49,9998	0,0959	0,9544	0,9537	50,3445	49,6376	Não
137	0,8750	0,9540	0,0001	50,0045	0,0947	0,9544	0,9537	50,3185	49,6609	Não
138	0,7146	0,9540	0,0001	50,0044	0,0955	0,9544	0,9537	50,3395	49,6445	Não
139	0,7131	0,9525	0,0059	50,2413	0,5806	0,9543	0,9011	54,3690	49,6624	Sim
140	0,8438	0,9540	0,0001	49,9982	0,0962	0,9544	0,9537	50,2930	49,6826	Não
141	0,8007	0,9540	0,0001	50,0021	0,0973	0,9544	0,9537	50,3418	49,6849	Não
142	0,7500	0,9540	0,0001	50,0041	0,0975	0,9544	0,9537	50,2823	49,6792	Não
143	0,8320	0,9540	0,0001	49,9998	0,0983	0,9544	0,9537	50,3891	49,7097	Não
144	0,8320	0,9540	0,0001	49,9986	0,0949	0,9545	0,9537	50,3075	49,6758	Não
145	0,8438	0,9540	0,0001	50,0017	0,0961	0,9544	0,9537	50,2808	49,6983	Não
146	0,7577	0,9540	0,0001	49,9989	0,0988	0,9544	0,9537	50,3613	49,6815	Não
147	0,8750	0,9540	0,0001	50,0033	0,0980	0,9543	0,9537	50,3014	49,6101	Não
148	0,8320	0,9540	0,0001	49,9999	0,0993	0,9543	0,9537	50,2895	49,6662	Não
149	0,6304	0,4142	0,2079	80,5586	10,7889	0,9540	0,1076	95,4796	50,1472	Sim
150	0,7248	0,9537	0,0020	50,0819	0,2827	0,9543	0,9206	53,4519	49,6349	Sim
151	0,7813	0,9540	0,0001	50,0016	0,0973	0,9544	0,9537	50,3185	49,6288	Não
152	0,8320	0,9540	0,0001	49,9973	0,1005	0,9544	0,9537	50,2872	49,6891	Não
153	0,8007	0,9540	0,0001	50,0001	0,0969	0,9543	0,9537	50,3014	49,7192	Não
154	0,8438	0,9540	0,0001	49,9978	0,0986	0,9544	0,9537	50,3140	49,7169	Não
155	0,8438	0,9540	0,0001	49,9965	0,0978	0,9544	0,9537	50,2850	49,6376	Não
156	0,8750	0,9540	0,0001	49,9940	0,0945	0,9544	0,9537	50,3017	49,7185	Não
157	0,8320	0,9540	0,0001	49,9995	0,0975	0,9544	0,9538	50,2827	49,7108	Não
158	0,6936	0,9540	0,0001	50,0011	0,1005	0,9543	0,9537	50,2941	49,6708	Não
159	0,5992	0,9437	0,0275	51,2872	2,0424	0,9544	0,5804	72,9893	49,8207	Sim
160	0,8750	0,9540	0,0001	49,9969	0,0978	0,9543	0,9537	50,3242	49,6792	Não
161	0,9688	0,9540	0,0001	49,9959	0,0974	0,9544	0,9537	50,3017	49,6540	Não
162	0,8750	0,9540	0,0001	50,0010	0,0992	0,9544	0,9537	50,2968	49,7181	Não
163	0,8750	0,9540	0,0001	50,0027	0,0964	0,9544	0,9537	50,3017	49,7051	Não
164	0,8945	0,9540	0,0001	50,0028	0,1019	0,9545	0,9537	50,3651	49,7013	Não
165	0,8632	0,9540	0,0001	50,0045	0,0984	0,9544	0,9537	50,2888	49,6944	Não
166	0,7695	0,9540	0,0001	50,0022	0,0965	0,9544	0,9537	50,3159	49,6616	Não
167	0,7146	0,9540	0,0001	50,0044	0,0951	0,9544	0,9537	50,3109	49,7250	Não
168	0,9063	0,9540	0,0001	49,9970	0,0953	0,9544	0,9537	50,2907	49,6918	Não
169	0,8438	0,9540	0,0001	50,0007	0,0974	0,9544	0,9537	50,3288	49,6979	Não
170	0,8632	0,9540	0,0001	49,9970	0,0995	0,9544	0,9537	50,2739	49,6735	Não
171	0,5434	0,9540	0,0001	50,0007	0,0989	0,9544	0,9537	50,3742	49,6292	Não
172	0,7695	0,9540	0,0001	50,0003	0,0991	0,9543	0,9537	50,2907	49,6040	Não
173	0,8125	0,9540	0,0001	49,9985	0,0998	0,9544	0,9537	50,3040	49,6445	Não
174	0,7813	0,9540	0,0001	50,0079	0,0972	0,9544	0,9537	50,3277	49,7501	Não

175	0,8438	0,9540	0,0001	49,9974	0,0967	0,9544	0,9537	50,3471	49,6906	Não
176	0,7813	0,9540	0,0001	49,9999	0,0927	0,9544	0,9537	50,2655	49,7269	Não
177	0,8320	0,9540	0,0001	50,0007	0,0946	0,9544	0,9537	50,3307	49,6983	Não
178	0,8320	0,9540	0,0001	49,9988	0,0948	0,9544	0,9536	50,2728	49,6887	Não
179	0,7248	0,7867	0,1249	61,1649	7,2947	0,9543	0,4774	78,1166	49,7890	Sim
180	0,8750	0,9540	0,0001	49,9966	0,0969	0,9544	0,9537	50,2758	49,6937	Não
181	0,7561	0,7923	0,1306	60,6254	7,6365	0,9543	0,4683	78,2669	49,7067	Sim
182	0,8438	0,9540	0,0001	50,0004	0,1014	0,9544	0,9537	50,2930	49,6967	Não
183	0,8320	0,9540	0,0001	50,0084	0,0969	0,9544	0,9537	50,3117	49,6941	Não
184	0,9375	0,9540	0,0001	50,0034	0,0988	0,9543	0,9537	50,3361	49,6876	Não
185	0,8750	0,9540	0,0001	50,0026	0,0987	0,9544	0,9537	50,2804	49,6822	Não
186	0,7771	0,9540	0,0001	49,9966	0,1012	0,9544	0,9537	50,3445	49,6796	Não
187	0,8125	0,9540	0,0001	50,0040	0,0974	0,9543	0,9537	50,2811	49,6979	Não
188	0,7561	0,9540	0,0001	49,9968	0,1003	0,9544	0,9537	50,3651	49,6517	Não
189	0,8202	0,9540	0,0001	50,0005	0,1004	0,9545	0,9538	50,3647	49,6941	Não
190	0,8320	0,9540	0,0001	49,9949	0,0994	0,9544	0,9538	50,2785	49,6685	Não
191	0,7070	0,9540	0,0001	50,0000	0,0970	0,9544	0,9537	50,3181	49,7089	Não
192	0,8125	0,9540	0,0001	49,9993	0,0958	0,9544	0,9537	50,3181	49,6845	Não
193	0,8750	0,9540	0,0001	49,9998	0,0978	0,9544	0,9537	50,3223	49,7128	Não
194	0,8438	0,9540	0,0001	50,0047	0,0997	0,9543	0,9536	50,2758	49,6559	Não
195	0,6875	0,9540	0,0001	49,9937	0,1008	0,9544	0,9537	50,3056	49,5956	Não
196	0,7264	0,9540	0,0001	50,0013	0,0946	0,9545	0,9536	50,3952	49,7105	Não
197	0,7146	0,9540	0,0001	50,0001	0,0955	0,9544	0,9537	50,3345	49,7005	Não
198	0,8750	0,9540	0,0001	50,0003	0,0986	0,9544	0,9537	50,3010	49,6754	Não
199	0,8632	0,9540	0,0001	50,0047	0,0988	0,9544	0,9537	50,3120	49,5995	Não
200	0,9063	0,9540	0,0001	50,0005	0,0968	0,9544	0,9537	50,3300	49,6811	Não
201	0,8438	0,9540	0,0001	49,9955	0,1013	0,9544	0,9537	50,3162	49,6246	Não
202	0,8750	0,9540	0,0001	50,0006	0,0974	0,9544	0,9537	50,3235	49,7017	Não
203	0,5778	0,1881	0,1346	92,3412	6,0328	0,8335	0,0001	99,9992	59,3807	Sim
204	0,8320	0,9540	0,0001	49,9983	0,0950	0,9543	0,9538	50,2750	49,6918	Não
205	0,9063	0,9540	0,0001	49,9996	0,0966	0,9544	0,9537	50,2663	49,7044	Não
206	0,8438	0,9540	0,0001	49,9969	0,1012	0,9545	0,9537	50,3090	49,6784	Não
207	0,8438	0,9540	0,0001	50,0028	0,0997	0,9544	0,9537	50,3017	49,6254	Não
208	0,8438	0,9540	0,0001	50,0008	0,0946	0,9544	0,9537	50,2518	49,6960	Não
209	0,8007	0,9540	0,0001	49,9958	0,0934	0,9543	0,9537	50,2663	49,6468	Não
210	0,9063	0,9540	0,0001	50,0030	0,0968	0,9544	0,9537	50,3254	49,6700	Não
211	0,7577	0,9540	0,0001	50,0033	0,0931	0,9545	0,9536	50,2750	49,6387	Não
212	0,6617	0,7584	0,0325	62,6572	1,8649	0,9475	0,6124	71,1945	50,8774	Sim
213	0,8750	0,9540	0,0001	49,9929	0,0983	0,9544	0,9537	50,3212	49,7101	Não
214	0,3278	0,0538	0,0676	97,5881	3,3330	0,4045	0,0007	99,9817	78,7045	Sim
215	0,7500	0,9540	0,0001	50,0000	0,0986	0,9544	0,9537	50,3124	49,6284	Não
216	0,9063	0,9540	0,0001	49,9962	0,0947	0,9544	0,9537	50,2998	49,6971	Não
217	0,9063	0,9540	0,0001	50,0028	0,0976	0,9544	0,9537	50,3555	49,7311	Não
218	0,8320	0,9540	0,0001	50,0011	0,0984	0,9544	0,9538	50,3262	49,7295	Não
219	0,8750	0,9540	0,0001	49,9999	0,0973	0,9544	0,9537	50,3010	49,6830	Não
220	0,7577	0,9516	0,0070	50,3719	0,7588	0,9544	0,8868	55,5981	49,6391	Sim
221	0,8438	0,9540	0,0001	49,9970	0,0977	0,9544	0,9537	50,3113	49,6784	Não
222	0,9063	0,9540	0,0001	49,9945	0,0953	0,9544	0,9537	50,3014	49,6887	Não
223	0,8320	0,9540	0,0001	49,9926	0,0960	0,9545	0,9537	50,2789	49,6765	Não
224	0,9063	0,9540	0,0001	50,0009	0,0995	0,9544	0,9537	50,3071	49,6223	Não
225	0,8438	0,9540	0,0001	49,9989	0,0984	0,9543	0,9537	50,3193	49,6410	Não
226	0,8007	0,9540	0,0001	50,0025	0,0948	0,9544	0,9537	50,3220	49,7147	Não
227	0,9063	0,9540	0,0001	49,9994	0,0974	0,9545	0,9537	50,2644	49,7169	Não
228	0,6250	0,6898	0,1175	66,4162	6,7592	0,9542	0,3833	82,2899	49,7879	Sim
229	0,9063	0,9540	0,0001	49,9948	0,0956	0,9543	0,9537	50,3490	49,7097	Não
230	0,8320	0,9540	0,0001	49,9998	0,0964	0,9543	0,9537	50,2789	49,7044	Não
231	0,8007	0,9540	0,0001	49,9984	0,0984	0,9544	0,9537	50,3117	49,6479	Não
232	0,9063	0,9540	0,0001	50,0001	0,0944	0,9544	0,9537	50,2720	49,6773	Não
233	0,8632	0,9540	0,0001	49,9993	0,0991	0,9544	0,9537	50,3414	49,7246	Não
234	0,8007	0,9540	0,0001	50,0039	0,0971	0,9544	0,9537	50,3460	49,7299	Não
235	0,7695	0,9533	0,0042	50,1299	0,4085	0,9544	0,8805	55,3947	49,6769	Sim
236	0,6875	0,9540	0,0001	49,9958	0,0986	0,9543	0,9536	50,3166	49,6799	Não
237	0,7695	0,9540	0,0001	50,0017	0,0963	0,9544	0,9537	50,3204	49,6323	Não
238	0,8750	0,9540	0,0001	49,9966	0,1005	0,9543	0,9537	50,3548	49,6181	Não
239	0,9063	0,9540	0,0001	50,0003	0,0956	0,9544	0,9537	50,2907	49,6571	Não
240	0,6952	0,9540	0,0001	50,0041	0,0952	0,9543	0,9537	50,3532	49,6124	Não
241	0,8945	0,9540	0,0001	49,9991	0,0984	0,9544	0,9537	50,2987	49,6643	Não
242	0,7561	0,9540	0,0001	49,9947	0,0989	0,9544	0,9537	50,2808	49,6677	Não
243	0,7146	0,9540	0,0001	49,9992	0,0918	0,9544	0,9537	50,2956	49,6590	Não
244	0,7771	0,9541	0,0001	50,0010	0,0990	0,9544	0,9537	50,2960	49,6628	Não
245	0,8750	0,9540	0,0001	49,9970	0,0984	0,9544	0,9538	50,2960	49,6876	Não
246	0,8320	0,9540	0,0001	50,0004	0,0967	0,9544	0,9537	50,2834	49,7368	Não
247	0,6875	0,9540	0,0001	50,0012	0,0962	0,9543	0,9537	50,3204	49,7215	Não
248	0,8320	0,9540	0,0001	50,0024	0,0985	0,9544	0,9537	50,3670	49,7074	Não
249	0,7695	0,9540	0,0001	50,0027	0,0953	0,9544	0,9537	50,3155	49,6754	Não
250	0,8438	0,9540	0,0001	50,0024	0,0969	0,9543	0,9537	50,2934	49,7059	Não
251	0,8632	0,9540	0,0001	50,0035	0,0996	0,9543	0,9537	50,3616	49,6208	Não
252	0,8320	0,9540	0,0001	49,9988	0,0990	0,9545	0,9536	50,2998	49,6719	Não
253	0,8632	0,9540	0,0001	49,9966	0,0985	0,9543	0,9537	50,2831	49,6830	Não
254	0,7771	0,9540	0,0001	50,0001	0,0975	0,9544	0,9537	50,3323	49,7200	Não

255	0,8125	0,9540	0,0001	49,9980	0,0962	0,9544	0,9537	50,3567	49,7067	Não
256	0,8632	0,9540	0,0001	49,9992	0,0995	0,9545	0,9537	50,3803	49,6887	Não
257	0,6936	0,9540	0,0001	50,0037	0,0978	0,9544	0,9537	50,3040	49,6902	Não
258	0,8438	0,9540	0,0001	50,0001	0,0982	0,9544	0,9537	50,3040	49,6246	Não
259	0,8007	0,9540	0,0001	50,0000	0,1017	0,9544	0,9537	50,3040	49,6029	Não
260	0,8007	0,9540	0,0001	49,9996	0,0957	0,9544	0,9537	50,4044	49,6624	Não
261	0,7382	0,9540	0,0001	49,9952	0,0972	0,9544	0,9537	50,2476	49,6933	Não
262	0,9063	0,9540	0,0001	50,0045	0,0984	0,9544	0,9536	50,3380	49,6765	Não
263	0,8750	0,9540	0,0001	49,9973	0,0941	0,9543	0,9537	50,2846	49,7223	Não
264	0,7264	0,9540	0,0001	50,0049	0,1009	0,9544	0,9537	50,3510	49,6391	Não
265	0,8125	0,9541	0,0001	50,0016	0,0940	0,9544	0,9537	50,3002	49,7356	Não
266	0,7146	0,9540	0,0001	49,9969	0,0999	0,9544	0,9537	50,3044	49,7025	Não
267	0,9063	0,9540	0,0001	49,9963	0,0982	0,9544	0,9537	50,3445	49,6307	Não
268	0,9375	0,9540	0,0001	49,9996	0,0966	0,9544	0,9537	50,2464	49,6510	Não
269	0,8320	0,9540	0,0001	49,9982	0,0976	0,9543	0,9537	50,3071	49,6464	Não
270	0,9063	0,9540	0,0001	50,0036	0,0983	0,9544	0,9536	50,2930	49,6574	Não
271	0,8438	0,9540	0,0001	50,0003	0,0968	0,9544	0,9537	50,2934	49,7204	Não
272	0,9063	0,9540	0,0001	49,9969	0,0988	0,9543	0,9537	50,2785	49,6464	Não
273	0,8320	0,9540	0,0001	49,9948	0,0990	0,9544	0,9538	50,3094	49,7192	Não
274	0,8320	0,9540	0,0001	50,0028	0,1002	0,9544	0,9537	50,3170	49,7017	Não
275	0,8320	0,9540	0,0001	49,9945	0,0981	0,9544	0,9537	50,3735	49,6689	Não
276	0,8438	0,9540	0,0001	50,0017	0,0982	0,9545	0,9537	50,3475	49,7272	Não
277	0,8750	0,9540	0,0001	49,9949	0,0944	0,9544	0,9538	50,4150	49,6956	Não
278	0,8125	0,9540	0,0001	50,0029	0,0980	0,9544	0,9537	50,3201	49,7078	Não
279	0,9063	0,9540	0,0001	50,0032	0,0983	0,9544	0,9537	50,2666	49,6269	Não
280	0,7500	0,9540	0,0001	50,0045	0,0971	0,9544	0,9537	50,3262	49,7120	Não
281	0,7500	0,9540	0,0001	49,9988	0,1003	0,9544	0,9537	50,3109	49,6811	Não
282	0,8007	0,9540	0,0001	49,9990	0,1018	0,9544	0,9537	50,3670	49,7013	Não
283	0,8438	0,9540	0,0001	50,0011	0,0968	0,9543	0,9537	50,2892	49,6128	Não
284	0,6250	0,9537	0,0008	50,6290	0,6641	0,9544	0,9481	53,6266	49,7898	Sim
285	0,8125	0,9540	0,0001	49,9947	0,0959	0,9544	0,9538	50,3639	49,7067	Não
286	0,8438	0,9540	0,0001	49,9962	0,1010	0,9544	0,9537	50,3757	49,6948	Não
287	0,8007	0,9540	0,0001	50,0003	0,0974	0,9544	0,9537	50,2811	49,6655	Não
288	0,8320	0,9540	0,0001	50,0007	0,1007	0,9543	0,9537	50,3494	49,7116	Não
289	0,8750	0,9540	0,0001	50,0012	0,0964	0,9544	0,9537	50,3792	49,7032	Não
290	0,8007	0,9540	0,0001	49,9977	0,0991	0,9544	0,9537	50,3017	49,6716	Não
291	0,8007	0,9540	0,0001	50,0014	0,0962	0,9544	0,9537	50,2998	49,6437	Não
292	0,8007	0,9540	0,0001	50,0063	0,0981	0,9543	0,9537	50,3784	49,7269	Não
293	0,8125	0,9540	0,0001	50,0021	0,1001	0,9544	0,9537	50,2979	49,7059	Não
294	0,7577	0,9540	0,0001	49,9991	0,0995	0,9544	0,9537	50,3250	49,6941	Não
295	0,8438	0,9540	0,0001	50,0010	0,0962	0,9544	0,9537	50,3086	49,6841	Não
296	0,8750	0,9540	0,0001	50,0021	0,0966	0,9544	0,9537	50,2823	49,7044	Não
297	0,9063	0,9540	0,0001	50,0028	0,0974	0,9543	0,9537	50,3376	49,6777	Não
298	0,7264	0,9062	0,0388	53,7595	2,6049	0,9542	0,7763	61,7107	49,7826	Sim
299	0,7873	0,9540	0,0001	49,9963	0,0991	0,9543	0,9537	50,3162	49,6883	Não
300	0,8750	0,9540	0,0001	50,0051	0,1000	0,9543	0,9537	50,3731	49,7337	Não
301	0,6875	0,9540	0,0001	49,9962	0,0987	0,9545	0,9537	50,2750	49,6826	Não
302	0,8438	0,9541	0,0001	49,9986	0,0997	0,9544	0,9537	50,3082	49,6918	Não
303	0,8007	0,9540	0,0001	50,0005	0,0974	0,9544	0,9537	50,3464	49,6944	Não
304	1,0000	0,9540	0,0001	50,0000	0,0941	0,9544	0,9537	50,3311	49,7017	Não
305	0,7889	0,9540	0,0001	49,9990	0,0949	0,9544	0,9538	50,2640	49,6624	Não
306	0,9063	0,9540	0,0001	50,0027	0,1021	0,9544	0,9537	50,2865	49,6559	Não
307	0,8438	0,9540	0,0001	49,9999	0,0986	0,9543	0,9537	50,2945	49,7124	Não
308	0,8750	0,9540	0,0001	49,9999	0,0982	0,9543	0,9537	50,3418	49,7166	Não
309	0,8750	0,9540	0,0001	50,0019	0,0989	0,9543	0,9537	50,3567	49,6284	Não
310	0,6250	0,5507	0,1602	74,0592	8,3378	0,9376	0,1130	95,5067	52,4162	Sim
311	0,7500	0,9540	0,0001	50,0070	0,0971	0,9543	0,9538	50,2995	49,6513	Não
312	0,8750	0,9540	0,0001	50,0013	0,0981	0,9544	0,9537	50,3010	49,6876	Não
313	0,7889	0,9540	0,0001	50,0012	0,0950	0,9544	0,9537	50,2735	49,6975	Não
314	0,9063	0,9540	0,0001	49,9989	0,0982	0,9543	0,9537	50,2792	49,7150	Não
315	0,8320	0,9540	0,0001	50,0001	0,1031	0,9544	0,9537	50,2983	49,6513	Não
316	0,8438	0,9540	0,0001	50,0001	0,0953	0,9544	0,9537	50,3445	49,6876	Não
317	0,9688	0,9540	0,0001	50,0038	0,0972	0,9544	0,9536	50,3086	49,6571	Não
318	0,8750	0,9540	0,0001	49,9973	0,0934	0,9544	0,9537	50,2605	49,6384	Não
319	0,7771	0,9540	0,0001	50,0025	0,1003	0,9544	0,9537	50,3246	49,7227	Não
320	0,8632	0,9540	0,0001	50,0024	0,0991	0,9543	0,9537	50,3372	49,6975	Não
321	0,6929	0,8615	0,0756	56,6433	4,5931	0,9542	0,5272	75,1419	49,8779	Sim
322	0,4917	0,2412	0,1224	89,1884	5,8751	0,8626	0,0154	99,4366	54,2442	Sim
323	0,8438	0,9540	0,0001	49,9976	0,0975	0,9544	0,9537	50,3033	49,6655	Não
324	0,9063	0,9541	0,0001	49,9988	0,0986	0,9543	0,9537	50,3189	49,6586	Não
325	0,7577	0,9540	0,0001	50,0030	0,0974	0,9544	0,9536	50,3490	49,6761	Não
326	0,8438	0,9540	0,0001	50,0085	0,0965	0,9544	0,9537	50,3021	49,6418	Não
327	0,7695	0,9540	0,0001	50,0075	0,0989	0,9544	0,9537	50,3250	49,6052	Não
328	0,8632	0,9540	0,0001	50,0030	0,0981	0,9544	0,9537	50,3105	49,7204	Não
329	0,8320	0,9540	0,0001	50,0002	0,0977	0,9544	0,9537	50,3799	49,7345	Não
330	0,8320	0,9540	0,0001	49,9976	0,0952	0,9543	0,9537	50,3284	49,6796	Não
331	0,6757	0,9540	0,0001	50,0070	0,1007	0,9544	0,9538	50,3574	49,6845	Não
332	0,9063	0,9540	0,0001	50,0003	0,0997	0,9544	0,9537	50,3513	49,5884	Não
333	0,9063	0,9540	0,0001	49,9973	0,0966	0,9543	0,9537	50,3197	49,6941	Não
334	0,8320	0,9540	0,0001	50,0005	0,0988	0,9544	0,9537	50,4192	49,6861	Não

335	0,8320	0,9540	0,0001	49,9959	0,0986	0,9544	0,9537	50,3094	49,7223	Não
336	0,8750	0,9540	0,0001	49,9918	0,0967	0,9544	0,9537	50,2529	49,6475	Não
337	0,5938	0,9210	0,0830	52,4386	5,3380	0,9544	0,5055	76,8547	49,7562	Sim
338	0,7889	0,9540	0,0001	49,9964	0,0994	0,9543	0,9537	50,3857	49,6677	Não
339	0,8632	0,9540	0,0001	50,0015	0,0984	0,9544	0,9536	50,2987	49,7341	Não
340	0,9375	0,9540	0,0001	49,9995	0,0965	0,9544	0,9537	50,3628	49,6704	Não
341	0,6929	0,9216	0,0358	52,6022	2,4951	0,9543	0,7999	60,1231	49,7799	Sim
342	0,8750	0,9540	0,0001	50,0017	0,0948	0,9544	0,9537	50,3120	49,7051	Não
343	0,7873	0,9540	0,0001	49,9979	0,0966	0,9544	0,9536	50,2651	49,7280	Não
344	0,8007	0,9540	0,0001	50,0037	0,0950	0,9544	0,9537	50,3529	49,6891	Não
345	0,6563	0,9540	0,0001	50,0010	0,1007	0,9543	0,9536	50,3174	49,7105	Não
346	0,8438	0,9540	0,0001	50,0003	0,0976	0,9543	0,9537	50,3242	49,6861	Não
347	0,6716	0,9540	0,0001	49,9998	0,0944	0,9543	0,9537	50,3086	49,6433	Não
348	0,7889	0,9540	0,0001	50,0013	0,0968	0,9544	0,9537	50,3037	49,6849	Não
349	0,6304	0,2309	0,1337	89,6875	6,4676	0,7975	0,0277	98,9578	60,6689	Sim
350	0,8438	0,9540	0,0001	49,9980	0,0958	0,9544	0,9537	50,3105	49,6910	Não
351	0,8750	0,9540	0,0001	49,9964	0,0959	0,9544	0,9537	50,3063	49,6716	Não
352	0,6952	0,9541	0,0001	49,9914	0,0965	0,9544	0,9538	50,2739	49,6761	Não
353	0,8125	0,9540	0,0001	50,0089	0,0987	0,9544	0,9537	50,3624	49,7032	Não
354	0,8125	0,9540	0,0001	49,9984	0,0964	0,9543	0,9536	50,2979	49,7082	Não
355	0,8750	0,9540	0,0001	50,0029	0,0999	0,9543	0,9537	50,3258	49,7105	Não
356	0,7577	0,9540	0,0001	50,0018	0,0988	0,9544	0,9537	50,4139	49,6338	Não
357	0,8438	0,9540	0,0001	49,9988	0,0972	0,9543	0,9537	50,2945	49,6220	Não
358	0,7500	0,9540	0,0001	50,0024	0,0992	0,9544	0,9537	50,3029	49,6319	Não
359	0,9375	0,9540	0,0001	49,9993	0,0984	0,9543	0,9537	50,2850	49,7131	Não
360	0,6563	0,9540	0,0001	50,0046	0,0951	0,9544	0,9537	50,3395	49,7108	Não
361	0,8632	0,9540	0,0001	49,9988	0,0971	0,9544	0,9536	50,3178	49,6449	Não
362	0,8438	0,9540	0,0001	49,9957	0,0969	0,9544	0,9537	50,2956	49,6563	Não
363	0,8438	0,9540	0,0001	49,9970	0,0970	0,9544	0,9537	50,3517	49,7082	Não
364	0,8438	0,9540	0,0001	49,9991	0,0951	0,9543	0,9537	50,3357	49,6914	Não
365	0,7500	0,9540	0,0001	49,9983	0,0967	0,9543	0,9537	50,2682	49,6803	Não
366	0,6716	0,9540	0,0001	50,0047	0,0985	0,9543	0,9537	50,3525	49,7097	Não
367	0,7500	0,9540	0,0001	50,0021	0,0948	0,9544	0,9537	50,3738	49,6780	Não
368	0,8125	0,9540	0,0001	49,9955	0,0995	0,9544	0,9537	50,3143	49,6422	Não
369	0,8007	0,9540	0,0001	50,0008	0,0957	0,9543	0,9537	50,3490	49,7414	Não
370	0,9375	0,9540	0,0001	49,9996	0,0992	0,9544	0,9537	50,2941	49,6517	Não
371	0,7813	0,9540	0,0001	49,9972	0,0959	0,9543	0,9537	50,2941	49,7242	Não
372	0,8632	0,9540	0,0001	50,0021	0,0992	0,9543	0,9537	50,4013	49,7093	Não
373	0,8438	0,9540	0,0001	49,9951	0,0968	0,9544	0,9537	50,2884	49,6540	Não
374	0,8632	0,9540	0,0001	49,9946	0,0956	0,9544	0,9537	50,3193	49,7189	Não
375	0,8632	0,9540	0,0001	50,0040	0,1016	0,9543	0,9537	50,3475	49,6841	Não
376	0,8438	0,9540	0,0001	50,0000	0,1026	0,9543	0,9537	50,2865	49,6738	Não
377	0,8438	0,9540	0,0001	50,0011	0,1002	0,9544	0,9537	50,3292	49,7147	Não
378	0,7500	0,9540	0,0001	50,0077	0,1002	0,9543	0,9537	50,3536	49,7223	Não
379	0,7500	0,9540	0,0001	49,9948	0,0990	0,9543	0,9538	50,2758	49,6876	Não
380	0,7131	0,9531	0,0050	50,1337	0,4661	0,9544	0,9023	54,3301	49,7044	Sim
381	0,8750	0,9540	0,0001	49,9959	0,0953	0,9544	0,9537	50,3052	49,6792	Não
382	0,7146	0,9540	0,0001	50,0000	0,0994	0,9543	0,9537	50,4028	49,6723	Não
383	0,5000	0,2438	0,1465	90,1538	6,3807	0,6881	0,0001	99,9992	66,7645	Sim
384	0,7889	0,9540	0,0001	50,0043	0,0975	0,9543	0,9536	50,3345	49,6960	Não
385	0,8320	0,9540	0,0001	49,9960	0,0961	0,9544	0,9537	50,3193	49,7025	Não
386	0,9063	0,9540	0,0001	49,9996	0,0982	0,9543	0,9537	50,3147	49,6635	Não
387	0,8125	0,9540	0,0001	49,9983	0,0990	0,9544	0,9537	50,3223	49,7154	Não
388	0,8438	0,9540	0,0001	49,9977	0,0930	0,9544	0,9536	50,2792	49,5949	Não
389	0,9063	0,9540	0,0001	50,0029	0,1006	0,9544	0,9537	50,3132	49,7166	Não
390	0,7264	0,8915	0,0381	54,6948	2,4717	0,9543	0,7879	60,7559	49,8245	Sim
391	0,7500	0,9540	0,0001	49,9997	0,0984	0,9544	0,9536	50,2800	49,7108	Não
392	0,6250	0,9540	0,0001	49,9950	0,0935	0,9544	0,9538	50,3448	49,7055	Não
393	0,8320	0,9540	0,0001	49,9996	0,0975	0,9544	0,9537	50,3082	49,6944	Não
394	0,7695	0,9540	0,0001	49,9964	0,0987	0,9544	0,9537	50,3155	49,6506	Não
395	0,8750	0,9540	0,0001	50,0027	0,1009	0,9543	0,9537	50,3269	49,6693	Não
396	0,7873	0,9540	0,0001	50,0038	0,0957	0,9544	0,9536	50,2876	49,5689	Não
397	0,8125	0,9540	0,0001	50,0022	0,0956	0,9543	0,9538	50,2846	49,6899	Não
398	0,7500	0,8504	0,0933	57,3347	5,7840	0,9544	0,5320	75,2708	49,7986	Sim
399	0,8750	0,9540	0,0001	49,9993	0,0960	0,9544	0,9537	50,3044	49,7074	Não
400	0,8632	0,9540	0,0001	49,9999	0,1012	0,9544	0,9537	50,2655	49,7139	Não
401	0,7500	0,9540	0,0001	50,0008	0,0966	0,9543	0,9537	50,3273	49,6975	Não
402	0,7577	0,9540	0,0001	50,0011	0,1016	0,9544	0,9536	50,3712	49,6960	Não
403	0,7577	0,9540	0,0001	49,9994	0,0954	0,9544	0,9537	50,3551	49,7215	Não
404	0,8007	0,9540	0,0001	50,0029	0,0988	0,9544	0,9537	50,3242	49,6563	Não
405	0,8750	0,9540	0,0001	49,9998	0,0978	0,9544	0,9537	50,3445	49,7013	Não
406	0,8438	0,9540	0,0001	49,9955	0,0999	0,9543	0,9537	50,3136	49,6647	Não
407	0,7695	0,9540	0,0001	50,0039	0,0972	0,9544	0,9537	50,2953	49,7185	Não
408	0,7500	0,9540	0,0001	50,0043	0,0962	0,9543	0,9537	50,2804	49,6449	Não
409	0,8007	0,9540	0,0001	50,0022	0,0948	0,9544	0,9537	50,3529	49,7269	Não
410	0,8750	0,9540	0,0001	49,9973	0,0941	0,9543	0,9537	50,2846	49,7223	Não
411	0,6014	0,8546	0,1068	56,8611	6,8152	0,9543	0,5526	74,3202	49,7471	Sim
412	0,8438	0,9540	0,0001	50,0003	0,0949	0,9544	0,9538	50,2705	49,7253	Não
413	0,7131	0,9529	0,0053	50,1464	0,4830	0,9543	0,8675	56,3309	49,7379	Sim
414	0,8632	0,9540	0,0001	49,9974	0,0944	0,9544	0,9538	50,2712	49,6952	Não

415	0,7382	0,9540	0,0001	50,0077	0,0983	0,9544	0,9537	50,3426	49,6735	Não
416	0,8007	0,9540	0,0001	49,9982	0,0966	0,9544	0,9537	50,2670	49,7211	Não
417	0,8320	0,9540	0,0001	49,9998	0,0968	0,9544	0,9537	50,2941	49,6468	Não
418	0,8438	0,9540	0,0001	49,9992	0,0964	0,9544	0,9537	50,2750	49,7192	Não
419	0,9688	0,9540	0,0001	49,9956	0,0934	0,9544	0,9537	50,2552	49,6830	Não
420	0,7146	0,9455	0,0302	50,8735	2,2266	0,9543	0,6678	67,9249	49,6983	Sim
421	0,8632	0,9540	0,0001	49,9994	0,0961	0,9543	0,9537	50,3063	49,7047	Não
422	0,8125	0,9540	0,0001	49,9963	0,0973	0,9544	0,9537	50,2811	49,6925	Não
423	0,8438	0,9540	0,0001	49,9982	0,0988	0,9544	0,9537	50,3899	49,6796	Não
424	0,7382	0,9540	0,0001	50,0038	0,0967	0,9544	0,9537	50,3574	49,6609	Não
425	0,8007	0,9540	0,0001	50,0036	0,0968	0,9545	0,9537	50,3105	49,6807	Não
426	0,8438	0,9540	0,0001	49,9976	0,0978	0,9544	0,9537	50,3086	49,6647	Não
427	0,8320	0,9540	0,0001	49,9963	0,0955	0,9543	0,9537	50,3345	49,6883	Não
428	0,6875	0,5719	0,1853	72,4229	9,6590	0,8914	0,1662	92,7937	54,9847	Sim
429	0,7561	0,8531	0,1110	57,2045	6,7737	0,9543	0,4962	77,2369	49,7890	Sim
430	0,7577	0,9540	0,0001	49,9973	0,0985	0,9544	0,9537	50,3517	49,6986	Não
431	0,6875	0,9540	0,0001	50,0015	0,0993	0,9544	0,9538	50,3292	49,6254	Não
432	0,8320	0,9540	0,0001	49,9970	0,0981	0,9544	0,9537	50,3265	49,6811	Não
433	0,7264	0,9541	0,0001	50,0011	0,0954	0,9544	0,9537	50,3407	49,6799	Não
434	0,8438	0,9540	0,0001	49,9982	0,0939	0,9544	0,9537	50,2918	49,7139	Não
435	0,9063	0,9540	0,0001	50,0020	0,0968	0,9544	0,9537	50,3017	49,6658	Não
436	0,8007	0,9540	0,0001	49,9988	0,0956	0,9543	0,9538	50,3277	49,6891	Não
437	0,7443	0,9540	0,0001	49,9945	0,0979	0,9544	0,9537	50,3250	49,7215	Não
438	0,8750	0,9540	0,0001	49,9995	0,0978	0,9543	0,9537	50,3265	49,6532	Não
439	0,8438	0,9540	0,0001	50,0002	0,0961	0,9543	0,9537	50,2853	49,6243	Não
440	0,8750	0,9540	0,0001	49,9987	0,0957	0,9544	0,9537	50,3380	49,7200	Não
441	0,6875	0,3397	0,2213	85,5993	11,3156	0,9539	0,0373	98,7698	50,5116	Sim
442	0,6327	0,4035	0,1551	81,3326	8,1225	0,9541	0,0977	96,0609	49,9725	Sim
443	0,7813	0,9540	0,0001	50,0034	0,0953	0,9544	0,9537	50,3231	49,6960	Não
444	0,8438	0,9540	0,0001	49,9937	0,0977	0,9544	0,9537	50,2869	49,7047	Não
445	0,8438	0,9541	0,0001	49,9995	0,0970	0,9543	0,9537	50,2773	49,7021	Não
446	0,8750	0,9540	0,0001	49,9951	0,0946	0,9543	0,9537	50,2647	49,6830	Não
447	0,8320	0,9540	0,0001	49,9987	0,0979	0,9544	0,9537	50,3357	49,6330	Não
448	0,7695	0,9540	0,0001	49,9984	0,0964	0,9544	0,9537	50,3494	49,7158	Não
449	0,8438	0,9540	0,0001	50,0044	0,0988	0,9543	0,9537	50,3204	49,6849	Não
450	0,8007	0,9540	0,0001	49,9992	0,0956	0,9543	0,9537	50,3166	49,7372	Não
451	0,8438	0,9540	0,0001	50,0010	0,0998	0,9544	0,9537	50,2953	49,6868	Não
452	0,8320	0,9540	0,0001	49,9964	0,1003	0,9543	0,9536	50,3063	49,6780	Não
453	0,8632	0,9540	0,0001	50,0000	0,0964	0,9544	0,9537	50,3326	49,5949	Não
454	0,8007	0,9540	0,0001	50,0015	0,0933	0,9544	0,9537	50,3613	49,7467	Não
455	0,7070	0,9540	0,0001	50,0041	0,0971	0,9543	0,9537	50,3265	49,7387	Não
456	0,5000	0,1469	0,1034	93,6170	4,8194	0,7372	0,0178	99,3279	64,5031	Sim
457	0,8632	0,9540	0,0001	49,9954	0,0937	0,9543	0,9537	50,2819	49,7005	Não
458	0,8320	0,9540	0,0001	50,0040	0,0987	0,9544	0,9537	50,3368	49,6784	Não
459	0,9375	0,9540	0,0001	49,9981	0,1013	0,9544	0,9537	50,3082	49,6536	Não
460	0,7577	0,9540	0,0001	50,0009	0,0990	0,9544	0,9537	50,2842	49,7169	Não
461	0,8632	0,9540	0,0001	49,9962	0,0966	0,9544	0,9537	50,3838	49,6719	Não
462	0,7695	0,9540	0,0001	50,0001	0,0961	0,9543	0,9537	50,3544	49,7467	Não
463	0,7889	0,9540	0,0001	49,9957	0,0915	0,9544	0,9537	50,2571	49,6490	Não
464	0,6716	0,9540	0,0001	49,9988	0,0959	0,9543	0,9537	50,2964	49,7070	Não
465	0,8320	0,9540	0,0001	49,9989	0,0999	0,9544	0,9537	50,3563	49,6376	Não
466	0,8438	0,9540	0,0001	50,0007	0,0974	0,9544	0,9537	50,3288	49,6979	Não
467	0,8438	0,9540	0,0001	50,0007	0,1020	0,9543	0,9536	50,3517	49,6887	Não
468	0,8632	0,9540	0,0001	50,0024	0,0992	0,9544	0,9537	50,3193	49,6494	Não
469	0,8007	0,9540	0,0001	49,9990	0,0965	0,9544	0,9537	50,2838	49,6693	Não
470	0,8750	0,9540	0,0001	49,9982	0,0967	0,9543	0,9537	50,3433	49,6910	Não
471	0,8438	0,9540	0,0001	50,0074	0,0994	0,9544	0,9537	50,2857	49,6914	Não
472	0,8007	0,9540	0,0001	49,9981	0,0950	0,9545	0,9536	50,2758	49,6964	Não
473	0,8125	0,9540	0,0001	49,9973	0,0936	0,9543	0,9538	50,3101	49,7223	Não
474	0,6929	0,9117	0,0699	53,2909	4,5891	0,9544	0,5507	74,3031	49,7753	Sim
475	0,8438	0,9540	0,0001	50,0043	0,0976	0,9544	0,9537	50,3475	49,6422	Não
476	0,8750	0,9540	0,0001	49,9989	0,0954	0,9544	0,9537	50,2853	49,6571	Não
477	0,6075	0,5414	0,1594	74,3660	8,4720	0,9540	0,2005	91,3235	49,9516	Sim
478	0,8320	0,9540	0,0001	49,9977	0,0986	0,9543	0,9537	50,3143	49,6822	Não
479	0,8632	0,9540	0,0001	50,0002	0,0943	0,9545	0,9537	50,2567	49,6849	Não
480	0,9688	0,9540	0,0001	49,9981	0,0935	0,9544	0,9537	50,3117	49,7089	Não
481	0,7561	0,9540	0,0001	50,0078	0,0968	0,9544	0,9538	50,2987	49,6700	Não
482	0,7500	0,9540	0,0002	50,0046	0,1105	0,9544	0,9491	51,4248	49,6738	Sim
483	0,8320	0,9540	0,0001	50,0033	0,0983	0,9544	0,9537	50,2987	49,7231	Não
484	0,9375	0,9540	0,0001	50,0037	0,0973	0,9544	0,9537	50,3105	49,7074	Não
485	0,8438	0,9540	0,0001	49,9976	0,0957	0,9544	0,9536	50,2769	49,6925	Não
486	0,6875	0,4901	0,1000	76,8336	5,3104	0,9539	0,2945	86,6032	49,9855	Sim
487	0,8750	0,9540	0,0001	50,0015	0,0920	0,9543	0,9537	50,3056	49,7097	Não
488	0,8125	0,9540	0,0001	49,9986	0,0991	0,9544	0,9537	50,3132	49,7047	Não
489	0,9063	0,9540	0,0001	49,9964	0,0990	0,9544	0,9537	50,2773	49,6918	Não
490	0,8125	0,9540	0,0001	50,0011	0,0959	0,9544	0,9537	50,3147	49,7047	Não
491	0,8438	0,9540	0,0001	50,0042	0,1001	0,9543	0,9537	50,3502	49,6944	Não
492	0,8007	0,9540	0,0001	49,9986	0,0970	0,9544	0,9537	50,3174	49,7040	Não
493	0,7500	0,9540	0,0001	50,0008	0,0952	0,9544	0,9537	50,2747	49,6716	Não
494	0,8438	0,9540	0,0001	49,9991	0,0981	0,9544	0,9537	50,3307	49,7375	Não

495	0,8125	0,9540	0,0001	50,0036	0,1009	0,9543	0,9537	50,2945	49,6910	Não
496	0,8750	0,9540	0,0001	50,0010	0,0955	0,9545	0,9537	50,3681	49,7242	Não
497	0,8750	0,9540	0,0001	49,9999	0,1001	0,9544	0,9537	50,3368	49,7181	Não
498	0,8125	0,9540	0,0001	50,0002	0,0945	0,9544	0,9537	50,3162	49,6761	Não
499	0,8750	0,9540	0,0001	50,0025	0,0977	0,9544	0,9537	50,3365	49,6918	Não
500	0,8125	0,9540	0,0001	50,0020	0,0978	0,9544	0,9537	50,2823	49,6761	Não

Tabela B.2: Resultados para o teste com o modelo de sensitividade fixa

B.2 Resultados do modelo com rotação da sensitividade

A	B	C	D	E	F	G	H	I	J	K
1	0,0000	0,0001	0,0000	99,9996	0,0000	0,0001	0,0001	99,9996	99,9996	Sim
2	0,0000	0,0001	0,0000	99,9996	0,0000	0,0001	0,0001	99,9996	99,9996	Sim
3	0,6372	0,9540	0,0001	49,9991	0,0966	0,9543	0,9536	50,3098	49,7284	Não
4	0,6372	0,9540	0,0001	49,9950	0,0979	0,9543	0,9537	50,3342	49,6777	Não
5	0,2500	0,3542	0,0000	87,0956	0,0000	0,3542	0,3542	87,0956	87,0956	Sim
6	0,2500	0,3542	0,0000	87,0956	0,0000	0,3542	0,3542	87,0956	87,0956	Sim
7	0,5000	0,5553	0,0000	74,9390	0,0000	0,5553	0,5553	74,9390	74,9390	Sim
8	0,7264	0,9540	0,0001	50,0008	0,0960	0,9544	0,9537	50,3414	49,6498	Não
9	0,7500	0,9540	0,0001	49,9997	0,1008	0,9544	0,9537	50,3899	49,6487	Não
10	0,7771	0,9540	0,0001	49,9999	0,0996	0,9544	0,9538	50,3296	49,6616	Não
11	0,8125	0,9540	0,0001	49,9989	0,0969	0,9544	0,9537	50,2930	49,7192	Não
12	0,9063	0,9540	0,0001	50,0014	0,0976	0,9544	0,9537	50,3048	49,7070	Não
13	0,8320	0,9540	0,0001	50,0068	0,0989	0,9544	0,9537	50,3635	49,6544	Não
14	0,8750	0,9540	0,0001	50,0036	0,0953	0,9544	0,9537	50,2850	49,6593	Não
15	0,8320	0,9540	0,0001	49,9973	0,1020	0,9543	0,9537	50,3609	49,6899	Não
16	0,7771	0,9540	0,0001	49,9989	0,0954	0,9544	0,9537	50,2575	49,7040	Não
17	0,7889	0,9540	0,0001	50,0001	0,0953	0,9544	0,9537	50,2689	49,7074	Não
18	0,8438	0,9540	0,0001	50,0002	0,0955	0,9544	0,9537	50,4112	49,6670	Não
19	0,8438	0,9540	0,0001	50,0031	0,1023	0,9543	0,9537	50,3269	49,7047	Não
20	0,7459	0,9540	0,0001	49,9962	0,0972	0,9544	0,9537	50,3037	49,6609	Não
21	0,8750	0,9540	0,0001	49,9997	0,0985	0,9544	0,9537	50,3056	49,6666	Não
22	0,8750	0,9540	0,0001	50,0005	0,0971	0,9544	0,9537	50,3757	49,6994	Não
23	0,7146	0,9540	0,0001	49,9983	0,0986	0,9544	0,9537	50,3395	49,6517	Não
24	0,7695	0,9540	0,0001	50,0014	0,1005	0,9543	0,9537	50,3399	49,6662	Não
25	0,7146	0,9540	0,0001	50,0021	0,0941	0,9544	0,9537	50,3719	49,6777	Não
26	0,9688	0,9540	0,0001	50,0050	0,0989	0,9544	0,9537	50,3445	49,6872	Não
27	0,8125	0,9540	0,0001	50,0029	0,0976	0,9545	0,9537	50,2380	49,6243	Não
28	0,9375	0,9540	0,0001	50,0051	0,0977	0,9544	0,9537	50,3174	49,7074	Não
29	0,8750	0,9540	0,0001	50,0001	0,0965	0,9544	0,9536	50,3300	49,6204	Não
30	0,8125	0,9540	0,0001	50,0104	0,0958	0,9545	0,9537	50,3483	49,7105	Não
31	0,7561	0,9539	0,0013	50,0414	0,2002	0,9543	0,9291	52,8141	49,6780	Sim
32	0,7873	0,9540	0,0001	50,0027	0,0980	0,9544	0,9537	50,3124	49,7139	Não
33	0,8750	0,9540	0,0001	50,0037	0,0953	0,9543	0,9537	50,3281	49,6849	Não
34	0,8320	0,9540	0,0001	49,9983	0,0976	0,9544	0,9537	50,3269	49,6796	Não
35	0,7889	0,9540	0,0001	49,9954	0,1015	0,9544	0,9538	50,3086	49,6704	Não
36	0,8186	0,9540	0,0001	49,9994	0,0977	0,9543	0,9537	50,3193	49,7135	Não
37	0,8632	0,9540	0,0001	50,0018	0,0974	0,9544	0,9537	50,2960	49,5651	Não
38	0,7577	0,9540	0,0001	49,9992	0,0990	0,9543	0,9537	50,3891	49,6712	Não
39	0,6563	0,9540	0,0001	50,0036	0,0991	0,9544	0,9537	50,4112	49,7181	Não
40	0,7695	0,9540	0,0001	49,9950	0,1004	0,9543	0,9537	50,3574	49,6929	Não
41	0,8438	0,9540	0,0001	49,9978	0,0965	0,9544	0,9537	50,3140	49,6052	Não
42	0,9063	0,9540	0,0001	50,0006	0,0999	0,9544	0,9537	50,3242	49,6925	Não
43	0,8125	0,9541	0,0001	49,9988	0,0949	0,9544	0,9538	50,3037	49,6986	Não
44	0,8320	0,9540	0,0001	50,0064	0,0987	0,9544	0,9537	50,3796	49,6761	Não
45	0,8320	0,9540	0,0001	49,9958	0,0956	0,9544	0,9537	50,3365	49,6342	Não
46	0,7889	0,9540	0,0001	50,0058	0,0966	0,9544	0,9537	50,4055	49,6902	Não
47	0,8632	0,9540	0,0001	50,0024	0,0993	0,9543	0,9537	50,3109	49,7223	Não
48	0,8632	0,9540	0,0001	50,0043	0,1009	0,9543	0,9537	50,3178	49,6490	Não
49	0,9063	0,9540	0,0001	49,9984	0,0964	0,9543	0,9537	50,3620	49,7528	Não
50	0,8438	0,9540	0,0001	50,0009	0,1006	0,9544	0,9537	50,3086	49,6975	Não
51	0,8320	0,9540	0,0001	50,0010	0,1011	0,9543	0,9537	50,3162	49,7120	Não
52	0,6875	0,9540	0,0001	49,9987	0,0972	0,9544	0,9536	50,3033	49,7135	Não
53	0,5000	0,1782	0,1387	92,5396	6,5828	0,9250	0,0197	99,3118	51,1883	Sim
54	0,7577	0,9540	0,0001	50,0012	0,0988	0,9544	0,9537	50,3162	49,7410	Não
55	0,6757	0,9540	0,0001	49,9957	0,0954	0,9544	0,9537	50,2739	49,6689	Não
56	0,8438	0,9540	0,0001	49,9954	0,0987	0,9544	0,9537	50,2831	49,7318	Não
57	0,8320	0,9540	0,0001	50,0055	0,0974	0,9544	0,9537	50,2972	49,6746	Não

58	0,8438	0,9540	0,0001	50,0049	0,0991	0,9544	0,9537	50,3670	49,7437	Não
59	0,7873	0,9540	0,0001	50,0028	0,0939	0,9545	0,9537	50,3151	49,6948	Não
60	0,6875	0,9457	0,0268	50,7925	2,0000	0,9543	0,6010	72,1268	49,6986	Sim
61	0,7695	0,9540	0,0001	49,9966	0,1019	0,9544	0,9537	50,3582	49,6578	Não
62	0,7146	0,9540	0,0001	50,0012	0,0973	0,9544	0,9537	50,3380	49,6746	Não
63	0,8007	0,9540	0,0001	50,0008	0,0999	0,9543	0,9537	50,3494	49,7452	Não
64	0,8750	0,9540	0,0001	50,0011	0,0955	0,9544	0,9537	50,3452	49,6773	Não
65	0,8438	0,9540	0,0001	49,9999	0,0999	0,9544	0,9537	50,3162	49,7044	Não
66	0,7264	0,9540	0,0001	50,0005	0,0987	0,9544	0,9537	50,3044	49,6532	Não
67	0,8438	0,9540	0,0001	50,0014	0,0982	0,9544	0,9537	50,2918	49,6662	Não
68	0,8007	0,9540	0,0001	49,9966	0,1000	0,9543	0,9537	50,3483	49,6571	Não
69	0,7695	0,9540	0,0001	50,0000	0,0998	0,9545	0,9537	50,3166	49,6933	Não
70	0,6250	0,9540	0,0001	50,0017	0,0992	0,9544	0,9538	50,3597	49,7173	Não
71	0,8438	0,9540	0,0001	49,9974	0,1002	0,9544	0,9537	50,2827	49,7116	Não
72	0,7771	0,9540	0,0001	49,9992	0,0979	0,9543	0,9538	50,3323	49,6483	Não
73	0,7188	0,9540	0,0001	50,0034	0,0960	0,9544	0,9537	50,2739	49,6937	Não
74	0,8750	0,9540	0,0001	49,9977	0,0980	0,9544	0,9537	50,3407	49,6586	Não
75	0,8125	0,9540	0,0001	50,0004	0,0986	0,9544	0,9537	50,2987	49,6540	Não
76	0,8750	0,9540	0,0001	49,9997	0,0966	0,9544	0,9537	50,3246	49,6708	Não
77	0,8632	0,9540	0,0001	49,9992	0,0971	0,9545	0,9537	50,2716	49,7017	Não
78	0,7146	0,9540	0,0001	50,0052	0,0967	0,9543	0,9537	50,2811	49,6979	Não
79	0,6952	0,9540	0,0001	49,9994	0,0976	0,9544	0,9537	50,3414	49,6700	Não
80	0,8632	0,9540	0,0001	50,0029	0,0990	0,9544	0,9537	50,3067	49,7410	Não
81	0,8750	0,9540	0,0001	50,0042	0,0989	0,9544	0,9537	50,2979	49,7032	Não
82	0,7771	0,9540	0,0001	49,9974	0,0981	0,9544	0,9537	50,2785	49,5129	Não
83	0,8945	0,9540	0,0001	49,9988	0,0983	0,9544	0,9536	50,2926	49,7040	Não
84	0,9063	0,9540	0,0001	50,0036	0,0975	0,9544	0,9537	50,2934	49,6956	Não
85	0,8438	0,9540	0,0001	49,9991	0,0994	0,9544	0,9537	50,3323	49,5964	Não
86	0,8320	0,9540	0,0001	49,9981	0,0989	0,9544	0,9537	50,3136	49,7391	Não
87	0,8438	0,9540	0,0001	49,9992	0,0981	0,9545	0,9536	50,3281	49,6986	Não
88	0,7873	0,9540	0,0001	50,0015	0,0957	0,9544	0,9537	50,2728	49,6342	Não
89	0,8320	0,9540	0,0001	50,0062	0,0963	0,9544	0,9537	50,3563	49,6590	Não
90	0,8320	0,9540	0,0001	50,0001	0,0962	0,9544	0,9537	50,2678	49,6479	Não
91	0,8750	0,9540	0,0001	50,0049	0,0935	0,9544	0,9537	50,2907	49,7116	Não
92	0,6250	0,9540	0,0001	50,0042	0,0924	0,9544	0,9537	50,2949	49,7410	Não
93	0,7146	0,9540	0,0001	50,0020	0,0963	0,9544	0,9537	50,3208	49,6586	Não
94	0,8320	0,9540	0,0001	50,0041	0,0986	0,9544	0,9537	50,2853	49,6437	Não
95	0,8750	0,9540	0,0001	49,9999	0,0966	0,9544	0,9537	50,2823	49,6853	Não
96	0,8750	0,9540	0,0001	49,9952	0,0949	0,9544	0,9537	50,3117	49,6613	Não
97	0,7382	0,9540	0,0001	49,9989	0,1011	0,9544	0,9537	50,3822	49,6922	Não
98	0,8750	0,9540	0,0001	49,9975	0,0977	0,9544	0,9537	50,3014	49,7192	Não
99	0,8750	0,9540	0,0001	50,0067	0,0970	0,9544	0,9537	50,2960	49,6944	Não
100	0,8125	0,9540	0,0001	49,9982	0,1003	0,9544	0,9537	50,2937	49,6819	Não
101	0,8320	0,9540	0,0001	50,0022	0,0971	0,9544	0,9537	50,2815	49,7391	Não
102	0,8632	0,9540	0,0001	50,0006	0,0971	0,9544	0,9537	50,3311	49,6849	Não
103	0,8438	0,9540	0,0001	50,0005	0,0976	0,9544	0,9537	50,3757	49,7108	Não
104	0,8438	0,9540	0,0001	50,0043	0,0949	0,9544	0,9537	50,2586	49,7227	Não
105	0,7146	0,9540	0,0001	50,0034	0,1008	0,9544	0,9537	50,3757	49,6944	Não
106	0,7500	0,9540	0,0001	49,9942	0,0988	0,9544	0,9537	50,3468	49,6964	Não
107	0,8438	0,9540	0,0001	50,0001	0,0998	0,9544	0,9537	50,3307	49,6891	Não
108	0,8007	0,9540	0,0001	50,0012	0,0987	0,9544	0,9537	50,4002	49,6502	Não
109	0,4054	0,1770	0,1436	92,0227	7,1528	0,9036	0,0094	99,6635	51,7979	Sim
110	0,8632	0,9540	0,0001	49,9985	0,0982	0,9544	0,9537	50,3384	49,7128	Não
111	0,8320	0,9540	0,0001	50,0021	0,0983	0,9544	0,9537	50,3479	49,7162	Não
112	0,8007	0,9540	0,0001	50,0028	0,0968	0,9544	0,9537	50,3300	49,6742	Não
113	0,8007	0,9540	0,0001	50,0043	0,0955	0,9544	0,9537	50,3181	49,6872	Não
114	0,8750	0,9540	0,0001	50,0013	0,0919	0,9544	0,9536	50,3109	49,6181	Não
115	0,7695	0,9540	0,0001	50,0024	0,0975	0,9544	0,9537	50,3120	49,7353	Não
116	0,7771	0,9540	0,0001	49,9966	0,0990	0,9544	0,9537	50,2556	49,6563	Não
117	0,8438	0,9540	0,0001	49,9989	0,0975	0,9544	0,9537	50,3029	49,7200	Não
118	0,7264	0,9540	0,0001	49,9991	0,0950	0,9543	0,9537	50,3273	49,7074	Não
119	0,8750	0,9540	0,0001	50,0074	0,0954	0,9544	0,9537	50,3098	49,6078	Não
120	0,9063	0,9540	0,0001	49,9979	0,0960	0,9544	0,9537	50,3433	49,6620	Não
121	0,8320	0,9540	0,0001	50,0014	0,0961	0,9544	0,9537	50,3540	49,7177	Não
122	0,7577	0,9540	0,0001	49,9997	0,0945	0,9544	0,9537	50,3372	49,7189	Não
123	0,8750	0,9540	0,0001	50,0006	0,0961	0,9543	0,9537	50,3693	49,6643	Não
124	0,8320	0,9540	0,0001	49,9994	0,0977	0,9544	0,9537	50,3319	49,6567	Não
125	0,9063	0,9540	0,0001	50,0008	0,0962	0,9543	0,9537	50,2884	49,7074	Não
126	0,7500	0,9540	0,0001	49,9987	0,0964	0,9543	0,9537	50,2777	49,7173	Não
127	0,9063	0,9540	0,0001	50,0003	0,0992	0,9544	0,9537	50,3361	49,6952	Não
128	0,8438	0,9540	0,0001	49,9981	0,0986	0,9544	0,9537	50,3223	49,6975	Não
129	0,8320	0,9540	0,0001	49,9935	0,1007	0,9544	0,9537	50,3033	49,6586	Não
130	0,9063	0,9540	0,0001	50,0017	0,0971	0,9544	0,9537	50,3113	49,6861	Não
131	0,8750	0,9540	0,0001	50,0022	0,0988	0,9544	0,9538	50,3010	49,6792	Não
132	0,8438	0,9540	0,0001	50,0025	0,0990	0,9544	0,9537	50,3551	49,7051	Não
133	0,8438	0,9540	0,0001	49,9974	0,0978	0,9544	0,9538	50,3014	49,6120	Não
134	0,8007	0,9540	0,0001	49,9996	0,0961	0,9544	0,9537	50,2804	49,6994	Não
135	0,8438	0,9540	0,0001	50,0001	0,0984	0,9543	0,9537	50,3120	49,7250	Não
136	0,8438	0,9540	0,0001	49,9971	0,0997	0,9544	0,9537	50,3620	49,7463	Não
137	0,8750	0,9540	0,0001	49,9992	0,0990	0,9544	0,9537	50,3429	49,6609	Não

138	0,7146	0,9541	0,0001	49,9992	0,0935	0,9544	0,9537	50,3128	49,7421	Não
139	0,7131	0,9540	0,0001	50,0005	0,0958	0,9544	0,9538	50,2758	49,7272	Não
140	0,8438	0,9540	0,0001	49,9976	0,0976	0,9543	0,9537	50,3544	49,6082	Não
141	0,8007	0,9540	0,0001	50,0064	0,0973	0,9544	0,9537	50,2831	49,7372	Não
142	0,7500	0,9540	0,0001	50,0013	0,1005	0,9544	0,9538	50,3296	49,6967	Não
143	0,8320	0,9540	0,0001	50,0042	0,0986	0,9544	0,9537	50,3418	49,7078	Não
144	0,8320	0,9540	0,0001	50,0018	0,0959	0,9544	0,9537	50,2548	49,7158	Não
145	0,8438	0,9540	0,0001	50,0031	0,0999	0,9545	0,9537	50,3037	49,7040	Não
146	0,7577	0,9540	0,0001	49,9983	0,0959	0,9543	0,9537	50,3052	49,6658	Não
147	0,8750	0,9540	0,0001	49,9979	0,0919	0,9543	0,9537	50,2651	49,7150	Não
148	0,8320	0,9540	0,0001	49,9948	0,1020	0,9544	0,9537	50,2880	49,6624	Não
149	0,6304	0,7753	0,1641	61,7477	9,7136	0,9543	0,2725	88,3583	49,7849	Sim
150	0,7248	0,9540	0,0001	49,9981	0,0982	0,9544	0,9537	50,3399	49,7097	Não
151	0,7813	0,9540	0,0001	49,9968	0,0951	0,9544	0,9537	50,3101	49,7055	Não
152	0,8320	0,9540	0,0001	50,0013	0,1009	0,9544	0,9537	50,3254	49,6460	Não
153	0,8007	0,9540	0,0001	49,9927	0,1000	0,9543	0,9537	50,3166	49,6395	Não
154	0,8438	0,9540	0,0001	50,0002	0,0930	0,9544	0,9537	50,2743	49,6922	Não
155	0,8438	0,9540	0,0001	50,0003	0,0991	0,9543	0,9538	50,2949	49,5800	Não
156	0,8750	0,9540	0,0001	49,9972	0,0972	0,9543	0,9537	50,3525	49,6666	Não
157	0,8320	0,9540	0,0001	49,9957	0,0976	0,9543	0,9538	50,3868	49,6986	Não
158	0,6936	0,9540	0,0001	50,0018	0,0983	0,9544	0,9537	50,3387	49,7345	Não
159	0,5992	0,9540	0,0001	50,0007	0,1051	0,9543	0,9537	50,3914	49,6696	Não
160	0,8750	0,9540	0,0001	49,9989	0,0981	0,9544	0,9537	50,2987	49,6746	Não
161	0,9688	0,9540	0,0001	49,9940	0,0964	0,9543	0,9537	50,3033	49,7139	Não
162	0,8750	0,9540	0,0001	49,9967	0,0993	0,9544	0,9537	50,3448	49,6685	Não
163	0,8750	0,9540	0,0001	50,0020	0,0956	0,9544	0,9537	50,3166	49,7272	Não
164	0,8945	0,9540	0,0001	50,0036	0,0964	0,9543	0,9537	50,3258	49,6925	Não
165	0,8632	0,9540	0,0001	50,0006	0,0971	0,9544	0,9537	50,3399	49,5869	Não
166	0,7695	0,9540	0,0001	50,0019	0,0981	0,9544	0,9537	50,2850	49,7124	Não
167	0,7146	0,9540	0,0001	50,0005	0,0934	0,9544	0,9537	50,2537	49,7288	Não
168	0,9063	0,9540	0,0001	50,0008	0,0981	0,9544	0,9537	50,2636	49,6922	Não
169	0,8438	0,9540	0,0001	49,9993	0,0974	0,9544	0,9537	50,2819	49,6445	Não
170	0,8632	0,9540	0,0001	50,0023	0,0951	0,9544	0,9537	50,3666	49,7112	Não
171	0,5434	0,9540	0,0001	50,0017	0,1004	0,9544	0,9537	50,2762	49,6311	Não
172	0,7695	0,9540	0,0001	49,9969	0,1002	0,9544	0,9536	50,2857	49,6609	Não
173	0,8125	0,9540	0,0001	49,9950	0,0968	0,9544	0,9537	50,2861	49,6857	Não
174	0,7813	0,9540	0,0001	49,9988	0,0979	0,9543	0,9537	50,2773	49,7147	Não
175	0,8438	0,9541	0,0001	49,9968	0,0966	0,9544	0,9538	50,3105	49,7002	Não
176	0,7813	0,9540	0,0001	49,9980	0,0991	0,9543	0,9537	50,2716	49,6677	Não
177	0,8320	0,9540	0,0001	50,0001	0,0960	0,9544	0,9537	50,3681	49,7238	Não
178	0,8320	0,9540	0,0001	50,0039	0,0984	0,9545	0,9537	50,3632	49,6696	Não
179	0,7248	0,9540	0,0003	50,0091	0,1145	0,9543	0,9481	50,9632	49,6696	Sim
180	0,8750	0,9540	0,0001	49,9989	0,1013	0,9544	0,9537	50,3075	49,6922	Não
181	0,7561	0,9540	0,0003	50,0025	0,1126	0,9544	0,9473	51,0891	49,6346	Sim
182	0,8438	0,9540	0,0001	50,0011	0,1001	0,9544	0,9537	50,3391	49,6441	Não
183	0,8320	0,9540	0,0001	50,0038	0,0933	0,9543	0,9537	50,3735	49,7181	Não
184	0,9375	0,9540	0,0001	49,9941	0,0970	0,9543	0,9537	50,2899	49,6727	Não
185	0,8750	0,9540	0,0001	49,9996	0,0940	0,9544	0,9537	50,3006	49,6799	Não
186	0,7771	0,9540	0,0001	49,9985	0,0981	0,9544	0,9538	50,3094	49,6304	Não
187	0,8125	0,9540	0,0001	49,9956	0,0944	0,9544	0,9537	50,2762	49,7116	Não
188	0,7561	0,9540	0,0001	50,0029	0,0999	0,9543	0,9537	50,3296	49,6849	Não
189	0,8202	0,9540	0,0001	49,9959	0,0999	0,9544	0,9537	50,2769	49,6426	Não
190	0,8320	0,9540	0,0001	50,0007	0,0931	0,9543	0,9537	50,2850	49,7349	Não
191	0,7070	0,9540	0,0001	49,9991	0,0956	0,9543	0,9537	50,2880	49,5991	Não
192	0,8125	0,9540	0,0001	49,9974	0,0947	0,9544	0,9537	50,3834	49,7200	Não
193	0,8750	0,9540	0,0001	50,0073	0,0930	0,9544	0,9537	50,3006	49,7536	Não
194	0,8438	0,9540	0,0001	50,0025	0,0974	0,9544	0,9537	50,3330	49,6887	Não
195	0,6875	0,9540	0,0001	50,0002	0,0977	0,9543	0,9537	50,2796	49,6460	Não
196	0,7264	0,9540	0,0001	49,9996	0,0965	0,9544	0,9537	50,2804	49,7047	Não
197	0,7146	0,9540	0,0001	49,9965	0,0966	0,9544	0,9537	50,2827	49,7158	Não
198	0,8750	0,9540	0,0001	50,0012	0,0989	0,9544	0,9536	50,3456	49,7528	Não
199	0,8632	0,9540	0,0001	50,0011	0,0952	0,9544	0,9537	50,3201	49,7166	Não
200	0,9063	0,9540	0,0001	50,0056	0,0971	0,9544	0,9537	50,2991	49,7299	Não
201	0,8438	0,9540	0,0001	49,9959	0,1026	0,9544	0,9537	50,3212	49,6819	Não
202	0,8750	0,9540	0,0001	49,9957	0,1023	0,9543	0,9537	50,2995	49,6056	Não
203	0,5778	0,5724	0,2166	73,2897	11,2208	0,9542	0,0813	96,6290	49,8722	Sim
204	0,8320	0,9540	0,0001	50,0054	0,1004	0,9543	0,9537	50,3994	49,6933	Não
205	0,9063	0,9540	0,0001	50,0024	0,0965	0,9544	0,9537	50,3490	49,6765	Não
206	0,8438	0,9540	0,0001	50,0006	0,0985	0,9544	0,9537	50,2995	49,6666	Não
207	0,8438	0,9540	0,0001	49,9998	0,0966	0,9544	0,9538	50,2819	49,6937	Não
208	0,8438	0,9540	0,0001	50,0015	0,0992	0,9544	0,9537	50,3849	49,7452	Não
209	0,8007	0,9540	0,0001	50,0004	0,1002	0,9543	0,9537	50,3365	49,7070	Não
210	0,9063	0,9540	0,0001	50,0016	0,0946	0,9544	0,9537	50,3456	49,7131	Não
211	0,7577	0,9540	0,0001	49,9980	0,0973	0,9544	0,9536	50,2682	49,6719	Não
212	0,6617	0,9540	0,0001	50,0014	0,0962	0,9544	0,9537	50,3094	49,7219	Não
213	0,8750	0,9540	0,0001	49,9988	0,0927	0,9544	0,9537	50,3456	49,7120	Não
214	0,3278	0,0391	0,0486	98,2972	2,5402	0,3363	0,0007	99,9870	76,1070	Sim
215	0,7500	0,9540	0,0001	50,0001	0,0960	0,9543	0,9537	50,3128	49,6159	Não
216	0,9063	0,9540	0,0001	49,9978	0,0979	0,9544	0,9537	50,3334	49,6906	Não
217	0,9063	0,9540	0,0001	49,9980	0,0983	0,9544	0,9536	50,3078	49,6040	Não

218	0,8320	0,9540	0,0001	50,0011	0,0943	0,9545	0,9537	50,2834	49,6685	Não
219	0,8750	0,9540	0,0001	50,0023	0,0963	0,9543	0,9537	50,3235	49,7211	Não
220	0,7577	0,9540	0,0001	50,0030	0,0961	0,9544	0,9537	50,3105	49,7147	Não
221	0,8438	0,9540	0,0001	49,9996	0,0972	0,9544	0,9537	50,3006	49,6567	Não
222	0,9063	0,9540	0,0001	49,9944	0,0955	0,9544	0,9537	50,3040	49,6964	Não
223	0,8320	0,9540	0,0001	49,9984	0,0959	0,9545	0,9537	50,3197	49,7005	Não
224	0,9063	0,9540	0,0001	50,0028	0,0942	0,9544	0,9537	50,3269	49,7356	Não
225	0,8438	0,9540	0,0001	50,0022	0,0995	0,9545	0,9538	50,3407	49,7089	Não
226	0,8007	0,9540	0,0001	49,9956	0,1003	0,9544	0,9536	50,4013	49,6422	Não
227	0,9063	0,9540	0,0001	50,0004	0,0983	0,9544	0,9536	50,3044	49,6750	Não
228	0,6250	0,9540	0,0001	49,9961	0,0987	0,9544	0,9537	50,3437	49,6864	Não
229	0,9063	0,9540	0,0001	49,9955	0,0966	0,9544	0,9537	50,3422	49,7105	Não
230	0,8320	0,9540	0,0001	49,9997	0,0968	0,9543	0,9537	50,3223	49,7494	Não
231	0,8007	0,9540	0,0001	50,0035	0,0936	0,9544	0,9537	50,3170	49,7269	Não
232	0,9063	0,9540	0,0001	50,0016	0,0998	0,9544	0,9536	50,3017	49,6925	Não
233	0,8632	0,9540	0,0001	50,0059	0,0984	0,9543	0,9537	50,3761	49,7108	Não
234	0,8007	0,9540	0,0001	49,9993	0,0987	0,9544	0,9536	50,3723	49,6830	Não
235	0,7695	0,9540	0,0001	49,9976	0,0949	0,9543	0,9537	50,3040	49,6361	Não
236	0,6875	0,9540	0,0001	50,0031	0,0957	0,9544	0,9537	50,3235	49,6998	Não
237	0,7695	0,9540	0,0001	49,9953	0,0938	0,9543	0,9537	50,3456	49,7116	Não
238	0,8750	0,9540	0,0001	49,9987	0,0991	0,9544	0,9537	50,3063	49,7021	Não
239	0,9063	0,9540	0,0001	50,0006	0,0987	0,9544	0,9537	50,3201	49,6693	Não
240	0,6952	0,9540	0,0001	50,0019	0,1002	0,9544	0,9537	50,3235	49,6925	Não
241	0,8945	0,9540	0,0001	50,0011	0,0998	0,9544	0,9537	50,3021	49,6445	Não
242	0,7561	0,9540	0,0001	49,9999	0,0971	0,9544	0,9538	50,2998	49,6964	Não
243	0,7146	0,9540	0,0001	50,0017	0,0945	0,9544	0,9537	50,2769	49,6990	Não
244	0,7771	0,9540	0,0001	49,9951	0,0991	0,9544	0,9536	50,3067	49,6674	Não
245	0,8750	0,9540	0,0001	50,0040	0,0976	0,9543	0,9537	50,2831	49,6632	Não
246	0,8320	0,9540	0,0001	50,0012	0,0973	0,9544	0,9536	50,3242	49,5922	Não
247	0,6875	0,9540	0,0001	49,9995	0,0936	0,9543	0,9537	50,2789	49,7044	Não
248	0,8320	0,9540	0,0001	49,9994	0,0971	0,9544	0,9536	50,2838	49,7009	Não
249	0,7695	0,9540	0,0001	50,0036	0,0977	0,9544	0,9537	50,3704	49,6895	Não
250	0,8438	0,9540	0,0001	50,0003	0,0990	0,9544	0,9537	50,2819	49,6346	Não
251	0,8632	0,9541	0,0001	49,9968	0,0997	0,9544	0,9537	50,3143	49,6841	Não
252	0,8320	0,9540	0,0001	50,0007	0,0982	0,9545	0,9537	50,3258	49,6887	Não
253	0,8632	0,9540	0,0001	50,0005	0,0930	0,9543	0,9537	50,2922	49,7250	Não
254	0,7771	0,9540	0,0001	49,9911	0,0970	0,9544	0,9537	50,3223	49,6971	Não
255	0,8125	0,9540	0,0001	50,0023	0,0975	0,9543	0,9537	50,3422	49,6864	Não
256	0,8632	0,9540	0,0001	50,0026	0,0948	0,9544	0,9537	50,2930	49,6620	Não
257	0,6936	0,9540	0,0001	50,0016	0,0970	0,9544	0,9537	50,2934	49,6357	Não
258	0,8438	0,9540	0,0001	50,0052	0,0992	0,9544	0,9537	50,3658	49,6731	Não
259	0,8007	0,9540	0,0001	50,0004	0,1000	0,9544	0,9537	50,3510	49,7040	Não
260	0,8007	0,9540	0,0001	49,9970	0,0968	0,9544	0,9537	50,3296	49,6883	Não
261	0,7382	0,9540	0,0001	49,9977	0,0976	0,9543	0,9537	50,3048	49,7292	Não
262	0,9063	0,9540	0,0001	49,9992	0,0984	0,9544	0,9537	50,3300	49,6670	Não
263	0,8750	0,9540	0,0001	49,9974	0,0924	0,9544	0,9537	50,2911	49,7360	Não
264	0,7264	0,9540	0,0001	50,0077	0,0980	0,9543	0,9537	50,3212	49,6937	Não
265	0,8125	0,9540	0,0001	49,9992	0,0952	0,9543	0,9537	50,3037	49,6479	Não
266	0,7146	0,9540	0,0001	49,9971	0,0989	0,9544	0,9537	50,2480	49,6445	Não
267	0,9063	0,9540	0,0001	49,9983	0,1010	0,9544	0,9536	50,3017	49,6990	Não
268	0,9375	0,9540	0,0001	50,0005	0,0954	0,9543	0,9537	50,2731	49,7208	Não
269	0,8320	0,9540	0,0001	49,9988	0,0953	0,9544	0,9538	50,3460	49,6346	Não
270	0,9063	0,9540	0,0001	49,9978	0,0955	0,9544	0,9537	50,2750	49,6651	Não
271	0,8438	0,9540	0,0001	49,9998	0,0962	0,9544	0,9537	50,2842	49,7391	Não
272	0,9063	0,9540	0,0001	49,9937	0,1015	0,9544	0,9537	50,3391	49,6681	Não
273	0,8320	0,9540	0,0001	50,0001	0,1011	0,9544	0,9537	50,2850	49,7303	Não
274	0,8320	0,9540	0,0001	50,0000	0,0977	0,9543	0,9537	50,3174	49,7124	Não
275	0,8320	0,9540	0,0001	49,9956	0,0966	0,9544	0,9537	50,3098	49,6677	Não
276	0,8438	0,9540	0,0001	49,9947	0,0957	0,9544	0,9537	50,3357	49,6582	Não
277	0,8750	0,9540	0,0001	49,9975	0,0965	0,9544	0,9536	50,2583	49,6773	Não
278	0,8125	0,9540	0,0001	49,9948	0,0953	0,9543	0,9537	50,3006	49,7021	Não
279	0,9063	0,9540	0,0001	50,0049	0,0945	0,9544	0,9537	50,3048	49,6521	Não
280	0,7500	0,9540	0,0001	49,9970	0,0978	0,9544	0,9536	50,3216	49,6128	Não
281	0,7500	0,9540	0,0001	49,9979	0,0973	0,9544	0,9537	50,3140	49,6788	Não
282	0,8007	0,9540	0,0001	50,0027	0,0983	0,9544	0,9537	50,2869	49,7341	Não
283	0,8438	0,9540	0,0001	49,9975	0,0984	0,9545	0,9538	50,3498	49,6204	Não
284	0,6250	0,9540	0,0001	50,0020	0,0991	0,9544	0,9537	50,2956	49,6559	Não
285	0,8125	0,9540	0,0001	49,9992	0,0964	0,9543	0,9537	50,3078	49,7215	Não
286	0,8438	0,9540	0,0001	49,9973	0,0978	0,9544	0,9536	50,3395	49,6548	Não
287	0,8007	0,9540	0,0001	50,0040	0,0967	0,9544	0,9537	50,3365	49,6071	Não
288	0,8320	0,9540	0,0001	50,0028	0,0971	0,9544	0,9537	50,3059	49,6769	Não
289	0,8750	0,9540	0,0001	49,9979	0,1005	0,9544	0,9537	50,3124	49,6834	Não
290	0,8007	0,9540	0,0001	50,0001	0,0994	0,9544	0,9537	50,2792	49,6155	Não
291	0,8007	0,9540	0,0001	49,9992	0,0976	0,9544	0,9537	50,2991	49,7078	Não
292	0,8007	0,9540	0,0001	50,0010	0,0948	0,9543	0,9537	50,3075	49,6265	Não
293	0,8125	0,9540	0,0001	50,0062	0,0960	0,9544	0,9536	50,3014	49,6758	Não
294	0,7577	0,9540	0,0001	49,9990	0,0959	0,9544	0,9535	50,3181	49,6712	Não
295	0,8438	0,9540	0,0001	49,9958	0,0962	0,9543	0,9537	50,3094	49,6082	Não
296	0,8750	0,9540	0,0001	49,9949	0,0952	0,9544	0,9536	50,2850	49,6868	Não
297	0,9063	0,9540	0,0001	49,9962	0,0989	0,9545	0,9536	50,3124	49,6883	Não

298	0,7264	0,9540	0,0001	50,0035	0,0955	0,9544	0,9537	50,2747	49,6738	Não
299	0,7873	0,9540	0,0001	50,0015	0,0957	0,9544	0,9537	50,2728	49,6342	Não
300	0,8750	0,9540	0,0001	50,0035	0,0969	0,9544	0,9537	50,3063	49,6872	Não
301	0,6875	0,9540	0,0001	50,0059	0,0973	0,9543	0,9537	50,3242	49,6849	Não
302	0,8438	0,9540	0,0001	49,9973	0,1020	0,9544	0,9537	50,3658	49,6574	Não
303	0,8007	0,9540	0,0001	50,0001	0,0959	0,9544	0,9537	50,2888	49,7005	Não
304	1,0000	0,9540	0,0001	50,0005	0,0949	0,9544	0,9537	50,3361	49,6960	Não
305	0,7889	0,9540	0,0001	49,9999	0,0980	0,9544	0,9537	50,2632	49,6708	Não
306	0,9063	0,9540	0,0001	49,9987	0,0975	0,9543	0,9537	50,3025	49,6784	Não
307	0,8438	0,9540	0,0001	50,0026	0,0987	0,9544	0,9537	50,3353	49,6693	Não
308	0,8750	0,9540	0,0001	49,9998	0,1041	0,9544	0,9537	50,3033	49,6067	Não
309	0,8750	0,9540	0,0001	49,9959	0,0993	0,9544	0,9537	50,3639	49,6490	Não
310	0,6250	0,8031	0,1709	60,0976	9,8564	0,9542	0,2190	90,7375	49,8394	Sim
311	0,7500	0,9540	0,0001	49,9995	0,0959	0,9543	0,9537	50,3265	49,7421	Não
312	0,8750	0,9540	0,0001	50,0016	0,0976	0,9544	0,9537	50,2934	49,6613	Não
313	0,7889	0,9540	0,0001	49,9999	0,0961	0,9544	0,9537	50,2964	49,7215	Não
314	0,9063	0,9540	0,0001	49,9952	0,1001	0,9543	0,9537	50,3456	49,6002	Não
315	0,8320	0,9540	0,0001	49,9982	0,0949	0,9544	0,9537	50,3208	49,6910	Não
316	0,8438	0,9540	0,0001	49,9980	0,0955	0,9544	0,9537	50,3262	49,6735	Não
317	0,9688	0,9540	0,0001	50,0073	0,0971	0,9544	0,9537	50,2934	49,7067	Não
318	0,8750	0,9540	0,0001	50,0049	0,0971	0,9543	0,9537	50,3361	49,6807	Não
319	0,7771	0,9540	0,0001	49,9996	0,0937	0,9544	0,9537	50,3975	49,7135	Não
320	0,8632	0,9540	0,0001	49,9978	0,0969	0,9544	0,9536	50,3040	49,7208	Não
321	0,6929	0,9540	0,0001	50,0028	0,0949	0,9544	0,9537	50,3441	49,7032	Não
322	0,4917	0,3394	0,1786	84,4708	8,7250	0,9218	0,0179	99,3305	52,2213	Sim
323	0,8438	0,9541	0,0001	50,0034	0,0957	0,9544	0,9536	50,3048	49,7528	Não
324	0,9063	0,9540	0,0001	49,9975	0,0991	0,9544	0,9537	50,2758	49,6792	Não
325	0,7577	0,9540	0,0001	49,9987	0,0985	0,9544	0,9537	50,3895	49,7131	Não
326	0,8438	0,9540	0,0001	50,0016	0,0969	0,9544	0,9537	50,2941	49,7292	Não
327	0,7695	0,9540	0,0001	50,0019	0,0995	0,9545	0,9537	50,4005	49,6761	Não
328	0,8632	0,9540	0,0001	49,9999	0,0974	0,9545	0,9537	50,2796	49,6716	Não
329	0,8320	0,9540	0,0001	49,9991	0,0982	0,9544	0,9537	50,3147	49,6254	Não
330	0,8320	0,9540	0,0001	50,0027	0,0975	0,9544	0,9537	50,3010	49,6403	Não
331	0,6757	0,9540	0,0001	49,9970	0,0968	0,9544	0,9537	50,3262	49,6567	Não
332	0,9063	0,9540	0,0001	49,9976	0,0987	0,9544	0,9537	50,3361	49,6723	Não
333	0,9063	0,9540	0,0001	50,0063	0,0983	0,9544	0,9537	50,3258	49,7288	Não
334	0,8320	0,9540	0,0001	49,9996	0,0968	0,9544	0,9537	50,3273	49,6643	Não
335	0,8320	0,9540	0,0001	49,9961	0,0995	0,9544	0,9538	50,3635	49,6998	Não
336	0,8750	0,9540	0,0001	50,0024	0,0984	0,9544	0,9537	50,2846	49,6830	Não
337	0,5938	0,9540	0,0001	49,9992	0,0996	0,9544	0,9535	50,3384	49,6372	Não
338	0,7889	0,9540	0,0001	50,0069	0,0954	0,9544	0,9537	50,3223	49,6761	Não
339	0,8632	0,9540	0,0001	50,0003	0,0984	0,9543	0,9538	50,2972	49,6754	Não
340	0,9375	0,9540	0,0001	50,0003	0,0958	0,9544	0,9536	50,2663	49,6861	Não
341	0,6929	0,9540	0,0001	50,0017	0,0988	0,9543	0,9537	50,2731	49,6513	Não
342	0,8750	0,9540	0,0001	50,0056	0,0992	0,9543	0,9537	50,3796	49,6773	Não
343	0,7873	0,9540	0,0001	49,9990	0,0991	0,9544	0,9537	50,3925	49,7002	Não
344	0,8007	0,9540	0,0001	50,0003	0,0993	0,9544	0,9538	50,2819	49,6750	Não
345	0,6563	0,9540	0,0001	50,0044	0,0968	0,9544	0,9537	50,3593	49,6922	Não
346	0,8438	0,9540	0,0001	49,9976	0,0983	0,9544	0,9537	50,2953	49,6971	Não
347	0,6716	0,9540	0,0001	50,0047	0,0997	0,9543	0,9537	50,3212	49,6635	Não
348	0,7889	0,9540	0,0001	49,9978	0,0985	0,9544	0,9537	50,2926	49,6639	Não
349	0,6304	0,5509	0,2216	73,8314	11,5982	0,9540	0,0916	96,0724	49,8878	Sim
350	0,8438	0,9540	0,0001	50,0019	0,0966	0,9544	0,9537	50,3693	49,7047	Não
351	0,8750	0,9540	0,0001	49,9984	0,0981	0,9544	0,9537	50,3548	49,6632	Não
352	0,6952	0,9540	0,0001	50,0037	0,0982	0,9544	0,9537	50,2861	49,7257	Não
353	0,8125	0,9540	0,0001	49,9985	0,0966	0,9544	0,9537	50,3094	49,6246	Não
354	0,8125	0,9540	0,0001	50,0010	0,0969	0,9543	0,9537	50,2884	49,6967	Não
355	0,8750	0,9540	0,0001	49,9932	0,0973	0,9544	0,9537	50,2678	49,6010	Não
356	0,7577	0,9540	0,0001	50,0008	0,1027	0,9544	0,9537	50,3330	49,6494	Não
357	0,8438	0,9541	0,0001	49,9990	0,0965	0,9544	0,9537	50,3143	49,7021	Não
358	0,7500	0,9540	0,0001	50,0036	0,0937	0,9544	0,9537	50,3162	49,7097	Não
359	0,9375	0,9540	0,0001	50,0000	0,1000	0,9544	0,9537	50,3445	49,6933	Não
360	0,6563	0,9540	0,0001	50,0083	0,0994	0,9544	0,9537	50,4032	49,7017	Não
361	0,8632	0,9540	0,0001	49,9952	0,0964	0,9544	0,9537	50,2720	49,6979	Não
362	0,8438	0,9540	0,0001	50,0017	0,0978	0,9544	0,9537	50,2701	49,6456	Não
363	0,8438	0,9540	0,0001	50,0059	0,0969	0,9544	0,9536	50,3193	49,7101	Não
364	0,8438	0,9540	0,0001	49,9973	0,0963	0,9544	0,9537	50,3448	49,6849	Não
365	0,7500	0,9540	0,0001	49,9973	0,0962	0,9544	0,9537	50,2903	49,6410	Não
366	0,6716	0,9540	0,0001	49,9989	0,0994	0,9543	0,9537	50,3098	49,6693	Não
367	0,7500	0,9540	0,0001	49,9995	0,0981	0,9544	0,9537	50,3254	49,7211	Não
368	0,8125	0,9540	0,0001	49,9938	0,0990	0,9544	0,9537	50,3868	49,6872	Não
369	0,8007	0,9540	0,0001	50,0009	0,1006	0,9544	0,9537	50,2758	49,6738	Não
370	0,9375	0,9540	0,0001	49,9999	0,0988	0,9544	0,9537	50,3422	49,6830	Não
371	0,7813	0,9540	0,0001	49,9996	0,0978	0,9544	0,9537	50,3487	49,6765	Não
372	0,8632	0,9540	0,0001	50,0036	0,0977	0,9544	0,9536	50,3185	49,6971	Não
373	0,8438	0,9541	0,0001	50,0016	0,0981	0,9544	0,9537	50,3128	49,6433	Não
374	0,8632	0,9540	0,0001	49,9972	0,0965	0,9544	0,9537	50,2831	49,6826	Não
375	0,8632	0,9540	0,0001	50,0031	0,0964	0,9543	0,9537	50,3632	49,7002	Não
376	0,8438	0,9540	0,0001	49,9929	0,0999	0,9544	0,9537	50,2964	49,6918	Não
377	0,8438	0,9540	0,0001	50,0064	0,0983	0,9543	0,9537	50,3647	49,7181	Não

378	0,7500	0,9540	0,0001	49,9989	0,0985	0,9543	0,9537	50,4082	49,7345	Não
379	0,7500	0,9540	0,0001	49,9980	0,1004	0,9543	0,9536	50,2930	49,6193	Não
380	0,7131	0,9540	0,0001	50,0011	0,1030	0,9543	0,9536	50,3948	49,6536	Não
381	0,8750	0,9540	0,0001	49,9997	0,0969	0,9543	0,9537	50,2789	49,7379	Não
382	0,7146	0,9540	0,0001	50,0025	0,1004	0,9544	0,9537	50,3315	49,6639	Não
383	0,5000	0,3400	0,2072	84,8899	9,9249	0,9477	0,0257	99,0562	51,2020	Sim
384	0,7889	0,9540	0,0001	49,9968	0,0961	0,9544	0,9537	50,3334	49,6395	Não
385	0,8320	0,9540	0,0001	50,0040	0,1012	0,9544	0,9537	50,3506	49,6624	Não
386	0,9063	0,9540	0,0001	49,9987	0,1014	0,9544	0,9537	50,3078	49,6521	Não
387	0,8125	0,9540	0,0001	50,0014	0,0971	0,9544	0,9537	50,3330	49,7288	Não
388	0,8438	0,9540	0,0001	49,9985	0,0933	0,9544	0,9537	50,3578	49,7181	Não
389	0,9063	0,9540	0,0001	49,9986	0,0993	0,9544	0,9537	50,2956	49,6845	Não
390	0,7264	0,9540	0,0001	49,9994	0,0970	0,9543	0,9537	50,2945	49,7314	Não
391	0,7500	0,9540	0,0001	50,0001	0,0975	0,9543	0,9537	50,3418	49,6952	Não
392	0,6250	0,9540	0,0001	49,9983	0,0993	0,9544	0,9537	50,3723	49,6647	Não
393	0,8320	0,9540	0,0001	50,0001	0,0966	0,9543	0,9537	50,2998	49,6819	Não
394	0,7695	0,9540	0,0001	49,9988	0,0948	0,9545	0,9537	50,2678	49,6922	Não
395	0,8750	0,9540	0,0001	49,9952	0,0973	0,9544	0,9537	50,2720	49,6536	Não
396	0,7873	0,9540	0,0001	49,9939	0,0963	0,9545	0,9537	50,2991	49,6319	Não
397	0,8125	0,9540	0,0001	49,9990	0,0954	0,9544	0,9537	50,3101	49,6395	Não
398	0,7500	0,9540	0,0001	50,0045	0,0999	0,9544	0,9535	50,3071	49,6552	Não
399	0,8750	0,9540	0,0001	50,0050	0,0986	0,9544	0,9537	50,3872	49,7353	Não
400	0,8632	0,9541	0,0001	50,0015	0,1009	0,9543	0,9537	50,3315	49,7135	Não
401	0,7500	0,9540	0,0001	49,9949	0,1007	0,9544	0,9537	50,2960	49,6742	Não
402	0,7577	0,9540	0,0001	50,0039	0,0977	0,9545	0,9537	50,2838	49,6925	Não
403	0,7577	0,9540	0,0001	49,9947	0,0969	0,9543	0,9537	50,3468	49,7108	Não
404	0,8007	0,9540	0,0001	50,0028	0,0979	0,9544	0,9537	50,3242	49,7337	Não
405	0,8750	0,9540	0,0001	50,0007	0,0944	0,9544	0,9537	50,3468	49,7059	Não
406	0,8438	0,9540	0,0001	49,9994	0,0935	0,9544	0,9537	50,2716	49,6769	Não
407	0,7695	0,9540	0,0001	49,9995	0,0967	0,9544	0,9537	50,3445	49,6799	Não
408	0,7500	0,9540	0,0001	50,0024	0,1007	0,9544	0,9537	50,2918	49,6422	Não
409	0,8007	0,9540	0,0001	49,9982	0,0958	0,9544	0,9537	50,3361	49,6857	Não
410	0,8750	0,9540	0,0001	49,9974	0,0924	0,9544	0,9537	50,2911	49,7360	Não
411	0,6014	0,9540	0,0001	50,0057	0,0970	0,9543	0,9538	50,4070	49,6758	Não
412	0,8438	0,9540	0,0001	49,9988	0,1008	0,9544	0,9537	50,2850	49,6628	Não
413	0,7131	0,9540	0,0001	49,9983	0,0959	0,9544	0,9537	50,2819	49,6777	Não
414	0,8632	0,9540	0,0001	49,9994	0,0936	0,9544	0,9537	50,2625	49,6746	Não
415	0,7382	0,9540	0,0001	49,9955	0,0984	0,9544	0,9537	50,2979	49,6513	Não
416	0,8007	0,9540	0,0001	49,9971	0,0964	0,9544	0,9537	50,3654	49,6929	Não
417	0,8320	0,9540	0,0001	50,0029	0,1031	0,9544	0,9537	50,3040	49,6632	Não
418	0,8438	0,9540	0,0001	49,9988	0,0965	0,9544	0,9537	50,3281	49,6452	Não
419	0,9688	0,9540	0,0001	50,0005	0,1014	0,9544	0,9537	50,2953	49,6975	Não
420	0,7146	0,9540	0,0001	49,9975	0,0962	0,9544	0,9537	50,2804	49,7398	Não
421	0,8632	0,9540	0,0001	49,9971	0,0970	0,9543	0,9537	50,3902	49,7070	Não
422	0,8125	0,9540	0,0001	50,0003	0,1003	0,9544	0,9537	50,3765	49,6563	Não
423	0,8438	0,9540	0,0001	50,0023	0,1036	0,9544	0,9537	50,3258	49,6593	Não
424	0,7382	0,9540	0,0001	49,9980	0,0994	0,9544	0,9537	50,3048	49,6838	Não
425	0,8007	0,9540	0,0001	49,9981	0,0980	0,9544	0,9537	50,3033	49,7208	Não
426	0,8438	0,9540	0,0001	50,0094	0,1004	0,9543	0,9537	50,3056	49,6746	Não
427	0,8320	0,9540	0,0001	50,0012	0,1011	0,9543	0,9537	50,3250	49,6513	Não
428	0,6875	0,9471	0,0260	50,6127	1,9929	0,9544	0,6862	67,8276	49,6399	Sim
429	0,7561	0,9540	0,0002	50,0060	0,1094	0,9544	0,9498	50,7629	49,6735	Sim
430	0,7577	0,9540	0,0001	49,9981	0,0993	0,9544	0,9537	50,2785	49,6796	Não
431	0,6875	0,9540	0,0001	49,9982	0,0959	0,9544	0,9537	50,3544	49,7044	Não
432	0,8320	0,9540	0,0001	50,0069	0,1043	0,9544	0,9536	50,3120	49,6380	Não
433	0,7264	0,9540	0,0001	50,0032	0,0919	0,9544	0,9537	50,3319	49,6651	Não
434	0,8438	0,9540	0,0001	49,9947	0,0971	0,9544	0,9537	50,2895	49,7406	Não
435	0,9063	0,9540	0,0001	49,9978	0,0987	0,9544	0,9537	50,3208	49,6986	Não
436	0,8007	0,9540	0,0001	49,9954	0,0943	0,9544	0,9538	50,3422	49,7246	Não
437	0,7443	0,9540	0,0001	49,9968	0,0993	0,9544	0,9537	50,3242	49,6227	Não
438	0,8750	0,9540	0,0001	50,0004	0,0950	0,9543	0,9537	50,3403	49,6830	Não
439	0,8438	0,9540	0,0001	50,0038	0,0944	0,9545	0,9537	50,3159	49,6506	Não
440	0,8750	0,9540	0,0001	50,0001	0,0978	0,9544	0,9537	50,3109	49,6696	Não
441	0,6875	0,9143	0,0566	53,3901	4,0682	0,9543	0,6176	71,6503	49,7501	Sim
442	0,6327	0,8519	0,1113	57,4515	6,8812	0,9542	0,4067	81,8855	49,7665	Sim
443	0,7813	0,9540	0,0001	49,9986	0,0984	0,9543	0,9537	50,3242	49,6635	Não
444	0,8438	0,9540	0,0001	50,0038	0,0988	0,9544	0,9538	50,3407	49,7086	Não
445	0,8438	0,9540	0,0001	50,0049	0,0940	0,9544	0,9537	50,3433	49,6853	Não
446	0,8750	0,9540	0,0001	49,9975	0,0958	0,9543	0,9537	50,3090	49,6918	Não
447	0,8320	0,9540	0,0001	50,0007	0,1022	0,9544	0,9537	50,3731	49,6487	Não
448	0,7695	0,9540	0,0001	49,9997	0,0932	0,9544	0,9537	50,2682	49,7383	Não
449	0,8438	0,9540	0,0001	50,0018	0,0989	0,9544	0,9537	50,3494	49,6216	Não
450	0,8007	0,9540	0,0001	50,0022	0,0986	0,9544	0,9537	50,3319	49,7028	Não
451	0,8438	0,9540	0,0001	49,9994	0,1003	0,9543	0,9537	50,3162	49,6708	Não
452	0,8320	0,9540	0,0001	50,0010	0,0975	0,9544	0,9537	50,2968	49,6792	Não
453	0,8632	0,9540	0,0001	50,0001	0,0949	0,9544	0,9537	50,2956	49,7467	Não
454	0,8007	0,9540	0,0001	49,9965	0,0958	0,9544	0,9537	50,2956	49,7025	Não
455	0,7070	0,9540	0,0001	49,9972	0,1002	0,9543	0,9538	50,2872	49,7093	Não
456	0,5000	0,3166	0,1753	85,7078	8,6550	0,9263	0,0378	98,5153	52,4746	Sim
457	0,8632	0,9540	0,0001	49,9993	0,0973	0,9544	0,9537	50,3799	49,6731	Não

458	0,8320	0,9540	0,0001	50,0019	0,0963	0,9544	0,9538	50,3502	49,6330	Não
459	0,9375	0,9540	0,0001	49,9967	0,0989	0,9543	0,9537	50,2804	49,6979	Não
460	0,7577	0,9540	0,0001	50,0091	0,1011	0,9544	0,9537	50,3838	49,6883	Não
461	0,8632	0,9540	0,0001	50,0015	0,0986	0,9544	0,9537	50,3422	49,6883	Não
462	0,7695	0,9540	0,0001	50,0031	0,0993	0,9544	0,9537	50,3151	49,6765	Não
463	0,7889	0,9540	0,0001	50,0031	0,0947	0,9544	0,9537	50,3048	49,7505	Não
464	0,6716	0,9540	0,0001	50,0035	0,0978	0,9544	0,9537	50,3483	49,6887	Não
465	0,8320	0,9540	0,0001	49,9926	0,0959	0,9544	0,9537	50,3254	49,6956	Não
466	0,8438	0,9540	0,0001	49,9993	0,0974	0,9544	0,9537	50,2819	49,6445	Não
467	0,8438	0,9540	0,0001	49,9969	0,0988	0,9544	0,9537	50,3365	49,6967	Não
468	0,8632	0,9540	0,0001	50,0006	0,0981	0,9544	0,9537	50,3437	49,6578	Não
469	0,8007	0,9540	0,0001	49,9978	0,0920	0,9544	0,9537	50,2708	49,6719	Não
470	0,8750	0,9540	0,0001	49,9972	0,0965	0,9544	0,9538	50,2628	49,7189	Não
471	0,8438	0,9540	0,0001	49,9999	0,0997	0,9544	0,9537	50,3460	49,7009	Não
472	0,8007	0,9540	0,0001	50,0009	0,0987	0,9544	0,9536	50,3021	49,7002	Não
473	0,8125	0,9540	0,0001	50,0040	0,0992	0,9544	0,9537	50,2899	49,6696	Não
474	0,6929	0,9540	0,0001	50,0077	0,1025	0,9543	0,9515	50,5669	49,7059	Sim
475	0,8438	0,9540	0,0001	49,9970	0,0957	0,9544	0,9537	50,2834	49,6704	Não
476	0,8750	0,9540	0,0001	50,0044	0,1003	0,9544	0,9537	50,3365	49,6784	Não
477	0,6075	0,9114	0,0729	53,5091	5,0571	0,9544	0,4495	80,1769	49,7372	Sim
478	0,8320	0,9540	0,0001	49,9928	0,0989	0,9544	0,9537	50,3418	49,6574	Não
479	0,8632	0,9540	0,0001	50,0026	0,0990	0,9543	0,9537	50,3502	49,6712	Não
480	0,9688	0,9540	0,0001	49,9986	0,0970	0,9543	0,9538	50,3658	49,6857	Não
481	0,7561	0,9540	0,0001	49,9978	0,0952	0,9544	0,9536	50,3227	49,6849	Não
482	0,7500	0,9540	0,0001	50,0087	0,0993	0,9544	0,9538	50,3284	49,6933	Não
483	0,8320	0,9540	0,0001	50,0003	0,0948	0,9544	0,9537	50,2651	49,7093	Não
484	0,9375	0,9540	0,0001	49,9976	0,0999	0,9544	0,9537	50,2644	49,6391	Não
485	0,8438	0,9540	0,0001	50,0031	0,1011	0,9543	0,9537	50,3349	49,6384	Não
486	0,6875	0,9540	0,0003	50,0089	0,1089	0,9544	0,9485	51,1013	49,6738	Sim
487	0,8750	0,9540	0,0001	49,9941	0,0961	0,9544	0,9536	50,2808	49,6365	Não
488	0,8125	0,9540	0,0001	49,9985	0,0981	0,9543	0,9537	50,3380	49,6819	Não
489	0,9063	0,9540	0,0001	50,0035	0,0946	0,9544	0,9537	50,2621	49,7528	Não
490	0,8125	0,9540	0,0001	49,9983	0,1014	0,9544	0,9537	50,3105	49,6464	Não
491	0,8438	0,9540	0,0001	50,0001	0,0976	0,9543	0,9537	50,2884	49,7101	Não
492	0,8007	0,9540	0,0001	50,0014	0,0982	0,9543	0,9537	50,3109	49,7097	Não
493	0,7500	0,9540	0,0001	50,0018	0,1026	0,9544	0,9537	50,4017	49,7215	Não
494	0,8438	0,9540	0,0001	49,9949	0,0988	0,9544	0,9537	50,3128	49,6666	Não
495	0,8125	0,9540	0,0001	49,9991	0,0958	0,9544	0,9537	50,3292	49,7093	Não
496	0,8750	0,9540	0,0001	50,0020	0,1013	0,9544	0,9537	50,3021	49,6647	Não
497	0,8750	0,9540	0,0001	49,9989	0,0990	0,9543	0,9537	50,3517	49,6147	Não
498	0,8125	0,9540	0,0001	50,0010	0,0961	0,9544	0,9537	50,3246	49,6582	Não
499	0,8750	0,9540	0,0001	49,9949	0,0952	0,9544	0,9537	50,3284	49,7028	Não
500	0,8125	0,9540	0,0001	50,0014	0,0992	0,9544	0,9537	50,2975	49,6044	Não

Tabela B.3: Resultados para o teste com o modelo com rotação da sensitividade

Apêndice C

Resultados dos testes da seção 6.4

Este apêndice possui os resultados obtidos dos testes realizados na seção 6.4. A tabela C.1 abaixo descreve as informação de cada uma das colunas das tabelas de resultados das seções C.1 e C.2.

Coluna	Descrição da informação
A	Índice do núcleo da regra
B	Núcleo da regra com ruído
C	Entropia do núcleo da regra
D	Entropia média da imagem da diferença)
E	Desvio padrão da entropia da imagem da diferença
F	Média do percentual de zeros da imagem da diferença
G	Desvio padrão do percentual de zeros da imagem da diferença
H	Entropia máxima da imagem da diferença
I	Entropia mínima da imagem da diferença
J	Percentual de zeros máximo da imagem da diferença
K	Percentual de zeros mínimo da imagem da diferença
L	Indica que regra apresentou alguma falha de segurança

Tabela C.1: Descrição das informações das colunas da tabela de resultado

C.1 Resultados do modelo com sensitividade fixa

A	B	C	D	E	F	G	H	I	J	K	L
1	0000000000001000	0,0000	0,7797	0,0657	50,2671	1,8616	0,9133	0,4792	57,9979	44,9951	Sim
2	1110111111111111	0,0000	0,6561	0,1052	69,6719	3,8141	0,8659	0,3088	78,3279	59,0656	Sim
3	1111011100000000	0,6372	0,9540	0,0001	49,9978	0,0973	0,9544	0,9537	50,3353	49,6452	Não
4	0001000011111111	0,6372	0,9540	0,0001	49,9946	0,0980	0,9544	0,9537	50,3048	49,6773	Não
5	1000101010101010	0,2500	0,9540	0,0001	50,0011	0,0988	0,9544	0,9537	50,3384	49,6918	Não
6	0101010101010100	0,2500	0,9540	0,0001	50,0018	0,0956	0,9544	0,9537	50,3120	49,7013	Não
7	1100100011001100	0,5000	0,9540	0,0001	50,0033	0,1009	0,9544	0,9537	50,2945	49,6136	Não
8	1110001110001110	0,7264	0,9540	0,0001	50,0008	0,0988	0,9544	0,9538	50,3345	49,6956	Não
9	1111000011110001	0,7500	0,9540	0,0001	49,9985	0,1007	0,9544	0,9537	50,2636	49,6422	Não
10	0110110011010101	0,7771	0,9540	0,0001	49,9958	0,0979	0,9544	0,9537	50,3071	49,7234	Não
11	1111010010011101	0,8125	0,9540	0,0001	50,0044	0,0976	0,9543	0,9537	50,3059	49,7063	Não
12	0011001011110000	0,9063	0,9540	0,0001	49,9969	0,0943	0,9544	0,9537	50,3395	49,6925	Não
13	0001001010011001	0,8320	0,9540	0,0001	50,0004	0,0977	0,9544	0,9537	50,3239	49,6723	Não
14	1100000010000111	0,8750	0,9540	0,0001	50,0001	0,0966	0,9543	0,9537	50,3189	49,7169	Não
15	1100111001101001	0,8320	0,9540	0,0001	50,0041	0,0999	0,9544	0,9538	50,2869	49,7200	Não
16	1111011001000110	0,7771	0,9540	0,0001	49,9968	0,0948	0,9544	0,9537	50,3014	49,6525	Não

17	1110111000111001	0,7889	0,9540	0,0001	49,9994	0,0975	0,9544	0,9537	50,3490	49,5960	Não
18	0110000010100010	0,8438	0,9540	0,0001	50,0023	0,0980	0,9544	0,9537	50,2872	49,6262	Não
19	1110000010100000	0,8438	0,9540	0,0001	49,9984	0,1016	0,9544	0,9537	50,3265	49,6746	Não
20	0110111110100011	0,7459	0,9540	0,0001	50,0023	0,0976	0,9544	0,9537	50,3513	49,7292	Não
21	1001011011011110	0,8750	0,9540	0,0001	50,0022	0,0942	0,9543	0,9536	50,2861	49,6964	Não
22	1100000010001110	0,8750	0,9540	0,0001	50,0016	0,0971	0,9545	0,9536	50,3040	49,6819	Não
23	0100101101001011	0,7146	0,9540	0,0001	50,0022	0,1014	0,9543	0,9537	50,2823	49,6784	Não
24	1011011100100110	0,7695	0,9540	0,0001	50,0008	0,0981	0,9544	0,9537	50,3433	49,6952	Não
25	1101101011101101	0,7146	0,9540	0,0001	49,9945	0,0944	0,9544	0,9537	50,2850	49,7124	Não
26	0011101100001101	0,9688	0,9540	0,0001	49,9996	0,0957	0,9545	0,9537	50,2682	49,7284	Não
27	0111100010011110	0,8125	0,9540	0,0001	50,0046	0,0978	0,9544	0,9537	50,3326	49,6666	Não
28	0001101011011110	0,9375	0,9540	0,0001	50,0001	0,0950	0,9544	0,9537	50,2804	49,7108	Não
29	1011101000101001	0,8750	0,9540	0,0001	49,9962	0,0956	0,9543	0,9537	50,3319	49,6929	Não
30	1010110101101000	0,8125	0,9540	0,0001	49,9977	0,0937	0,9544	0,9536	50,2975	49,7215	Não
31	0010101000011000	0,7561	0,9540	0,0001	50,0057	0,0983	0,9543	0,9537	50,2811	49,7009	Não
32	1011111111000011	0,7873	0,9540	0,0001	49,9997	0,0964	0,9544	0,9537	50,3632	49,6864	Não
33	1101001010110011	0,8750	0,9540	0,0001	50,0060	0,0965	0,9544	0,9537	50,3323	49,6826	Não
34	1010100100100011	0,8320	0,9540	0,0001	50,0034	0,0989	0,9543	0,9537	50,3269	49,6998	Não
35	0001101011110001	0,7889	0,9540	0,0001	50,0006	0,0981	0,9544	0,9537	50,3242	49,6628	Não
36	1111001010001110	0,8186	0,9540	0,0001	49,9974	0,1001	0,9544	0,9537	50,3410	49,7200	Não
37	0000101110010101	0,8632	0,9540	0,0001	50,0038	0,0982	0,9544	0,9537	50,3204	49,6887	Não
38	1010001000001110	0,7577	0,9540	0,0001	49,9982	0,0981	0,9544	0,9538	50,3140	49,6002	Não
39	0001000000101001	0,6563	0,9540	0,0001	49,9951	0,0965	0,9544	0,9537	50,2850	49,5964	Não
40	0101001010100111	0,7695	0,9540	0,0001	49,9992	0,0993	0,9544	0,9537	50,2892	49,6994	Não
41	1100011011110101	0,8438	0,9540	0,0001	49,9994	0,0955	0,9544	0,9537	50,2949	49,6658	Não
42	0011110000110110	0,9063	0,9540	0,0001	50,0010	0,0963	0,9544	0,9537	50,2693	49,6479	Não
43	1010010011101111	0,8125	0,9540	0,0001	50,0037	0,0962	0,9544	0,9536	50,3330	49,6998	Não
44	0111101101010111	0,8320	0,9541	0,0001	50,0032	0,0975	0,9544	0,9537	50,3216	49,6635	Não
45	1011100100011011	0,8320	0,9540	0,0001	50,0001	0,0992	0,9545	0,9537	50,3059	49,6872	Não
46	1001001101001100	0,7889	0,9540	0,0001	50,0018	0,1004	0,9544	0,9538	50,2827	49,6742	Não
47	0101000000111011	0,8632	0,9540	0,0001	49,9963	0,0984	0,9543	0,9537	50,3048	49,6872	Não
48	0100001011011111	0,8632	0,9540	0,0001	50,0018	0,0999	0,9543	0,9536	50,3059	49,6696	Não
49	0000111101100001	0,9063	0,9541	0,0001	50,0033	0,0961	0,9544	0,9538	50,3098	49,6994	Não
50	0001010001100100	0,8438	0,9540	0,0001	50,0061	0,0982	0,9543	0,9537	50,3441	49,7063	Não
51	1101000111111100	0,8320	0,9540	0,0001	49,9938	0,0997	0,9544	0,9537	50,2884	49,6490	Não
52	1100010111101111	0,6875	0,9540	0,0001	49,9987	0,0947	0,9544	0,9537	50,2689	49,6902	Não
53	0111110111111101	0,5000	0,9365	0,0262	54,2098	2,5505	0,9540	0,4163	83,9394	49,4812	Sim
54	0011011000010010	0,7577	0,9540	0,0001	50,0022	0,0935	0,9543	0,9537	50,2609	49,7208	Não
55	1011001001001011	0,6757	0,9540	0,0001	49,9987	0,1003	0,9544	0,9537	50,2808	49,6647	Não
56	1111111011011000	0,8438	0,9540	0,0001	49,9974	0,0966	0,9543	0,9537	50,2762	49,6746	Não
57	1101010100100001	0,8320	0,9540	0,0001	50,0005	0,0981	0,9544	0,9537	50,4009	49,7196	Não
58	0100011010000010	0,8438	0,9540	0,0001	49,9983	0,1005	0,9543	0,9537	50,3250	49,7433	Não
59	0100111011110110	0,7873	0,9540	0,0001	49,9977	0,0936	0,9544	0,9537	50,2964	49,7421	Não
60	0000100010100000	0,6875	0,9540	0,0001	50,0006	0,0972	0,9544	0,9537	50,3807	49,7215	Não
61	1011101100101100	0,7695	0,9540	0,0001	50,0058	0,0923	0,9544	0,9537	50,3159	49,6777	Não
62	1111011101101111	0,7146	0,9540	0,0001	49,9989	0,0998	0,9544	0,9536	50,2605	49,6628	Não
63	1010001101000010	0,8007	0,9540	0,0001	49,9992	0,0990	0,9544	0,9537	50,3651	49,6700	Não
64	0001101010111110	0,8750	0,9540	0,0001	49,9962	0,1000	0,9543	0,9537	50,3033	49,6395	Não
65	1111100110100110	0,8438	0,9540	0,0001	50,0015	0,1000	0,9544	0,9537	50,3063	49,6471	Não
66	0010000000101101	0,7264	0,9540	0,0001	50,0020	0,0980	0,9543	0,9536	50,3632	49,7074	Não
67	1010011011111011	0,8438	0,9540	0,0001	49,9994	0,0985	0,9544	0,9537	50,2769	49,6704	Não
68	1110010111110101	0,8007	0,9540	0,0001	50,0031	0,0969	0,9544	0,9537	50,2872	49,6353	Não
69	0000010010000110	0,7695	0,9540	0,0001	49,9982	0,0956	0,9544	0,9537	50,2884	49,7410	Não
70	1001101101101111	0,6250	0,9540	0,0001	50,0077	0,0973	0,9543	0,9537	50,3239	49,6868	Não
71	1011101001111101	0,8438	0,9540	0,0001	49,9986	0,0995	0,9544	0,9537	50,3098	49,7154	Não
72	1101101110100000	0,7771	0,9540	0,0001	49,9941	0,0958	0,9543	0,9537	50,2533	49,6758	Não
73	1001111010101010	0,7188	0,9540	0,0001	49,9976	0,0976	0,9544	0,9536	50,3891	49,6975	Não
74	1100011010110101	0,8750	0,9540	0,0001	50,0021	0,0982	0,9544	0,9537	50,3162	49,6559	Não
75	0011100011101110	0,8125	0,9540	0,0001	50,0012	0,1019	0,9544	0,9537	50,3189	49,7082	Não
76	1111001011000000	0,8750	0,9540	0,0001	50,0003	0,0998	0,9544	0,9537	50,2735	49,6719	Não
77	1011110010111000	0,8632	0,9540	0,0001	50,0033	0,0982	0,9544	0,9537	50,3551	49,7208	Não
78	1010010110010110	0,7146	0,9540	0,0001	49,9997	0,0947	0,9544	0,9537	50,3197	49,6483	Não
79	0110001100110010	0,6952	0,9540	0,0001	49,9989	0,0986	0,9543	0,9536	50,3025	49,7494	Não
80	0001011001010110	0,8632	0,9540	0,0001	49,9931	0,0972	0,9544	0,9537	50,3059	49,7089	Não
81	0110110000011100	0,8750	0,9540	0,0001	49,9997	0,0993	0,9543	0,9537	50,2583	49,7002	Não
82	1111100101010111	0,7771	0,9540	0,0001	49,9998	0,0953	0,9544	0,9537	50,2495	49,6704	Não
83	0000011011001101	0,8945	0,9540	0,0001	50,0034	0,0997	0,9544	0,9537	50,2979	49,7055	Não
84	0001110111101100	0,9063	0,9540	0,0001	50,0038	0,0978	0,9544	0,9537	50,3292	49,6838	Não
85	1101011100111110	0,8438	0,9540	0,0001	49,9986	0,0976	0,9543	0,9537	50,3033	49,7223	Não
86	1001001101010100	0,8320	0,9540	0,0001	49,9993	0,0962	0,9544	0,9537	50,3284	49,6784	Não
87	1111011110001101	0,8438	0,9540	0,0001	50,0010	0,0948	0,9544	0,9537	50,3830	49,7414	Não
88	1100000001101110	0,7873	0,9540	0,0001	49,9967	0,0942	0,9544	0,9538	50,2792	49,6693	Não
89	1011111100111010	0,8320	0,9540	0,0001	50,0091	0,1031	0,9544	0,9537	50,3387	49,6975	Não
90	0010010010111000	0,8320	0,9540	0,0001	49,9989	0,0939	0,9544	0,9537	50,3132	49,6822	Não
91	1100100001101101	0,8750	0,9540	0,0001	50,0021	0,0951	0,9544	0,9537	50,2972	49,6704	Não
92	0001001011000010	0,6250	0,9540	0,0001	49,9999	0,0962	0,9544	0,9537	50,2739	49,7097	Não
93	0110011010110001	0,7146	0,9540	0,0001	49,9987	0,0995	0,9544	0,9537	50,2953	49,6597	Não
94	1101100110111110	0,8320	0,9540	0,0001	50,0046	0,0976	0,9543	0,9537	50,3174	49,7093	Não
95	1001011101001111	0,8750	0,9540	0,0001	50,0003	0,0962	0,9544	0,9537	50,3189	49,7459	Não
96	0101111000010001	0,8750	0,9540	0,0001	50,0023	0,0977	0,9543	0,9537	50,2945	49,7276	Não

97	0100111011111110	0,7382	0,9540	0,0001	50,0004	0,0984	0,9544	0,9538	50,2846	49,6853	Não
98	0100111011000011	0,8750	0,9540	0,0001	49,9940	0,0979	0,9543	0,9537	50,2922	49,5865	Não
99	0111010100001111	0,8750	0,9540	0,0001	49,9964	0,0947	0,9544	0,9537	50,2998	49,7116	Não
100	1100010001011000	0,8125	0,9540	0,0001	50,0012	0,0973	0,9544	0,9537	50,2541	49,6510	Não
101	0011010110011111	0,8320	0,9540	0,0001	50,0053	0,0959	0,9544	0,9537	50,3414	49,7246	Não
102	0100001110001011	0,8632	0,9540	0,0001	49,9977	0,0983	0,9545	0,9537	50,3185	49,6811	Não
103	0101000110001110	0,8438	0,9540	0,0001	50,0044	0,1004	0,9544	0,9538	50,2609	49,7135	Não
104	0100010101110011	0,8438	0,9540	0,0001	50,0008	0,0989	0,9544	0,9538	50,3098	49,6834	Não
105	0011010001001001	0,7146	0,9540	0,0001	49,9965	0,0962	0,9543	0,9537	50,2846	49,6769	Não
106	0111011101101110	0,7500	0,9540	0,0001	50,0057	0,0962	0,9543	0,9537	50,3082	49,7135	Não
107	1001110010000000	0,8438	0,9540	0,0001	50,0036	0,0958	0,9544	0,9537	50,2972	49,6727	Não
108	1111001000010101	0,8007	0,9540	0,0001	50,0051	0,0978	0,9544	0,9536	50,2689	49,6925	Não
109	1111111101111100	0,4054	0,9540	0,0001	49,9950	0,0952	0,9544	0,9537	50,3265	49,6964	Não
110	1010011010110110	0,8632	0,9540	0,0001	50,0009	0,0974	0,9544	0,9537	50,2934	49,6925	Não
111	0111110001001000	0,8320	0,9540	0,0001	50,0004	0,0962	0,9544	0,9537	50,3654	49,6906	Não
112	1111110011000100	0,8007	0,9540	0,0001	49,9973	0,1016	0,9543	0,9537	50,2815	49,7082	Não
113	1100010110111000	0,8007	0,9540	0,0001	49,9994	0,1008	0,9544	0,9537	50,4185	49,7242	Não
114	0011011101110010	0,8750	0,9540	0,0001	50,0003	0,0990	0,9544	0,9537	50,2796	49,7280	Não
115	0000111001001100	0,7695	0,9540	0,0001	49,9979	0,1001	0,9544	0,9538	50,3181	49,6483	Não
116	0111001101001011	0,7771	0,9540	0,0001	49,9999	0,0995	0,9543	0,9538	50,2487	49,7040	Não
117	1010110011100100	0,8438	0,9540	0,0001	49,9996	0,0958	0,9544	0,9537	50,2876	49,7334	Não
118	1000010000001101	0,7264	0,9540	0,0001	50,0039	0,0995	0,9544	0,9537	50,3868	49,6899	Não
119	1100001011011001	0,8750	0,9540	0,0001	50,0014	0,0986	0,9543	0,9537	50,2701	49,6685	Não
120	0011101011001000	0,9063	0,9540	0,0001	50,0003	0,0947	0,9545	0,9537	50,2842	49,7108	Não
121	1101110101100110	0,8320	0,9540	0,0001	49,9998	0,0973	0,9545	0,9537	50,2853	49,6098	Não
122	0001100111101100	0,7577	0,9540	0,0001	50,0038	0,0955	0,9544	0,9537	50,3166	49,6254	Não
123	1110001111010000	0,8750	0,9540	0,0001	50,0006	0,0998	0,9544	0,9537	50,3265	49,6944	Não
124	0110011010111001	0,8320	0,9540	0,0001	49,9972	0,0953	0,9544	0,9537	50,3250	49,6696	Não
125	1010100000111111	0,9063	0,9540	0,0001	49,9960	0,0952	0,9544	0,9537	50,3033	49,6723	Não
126	1101010000101011	0,7500	0,9540	0,0001	49,9967	0,0938	0,9544	0,9537	50,3330	49,6796	Não
127	0100000110101001	0,9063	0,9540	0,0001	49,9946	0,0985	0,9543	0,9537	50,3487	49,7086	Não
128	1000010001010001	0,8438	0,9540	0,0001	50,0032	0,0952	0,9545	0,9537	50,3189	49,6914	Não
129	0111001011000001	0,8320	0,9540	0,0001	49,9996	0,0926	0,9544	0,9537	50,3403	49,6933	Não
130	1011100001000101	0,9063	0,9541	0,0001	49,9970	0,0964	0,9544	0,9537	50,3185	49,6906	Não
131	1100011111011001	0,8750	0,9540	0,0001	50,0010	0,0933	0,9544	0,9537	50,2876	49,6883	Não
132	1101100011111110	0,8438	0,9540	0,0001	49,9977	0,0956	0,9544	0,9537	50,3281	49,6967	Não
133	0010111101111010	0,8438	0,9540	0,0001	50,0048	0,0998	0,9544	0,9536	50,2701	49,6246	Não
134	1101110000101011	0,8007	0,9540	0,0001	50,0048	0,0982	0,9543	0,9537	50,2831	49,6468	Não
135	0111000100000100	0,8438	0,9540	0,0001	50,0054	0,0921	0,9544	0,9536	50,3040	49,7028	Não
136	0101011000101111	0,8438	0,9540	0,0001	49,9996	0,0964	0,9544	0,9537	50,3048	49,5865	Não
137	1110101000010100	0,8750	0,9540	0,0001	50,0037	0,0988	0,9544	0,9537	50,3582	49,7162	Não
138	0110100101000010	0,7146	0,9540	0,0001	50,0060	0,0979	0,9544	0,9537	50,3414	49,7116	Não
139	0000001101000100	0,7131	0,9540	0,0001	49,9957	0,1000	0,9544	0,9537	50,2903	49,6849	Não
140	1110111100001101	0,8438	0,9540	0,0001	49,9986	0,0964	0,9544	0,9537	50,2808	49,6834	Não
141	0001011010101010	0,8007	0,9540	0,0001	50,0000	0,0968	0,9544	0,9537	50,3323	49,7028	Não
142	1100111011111100	0,7500	0,9540	0,0001	49,9970	0,1005	0,9544	0,9537	50,2735	49,6635	Não
143	0110100000011010	0,8320	0,9540	0,0001	50,0071	0,0979	0,9544	0,9537	50,2888	49,6716	Não
144	1011101000111111	0,8320	0,9540	0,0001	50,0004	0,0998	0,9543	0,9537	50,2842	49,6487	Não
145	0010100110101011	0,8438	0,9540	0,0001	49,9976	0,0979	0,9543	0,9537	50,3403	49,7154	Não
146	0100111001110000	0,7577	0,9540	0,0001	50,0027	0,0998	0,9544	0,9537	50,2922	49,7379	Não
147	0010111101100100	0,8750	0,9540	0,0001	50,0039	0,0995	0,9544	0,9537	50,2930	49,6803	Não
148	0010011001010001	0,8320	0,9540	0,0001	49,9989	0,0991	0,9544	0,9538	50,3559	49,6986	Não
149	0111111010011111	0,6304	0,9540	0,0001	50,0010	0,0974	0,9543	0,9535	50,3273	49,6964	Não
150	0000101010110000	0,7248	0,9540	0,0001	49,9995	0,0973	0,9544	0,9537	50,3159	49,6571	Não
151	1100000011100111	0,7813	0,9540	0,0001	49,9991	0,0927	0,9544	0,9537	50,3334	49,7303	Não
152	1111100111001101	0,8320	0,9540	0,0001	49,9993	0,0975	0,9544	0,9537	50,2842	49,7112	Não
153	0100111010101011	0,8007	0,9540	0,0001	50,0020	0,0933	0,9544	0,9537	50,3117	49,7055	Não
154	1000011100111000	0,8438	0,9540	0,0001	49,9929	0,0942	0,9544	0,9537	50,3140	49,6490	Não
155	0100111111100010	0,8438	0,9540	0,0001	50,0001	0,1002	0,9544	0,9537	50,3319	49,5983	Não
156	1101000011001110	0,8750	0,9540	0,0001	50,0042	0,0989	0,9544	0,9537	50,3574	49,6990	Não
157	1110011111000010	0,8320	0,9540	0,0001	49,9970	0,0987	0,9544	0,9537	50,3277	49,6262	Não
158	1100111101110001	0,6936	0,9540	0,0001	49,9982	0,0956	0,9544	0,9538	50,2781	49,6498	Não
159	0000001100010000	0,5992	0,9540	0,0001	49,9964	0,1008	0,9544	0,9537	50,3304	49,6624	Não
160	1010111001110000	0,8750	0,9540	0,0001	50,0076	0,1003	0,9544	0,9536	50,3494	49,6704	Não
161	0010010011101011	0,9688	0,9540	0,0001	49,9975	0,0991	0,9544	0,9537	50,3281	49,6712	Não
162	0100101110111100	0,8750	0,9540	0,0001	50,0044	0,0975	0,9544	0,9537	50,2781	49,6437	Não
163	0000110000001101	0,8750	0,9540	0,0001	50,0061	0,1001	0,9544	0,9537	50,3052	49,5811	Não
164	0011110000110000	0,8945	0,9540	0,0001	49,9996	0,1002	0,9543	0,9537	50,4314	49,7337	Não
165	0110100011101011	0,8632	0,9540	0,0001	50,0016	0,0991	0,9544	0,9537	50,3281	49,6479	Não
166	0111011111100010	0,7695	0,9540	0,0001	50,0063	0,0969	0,9544	0,9537	50,3510	49,6162	Não
167	0010101011111011	0,7146	0,9540	0,0001	50,0024	0,0985	0,9544	0,9537	50,3937	49,6986	Não
168	0001010100110111	0,9063	0,9540	0,0001	50,0019	0,0970	0,9545	0,9537	50,3410	49,6475	Não
169	1111000010010001	0,8438	0,9540	0,0001	50,0021	0,0992	0,9545	0,9538	50,3708	49,7158	Não
170	1000110111010101	0,8632	0,9540	0,0001	50,0042	0,0982	0,9543	0,9536	50,3204	49,7143	Não
171	0101011101001001	0,5434	0,9540	0,0001	50,0046	0,0973	0,9544	0,9537	50,3223	49,6586	Não
172	1010110011111100	0,7695	0,9540	0,0001	49,9984	0,1004	0,9544	0,9537	50,2953	49,6849	Não
173	0111000101010110	0,8125	0,9540	0,0001	50,0015	0,0983	0,9544	0,9538	50,2651	49,6529	Não
174	1010001001111111	0,7813	0,9540	0,0001	50,0015	0,0968	0,9543	0,9537	50,3101	49,6662	Não
175	0110000110111011	0,8438	0,9540	0,0001	49,9972	0,0976	0,9544	0,9537	50,2544	49,6613	Não
176	0111111111110010	0,7813	0,9540	0,0001	49,9944	0,0983	0,9544	0,9537	50,2785	49,6841	Não

177	0101100000011100	0,8320	0,9540	0,0001	49,9990	0,0955	0,9544	0,9536	50,3407	49,7044	Não
178	0000000011101001	0,8320	0,9540	0,0001	50,0033	0,1001	0,9544	0,9537	50,4360	49,6475	Não
179	1110101111101111	0,7248	0,9540	0,0001	50,0010	0,0973	0,9544	0,9537	50,3071	49,6887	Não
180	0100001111011101	0,8750	0,9540	0,0001	49,9978	0,0974	0,9544	0,9537	50,2800	49,7402	Não
181	1100111100101111	0,7561	0,9540	0,0001	50,0026	0,0974	0,9544	0,9537	50,2762	49,6677	Não
182	1101001010010111	0,8438	0,9540	0,0001	49,9990	0,0948	0,9544	0,9537	50,2926	49,6613	Não
183	1100010001010110	0,8320	0,9540	0,0001	50,0025	0,0957	0,9544	0,9537	50,2903	49,6460	Não
184	1111011000100001	0,9375	0,9540	0,0001	49,9977	0,0975	0,9544	0,9537	50,2842	49,6998	Não
185	1101110011100101	0,8750	0,9540	0,0001	49,9992	0,0970	0,9544	0,9537	50,3048	49,6983	Não
186	0010110111011011	0,7771	0,9540	0,0001	49,9958	0,1003	0,9544	0,9537	50,3025	49,6628	Não
187	1000101011000000	0,8125	0,9540	0,0001	49,9981	0,1001	0,9544	0,9537	50,3719	49,6876	Não
188	1100010100000011	0,7561	0,9540	0,0001	50,0025	0,0970	0,9544	0,9536	50,3147	49,7040	Não
189	1011011010011111	0,8202	0,9540	0,0001	49,9949	0,0969	0,9543	0,9537	50,2693	49,6670	Não
190	0101110001101011	0,8320	0,9540	0,0001	50,0022	0,0938	0,9544	0,9537	50,2899	49,7128	Não
191	1101101110101100	0,7070	0,9540	0,0001	50,0001	0,0970	0,9543	0,9537	50,2914	49,6746	Não
192	1010111011001010	0,8125	0,9540	0,0001	50,0038	0,0956	0,9544	0,9537	50,3990	49,6696	Não
193	0110001110101001	0,8750	0,9540	0,0001	50,0016	0,0975	0,9544	0,9537	50,3037	49,7215	Não
194	0110011100100101	0,8438	0,9540	0,0001	50,0006	0,0942	0,9544	0,9536	50,4181	49,6666	Não
195	1010011100100111	0,6875	0,9540	0,0001	49,9971	0,0995	0,9544	0,9536	50,3963	49,6990	Não
196	0001100000110111	0,7264	0,9540	0,0001	50,0012	0,0969	0,9544	0,9537	50,2926	49,7166	Não
197	0111101111000111	0,7146	0,9540	0,0001	49,9970	0,0951	0,9544	0,9537	50,2647	49,7231	Não
198	1010010111101000	0,8750	0,9541	0,0001	50,0016	0,0979	0,9544	0,9537	50,3155	49,6849	Não
199	1100000011111101	0,8632	0,9540	0,0001	50,0002	0,0977	0,9544	0,9537	50,2670	49,7166	Não
200	1110111010001001	0,9063	0,9540	0,0001	49,9984	0,1021	0,9544	0,9537	50,3414	49,5483	Não
201	0101110110101110	0,8438	0,9540	0,0001	49,9985	0,1013	0,9543	0,9538	50,3048	49,6471	Não
202	0010111000011111	0,8750	0,9540	0,0001	50,0006	0,0962	0,9544	0,9537	50,3037	49,6574	Não
203	1110111011111111	0,5778	0,8927	0,0885	55,8370	3,8095	0,9541	0,4432	69,1662	49,7753	Sim
204	1001010111101111	0,8320	0,9540	0,0001	49,9969	0,1004	0,9544	0,9537	50,3529	49,6750	Não
205	0110100011011101	0,9063	0,9540	0,0001	50,0019	0,1000	0,9544	0,9537	50,2930	49,6780	Não
206	0110111010011111	0,8438	0,9541	0,0001	49,9938	0,0958	0,9544	0,9537	50,2743	49,6761	Não
207	1110111110010010	0,8438	0,9540	0,0001	49,9971	0,1013	0,9544	0,9537	50,3567	49,6330	Não
208	1110011001011100	0,8438	0,9540	0,0001	50,0018	0,1004	0,9544	0,9537	50,3540	49,6960	Não
209	0001000100100100	0,8007	0,9540	0,0001	49,9965	0,0965	0,9544	0,9537	50,2831	49,7208	Não
210	0001011001001101	0,9063	0,9540	0,0001	50,0013	0,0958	0,9544	0,9537	50,3712	49,7204	Não
211	1100100100011100	0,7577	0,9540	0,0001	49,9991	0,0971	0,9544	0,9537	50,3014	49,6880	Não
212	0100000000101101	0,6617	0,9540	0,0001	50,0028	0,0980	0,9543	0,9537	50,3445	49,6632	Não
213	0010111000100110	0,8750	0,9540	0,0001	49,9972	0,0950	0,9544	0,9537	50,2869	49,7307	Não
214	0000000010010000	0,3278	0,9373	0,0172	50,0145	0,1862	0,9542	0,8660	50,9892	49,1924	Sim
215	0000100010011000	0,7500	0,9540	0,0001	50,0023	0,1024	0,9544	0,9536	50,3338	49,6460	Não
216	0100011111011000	0,9063	0,9540	0,0001	49,9982	0,0950	0,9544	0,9537	50,3094	49,6910	Não
217	0000110101011010	0,9063	0,9540	0,0001	49,9984	0,0963	0,9544	0,9537	50,3254	49,6845	Não
218	0111001110101001	0,8320	0,9540	0,0001	49,9984	0,1011	0,9544	0,9537	50,2655	49,6113	Não
219	1011000101110001	0,8750	0,9540	0,0001	50,0046	0,0954	0,9544	0,9537	50,3132	49,6826	Não
220	1000000110010100	0,7577	0,9540	0,0001	50,0027	0,0973	0,9544	0,9537	50,3098	49,7200	Não
221	0001110010110101	0,8438	0,9540	0,0001	49,9966	0,0956	0,9544	0,9537	50,2686	49,6887	Não
222	0101100001011110	0,9063	0,9540	0,0001	49,9984	0,0980	0,9544	0,9537	50,3056	49,7414	Não
223	1011000001110101	0,8320	0,9540	0,0001	49,9990	0,0974	0,9544	0,9537	50,3231	49,7162	Não
224	1111011001100011	0,9063	0,9540	0,0001	49,9960	0,0999	0,9543	0,9537	50,3258	49,6574	Não
225	0100111100101000	0,8438	0,9540	0,0001	49,9955	0,0980	0,9543	0,9537	50,3960	49,6964	Não
226	1011010011111001	0,8007	0,9540	0,0001	49,9938	0,0993	0,9544	0,9537	50,2537	49,6002	Não
227	0101000101100101	0,9063	0,9540	0,0001	50,0038	0,0956	0,9544	0,9537	50,2785	49,7200	Não
228	0101010101010100	0,6250	0,9540	0,0001	50,0038	0,1004	0,9543	0,9537	50,3830	49,6876	Não
229	0110100011110100	0,9063	0,9540	0,0001	50,0021	0,0987	0,9544	0,9536	50,3677	49,6346	Não
230	0001011010000010	0,8320	0,9540	0,0001	50,0011	0,0969	0,9543	0,9536	50,2964	49,7032	Não
231	0010100011001010	0,8007	0,9540	0,0001	50,0022	0,0974	0,9543	0,9537	50,3830	49,7288	Não
232	1001011111111000	0,9063	0,9540	0,0001	49,9951	0,0949	0,9544	0,9537	50,2861	49,6655	Não
233	0011100110000001	0,8632	0,9540	0,0001	50,0061	0,0948	0,9544	0,9537	50,2804	49,6826	Não
234	0010100011101000	0,8007	0,9540	0,0001	49,9956	0,0990	0,9544	0,9538	50,3101	49,7070	Não
235	0100000111111101	0,7695	0,9540	0,0001	50,0032	0,0968	0,9543	0,9537	50,3078	49,6925	Não
236	1100000101110001	0,6875	0,9540	0,0001	50,0034	0,0947	0,9544	0,9538	50,2892	49,7154	Não
237	1110100110111001	0,7695	0,9540	0,0001	50,0001	0,0972	0,9544	0,9537	50,3330	49,6857	Não
238	1111101001010000	0,8750	0,9540	0,0001	50,0065	0,0986	0,9544	0,9537	50,3189	49,6876	Não
239	0010111101101010	0,9063	0,9540	0,0001	49,9997	0,0965	0,9544	0,9537	50,2975	49,6758	Não
240	0000111001101000	0,6952	0,9540	0,0001	50,0023	0,0964	0,9543	0,9537	50,3044	49,6948	Não
241	0000001101001011	0,8945	0,9540	0,0001	50,0036	0,0996	0,9544	0,9536	50,3326	49,6437	Não
242	0000101100110001	0,7561	0,9540	0,0001	49,9956	0,1018	0,9544	0,9537	50,3242	49,6311	Não
243	1011110011110011	0,7146	0,9540	0,0001	49,9984	0,0979	0,9543	0,9537	50,2831	49,6937	Não
244	0110110110000111	0,7771	0,9540	0,0001	49,9986	0,1001	0,9544	0,9537	50,2758	49,6681	Não
245	0101110101100011	0,8750	0,9540	0,0001	50,0039	0,0941	0,9544	0,9537	50,3265	49,7032	Não
246	1010111110111001	0,8320	0,9540	0,0001	50,0030	0,0986	0,9544	0,9537	50,3242	49,6151	Não
247	0011010101111010	0,6875	0,9540	0,0001	49,9982	0,1033	0,9543	0,9537	50,2922	49,6807	Não
248	0011101001000010	0,8320	0,9540	0,0001	49,9974	0,0978	0,9544	0,9537	50,3178	49,7158	Não
249	1110101010100111	0,7695	0,9540	0,0001	50,0027	0,0962	0,9543	0,9537	50,3162	49,6868	Não
250	0110100000100111	0,8438	0,9540	0,0001	49,9982	0,0990	0,9544	0,9537	50,2609	49,6391	Não
251	1100001011001011	0,8632	0,9540	0,0001	50,0089	0,0939	0,9544	0,9537	50,3635	49,7341	Não
252	1011100110110110	0,8320	0,9540	0,0001	49,9950	0,0994	0,9544	0,9537	50,3101	49,6838	Não
253	1001000001000011	0,8632	0,9540	0,0001	50,0000	0,0953	0,9544	0,9538	50,2979	49,6601	Não
254	0110001101110110	0,7771	0,9540	0,0001	49,9988	0,0970	0,9544	0,9537	50,2964	49,6536	Não
255	0111000000011100	0,8125	0,9540	0,0001	49,9977	0,0997	0,9543	0,9538	50,2708	49,6326	Não
256	1110111100000111	0,8632	0,9540	0,0001	50,0028	0,0982	0,9544	0,9537	50,3262	49,6342	Não

257	1000001100000001	0,6936	0,9540	0,0001	50,0032	0,0957	0,9543	0,9537	50,3796	49,7017	Não
258	0110111100000101	0,8438	0,9540	0,0001	50,0010	0,1004	0,9543	0,9537	50,3071	49,6922	Não
259	1100100100101101	0,8007	0,9540	0,0001	50,0032	0,0966	0,9544	0,9537	50,3208	49,6731	Não
260	1010101011110010	0,8007	0,9540	0,0001	50,0030	0,0956	0,9543	0,9536	50,3376	49,6937	Não
261	0000111100011110	0,7382	0,9540	0,0001	50,0039	0,0993	0,9544	0,9537	50,3551	49,7177	Não
262	0000111101001101	0,9063	0,9540	0,0001	49,9990	0,0938	0,9544	0,9537	50,3597	49,6853	Não
263	0001010111110010	0,8750	0,9540	0,0001	49,9971	0,0956	0,9543	0,9537	50,2838	49,7047	Não
264	1101011101111110	0,7264	0,9540	0,0001	50,0020	0,0947	0,9544	0,9537	50,3384	49,7040	Não
265	1001001110100011	0,8125	0,9540	0,0001	49,9984	0,0997	0,9544	0,9536	50,3422	49,6750	Não
266	1011110010101101	0,7146	0,9540	0,0001	50,0022	0,0978	0,9544	0,9537	50,3353	49,6189	Não
267	0000011110110100	0,9063	0,9540	0,0001	50,0009	0,0957	0,9544	0,9537	50,3044	49,6410	Não
268	1100110100001001	0,9375	0,9540	0,0001	49,9979	0,0972	0,9544	0,9537	50,2926	49,7158	Não
269	0111000001101010	0,8320	0,9540	0,0001	50,0002	0,0972	0,9545	0,9537	50,3582	49,7009	Não
270	0011100100101000	0,9063	0,9540	0,0001	49,9991	0,0959	0,9544	0,9537	50,3860	49,6895	Não
271	1110110110011101	0,8438	0,9540	0,0001	49,9953	0,0953	0,9544	0,9537	50,3006	49,7337	Não
272	0011011000011111	0,9063	0,9540	0,0001	49,9961	0,0996	0,9543	0,9537	50,3185	49,6651	Não
273	0111110111101010	0,8320	0,9540	0,0001	49,9991	0,0974	0,9544	0,9537	50,3071	49,6613	Não
274	1110100110101100	0,8320	0,9540	0,0001	49,9982	0,0971	0,9544	0,9537	50,3609	49,6681	Não
275	0001100011001101	0,8320	0,9540	0,0001	49,9967	0,0960	0,9543	0,9537	50,2724	49,6853	Não
276	1000001111100101	0,8438	0,9540	0,0001	49,9954	0,0993	0,9544	0,9537	50,3193	49,6727	Não
277	0110111100110101	0,8750	0,9540	0,0001	50,0009	0,0989	0,9543	0,9537	50,2934	49,6632	Não
278	1101100111010000	0,8125	0,9540	0,0001	49,9952	0,0970	0,9544	0,9537	50,3365	49,6929	Não
279	1011110011001100	0,9063	0,9540	0,0001	50,0020	0,0981	0,9544	0,9537	50,3395	49,7051	Não
280	1001000011000110	0,7500	0,9540	0,0001	50,0034	0,0935	0,9544	0,9536	50,3334	49,7086	Não
281	1010000101001010	0,7500	0,9540	0,0001	49,9950	0,0991	0,9544	0,9537	50,3014	49,6506	Não
282	0001011111101100	0,8007	0,9540	0,0001	49,9993	0,0970	0,9544	0,9537	50,3033	49,7410	Não
283	1110010110100110	0,8438	0,9540	0,0001	50,0012	0,0970	0,9544	0,9537	50,2899	49,6864	Não
284	1011101010101010	0,6250	0,9540	0,0001	50,0507	0,1351	0,9544	0,9537	51,0147	49,6914	Sim
285	1101010000001111	0,8125	0,9540	0,0001	50,0017	0,0974	0,9545	0,9537	50,3464	49,7131	Não
286	1110101011101101	0,8438	0,9540	0,0001	49,9938	0,0976	0,9543	0,9537	50,2914	49,7116	Não
287	0110111000111110	0,8007	0,9540	0,0001	50,0038	0,1005	0,9544	0,9537	50,3414	49,7311	Não
288	1010110000101100	0,8320	0,9540	0,0001	49,9975	0,0964	0,9543	0,9537	50,3250	49,7074	Não
289	1011000110000011	0,8750	0,9540	0,0001	50,0048	0,1029	0,9543	0,9537	50,2922	49,6983	Não
290	1001111101111101	0,8007	0,9540	0,0001	49,9966	0,0984	0,9544	0,9537	50,2792	49,6792	Não
291	0011010000001010	0,8007	0,9540	0,0001	50,0011	0,0949	0,9544	0,9537	50,3185	49,7025	Não
292	1010011111011111	0,8007	0,9540	0,0001	49,9989	0,0975	0,9544	0,9537	50,3548	49,7143	Não
293	0010100111001000	0,8125	0,9540	0,0001	49,9997	0,0986	0,9543	0,9537	50,2987	49,7295	Não
294	1000111011100101	0,7577	0,9540	0,0001	50,0044	0,0942	0,9544	0,9538	50,3281	49,7116	Não
295	1100010011011010	0,8438	0,9540	0,0001	49,9999	0,0953	0,9543	0,9537	50,3105	49,7150	Não
296	1011100010110001	0,8750	0,9540	0,0001	50,0034	0,0954	0,9544	0,9537	50,3239	49,6582	Não
297	0111100010100001	0,9063	0,9540	0,0001	50,0023	0,0974	0,9544	0,9537	50,2697	49,6925	Não
298	0001010111100000	0,7264	0,9540	0,0001	50,0033	0,0952	0,9544	0,9537	50,3124	49,7292	Não
299	1100000100101110	0,7873	0,9540	0,0001	50,0057	0,0965	0,9544	0,9537	50,3098	49,6899	Não
300	1101000010111010	0,8750	0,9540	0,0001	49,9940	0,0947	0,9543	0,9538	50,2781	49,6967	Não
301	0111111010101101	0,6875	0,9540	0,0001	50,0032	0,0963	0,9544	0,9537	50,3529	49,6468	Não
302	1110101011100010	0,8438	0,9540	0,0001	49,9931	0,0941	0,9544	0,9536	50,3231	49,7051	Não
303	1011100101101110	0,8007	0,9540	0,0001	49,9994	0,0985	0,9544	0,9537	50,2911	49,6895	Não
304	1001010000110101	1,0000	0,9540	0,0001	50,0046	0,1016	0,9544	0,9537	50,3273	49,6922	Não
305	1001011010110110	0,7889	0,9540	0,0001	50,0010	0,0968	0,9544	0,9537	50,2964	49,6887	Não
306	0101111111001100	0,9063	0,9540	0,0001	50,0034	0,0994	0,9544	0,9537	50,3052	49,7025	Não
307	0011111010011111	0,8438	0,9540	0,0001	50,0011	0,0992	0,9544	0,9537	50,3323	49,6647	Não
308	1100001011110010	0,8750	0,9540	0,0001	50,0006	0,1005	0,9544	0,9537	50,2853	49,7070	Não
309	0001110101001011	0,8750	0,9540	0,0001	50,0011	0,0977	0,9544	0,9538	50,2903	49,6769	Não
310	1011000111111111	0,6250	0,9540	0,0001	50,0012	0,0939	0,9544	0,9537	50,2590	49,7028	Não
311	1110010110100101	0,7500	0,9540	0,0001	50,0016	0,0944	0,9544	0,9537	50,2850	49,7070	Não
312	1111010000111011	0,8750	0,9540	0,0001	49,9992	0,0975	0,9544	0,9537	50,2590	49,6902	Não
313	0110101100001001	0,7889	0,9540	0,0001	49,9999	0,0994	0,9544	0,9537	50,3075	49,6727	Não
314	1001010001111110	0,9063	0,9540	0,0001	49,9989	0,1001	0,9544	0,9537	50,3044	49,6990	Não
315	1001001101100000	0,8320	0,9540	0,0001	49,9987	0,1006	0,9545	0,9537	50,3124	49,7288	Não
316	0001010111011001	0,8438	0,9540	0,0001	49,9934	0,0961	0,9543	0,9537	50,2762	49,6483	Não
317	0000011010010011	0,9688	0,9540	0,0001	50,0005	0,0990	0,9544	0,9537	50,2869	49,6143	Não
318	1000101111011101	0,8750	0,9540	0,0001	50,0000	0,0944	0,9544	0,9537	50,3345	49,6941	Não
319	0001001011111001	0,7771	0,9540	0,0001	50,0007	0,0954	0,9543	0,9537	50,3395	49,5949	Não
320	0001101001001011	0,8632	0,9540	0,0001	50,0046	0,0969	0,9544	0,9537	50,3479	49,7044	Não
321	1111111100011111	0,6929	0,9540	0,0001	50,0016	0,1009	0,9545	0,9538	50,3475	49,6559	Não
322	1111101111110110	0,4917	0,9540	0,0001	50,0014	0,0997	0,9544	0,9537	50,3063	49,7108	Não
323	1100111001100010	0,8438	0,9540	0,0001	50,0036	0,1000	0,9544	0,9538	50,3590	49,6727	Não
324	1011101010000001	0,9063	0,9540	0,0001	50,0011	0,0958	0,9544	0,9537	50,3410	49,6529	Não
325	0011011001001001	0,7577	0,9540	0,0001	49,9998	0,0978	0,9544	0,9537	50,2846	49,6765	Não
326	1011101110001101	0,8438	0,9541	0,0001	50,0011	0,0940	0,9544	0,9537	50,3063	49,6964	Não
327	0100100000100110	0,7695	0,9540	0,0001	49,9992	0,0995	0,9543	0,9536	50,3311	49,6895	Não
328	0001111110101001	0,8632	0,9540	0,0001	49,9973	0,0954	0,9543	0,9537	50,3639	49,7276	Não
329	1001010010001101	0,8320	0,9540	0,0001	49,9984	0,0957	0,9544	0,9537	50,2735	49,6971	Não
330	1111101100101101	0,8320	0,9540	0,0001	49,9961	0,0994	0,9543	0,9537	50,3475	49,6132	Não
331	0011010001101101	0,6757	0,9540	0,0001	49,9972	0,0953	0,9543	0,9537	50,3662	49,6948	Não
332	1011100001101001	0,9063	0,9540	0,0001	50,0041	0,0960	0,9543	0,9537	50,3498	49,7185	Não
333	0011011100001101	0,9063	0,9540	0,0001	50,0019	0,0975	0,9543	0,9537	50,3281	49,6944	Não
334	0101000001001001	0,8320	0,9540	0,0001	50,0008	0,0950	0,9544	0,9536	50,2785	49,6376	Não
335	0100101011001010	0,8320	0,9541	0,0001	50,0011	0,0987	0,9545	0,9537	50,3189	49,6731	Não
336	1111001000101100	0,8750	0,9540	0,0001	49,9997	0,0985	0,9544	0,9537	50,3288	49,6506	Não

337	1110000000000110	0,5938	0,9540	0,0001	50,0029	0,1001	0,9544	0,9537	50,2987	49,5846	Não
338	1010100100111111	0,7889	0,9540	0,0001	49,9992	0,0979	0,9543	0,9537	50,2758	49,7421	Não
339	1000000011010110	0,8632	0,9540	0,0001	49,9995	0,0998	0,9544	0,9537	50,3551	49,6719	Não
340	0101000111011100	0,9375	0,9540	0,0001	49,9995	0,0943	0,9544	0,9537	50,2888	49,7063	Não
341	0100001011111111	0,6929	0,9540	0,0001	50,0012	0,0980	0,9543	0,9537	50,3403	49,6948	Não
342	1000111011101001	0,8750	0,9540	0,0001	49,9966	0,0975	0,9545	0,9537	50,2773	49,7009	Não
343	1101100000001101	0,7873	0,9540	0,0001	49,9988	0,0966	0,9544	0,9537	50,3498	49,7177	Não
344	1110001100100000	0,8007	0,9540	0,0001	49,9926	0,0971	0,9543	0,9537	50,3197	49,6925	Não
345	1101001001000100	0,6563	0,9540	0,0001	50,0020	0,0991	0,9544	0,9536	50,3521	49,7116	Não
346	1001100111110010	0,8438	0,9540	0,0001	50,0053	0,1013	0,9544	0,9537	50,3544	49,5728	Não
347	0011101111010111	0,6716	0,9540	0,0001	50,0023	0,0985	0,9544	0,9537	50,3071	49,6841	Não
348	1101010001100000	0,7889	0,9540	0,0001	50,0013	0,0961	0,9544	0,9537	50,3181	49,7234	Não
349	1000000111000000	0,6304	0,9540	0,0001	49,9934	0,0946	0,9544	0,9537	50,3120	49,7158	Não
350	0111001010011110	0,8438	0,9540	0,0001	50,0023	0,0958	0,9544	0,9537	50,2766	49,6861	Não
351	0011000110111010	0,8750	0,9540	0,0001	50,0003	0,0964	0,9543	0,9537	50,3246	49,6914	Não
352	1000000010110110	0,6952	0,9540	0,0001	50,0006	0,0963	0,9544	0,9537	50,2960	49,7135	Não
353	0101011000011100	0,8125	0,9540	0,0001	49,9966	0,0985	0,9544	0,9537	50,3029	49,6689	Não
354	0000100110100010	0,8125	0,9540	0,0001	50,0014	0,0983	0,9544	0,9537	50,2895	49,7009	Não
355	0001010000011100	0,8750	0,9540	0,0001	50,0041	0,0967	0,9544	0,9537	50,3418	49,6311	Não
356	0011110010010111	0,7577	0,9540	0,0001	50,0015	0,0960	0,9544	0,9538	50,3487	49,6719	Não
357	0111001000011100	0,8438	0,9540	0,0001	49,9988	0,1002	0,9544	0,9537	50,3143	49,6998	Não
358	1000011110100111	0,7500	0,9540	0,0001	50,0015	0,0954	0,9545	0,9537	50,3029	49,6914	Não
359	1010110000111000	0,9375	0,9540	0,0001	49,9973	0,0974	0,9545	0,9537	50,2686	49,6811	Não
360	0010111010111011	0,6563	0,9540	0,0001	49,9961	0,0970	0,9544	0,9538	50,3048	49,6689	Não
361	0101010111000000	0,8632	0,9540	0,0001	50,0030	0,1000	0,9544	0,9537	50,3204	49,6841	Não
362	1111010001010101	0,8438	0,9540	0,0001	50,0001	0,0973	0,9544	0,9537	50,2995	49,5949	Não
363	1011010110111100	0,8438	0,9540	0,0001	49,9926	0,0963	0,9544	0,9537	50,2850	49,6346	Não
364	1111000011001000	0,8438	0,9540	0,0001	50,0048	0,0971	0,9544	0,9537	50,3345	49,7158	Não
365	1011001010010100	0,7500	0,9540	0,0001	49,9997	0,0975	0,9544	0,9537	50,3792	49,5510	Não
366	1101011101100010	0,6716	0,9540	0,0001	49,9970	0,1006	0,9544	0,9537	50,2903	49,6670	Não
367	0111001001111001	0,7500	0,9540	0,0001	50,0024	0,0984	0,9544	0,9537	50,3037	49,6731	Não
368	1111001110100000	0,8125	0,9540	0,0001	50,0082	0,1006	0,9544	0,9537	50,3414	49,6952	Não
369	1110000110001101	0,8007	0,9540	0,0001	49,9939	0,0957	0,9543	0,9537	50,2911	49,6494	Não
370	1111001110100010	0,9375	0,9540	0,0001	49,9983	0,0999	0,9543	0,9537	50,3067	49,7089	Não
371	0110011111000010	0,7813	0,9540	0,0001	50,0048	0,0960	0,9544	0,9537	50,3105	49,6933	Não
372	0001110101000011	0,8632	0,9540	0,0001	49,9988	0,0960	0,9544	0,9537	50,2743	49,6597	Não
373	0010101101111000	0,8438	0,9540	0,0001	50,0023	0,0995	0,9545	0,9536	50,3639	49,6502	Não
374	0001100101011111	0,8632	0,9540	0,0001	50,0029	0,0959	0,9544	0,9537	50,3006	49,7135	Não
375	0100001110111111	0,8632	0,9540	0,0001	50,0004	0,0984	0,9544	0,9537	50,4154	49,7265	Não
376	1110011100011100	0,8438	0,9540	0,0001	49,9954	0,0968	0,9543	0,9537	50,2811	49,6662	Não
377	0110011011100010	0,8438	0,9540	0,0001	49,9999	0,0974	0,9544	0,9537	50,2895	49,6727	Não
378	0000001001000001	0,7500	0,9540	0,0001	50,0011	0,0952	0,9543	0,9537	50,3635	49,6937	Não
379	0011110100101111	0,7500	0,9540	0,0001	49,9991	0,0980	0,9544	0,9537	50,2571	49,6605	Não
380	1101010100101111	0,7131	0,9540	0,0001	49,9972	0,0963	0,9544	0,9538	50,4215	49,6799	Não
381	1010010101011011	0,8750	0,9540	0,0001	49,9968	0,0938	0,9544	0,9537	50,2972	49,6704	Não
382	0011011010110111	0,7146	0,9540	0,0001	49,9964	0,0984	0,9544	0,9537	50,3250	49,7124	Não
383	1111111111111110	0,5000	0,8983	0,0522	54,4482	2,3208	0,9501	0,5617	62,4050	47,6044	Sim
384	1111110011000000	0,7889	0,9540	0,0001	50,0004	0,0995	0,9544	0,9537	50,2998	49,5800	Não
385	0000111110000011	0,8320	0,9540	0,0001	50,0032	0,1042	0,9544	0,9537	50,3288	49,6532	Não
386	0000100111011110	0,9063	0,9540	0,0001	49,9994	0,0978	0,9544	0,9537	50,3517	49,6639	Não
387	0110111010111100	0,8125	0,9540	0,0001	49,9957	0,0997	0,9543	0,9538	50,3124	49,6979	Não
388	0000101000001100	0,8438	0,9540	0,0001	49,9978	0,0991	0,9544	0,9536	50,3296	49,6895	Não
389	1000001101101000	0,9063	0,9540	0,0001	49,9936	0,0977	0,9544	0,9536	50,2647	49,6910	Não
390	0000011111010000	0,7264	0,9541	0,0001	49,9973	0,0936	0,9543	0,9537	50,2697	49,6582	Não
391	1101110011001100	0,7500	0,9540	0,0001	50,0031	0,0973	0,9544	0,9537	50,3319	49,5949	Não
392	0011011101101111	0,6250	0,9540	0,0001	49,9985	0,1026	0,9544	0,9536	50,3494	49,7021	Não
393	0110011010010100	0,8320	0,9540	0,0001	50,0009	0,1008	0,9543	0,9537	50,4005	49,6658	Não
394	1100110110111110	0,7695	0,9540	0,0001	50,0025	0,0961	0,9543	0,9536	50,3506	49,6456	Não
395	1101000100101100	0,8750	0,9540	0,0001	50,0024	0,1006	0,9544	0,9537	50,3712	49,7177	Não
396	1011011100010000	0,7873	0,9540	0,0001	49,9968	0,0997	0,9544	0,9536	50,2636	49,6933	Não
397	1100111100011011	0,8125	0,9540	0,0001	49,9974	0,1004	0,9543	0,9537	50,2724	49,7005	Não
398	0101101100111111	0,7500	0,9540	0,0001	49,9961	0,0933	0,9544	0,9537	50,3326	49,6990	Não
399	0110100000110110	0,8750	0,9540	0,0001	49,9981	0,0987	0,9543	0,9537	50,3750	49,7326	Não
400	1001000010101111	0,8632	0,9540	0,0001	49,9976	0,0977	0,9544	0,9537	50,3414	49,7017	Não
401	0000010000110110	0,7500	0,9540	0,0001	50,0021	0,0998	0,9544	0,9537	50,3887	49,6864	Não
402	0110001011001001	0,7577	0,9540	0,0001	50,0008	0,1012	0,9544	0,9537	50,4234	49,7055	Não
403	1001010011101110	0,7577	0,9540	0,0001	50,0014	0,0964	0,9544	0,9537	50,2926	49,6929	Não
404	0011100111011011	0,8007	0,9540	0,0001	49,9980	0,0964	0,9544	0,9537	50,2831	49,7303	Não
405	1101000001110001	0,8750	0,9540	0,0001	49,9939	0,0954	0,9543	0,9537	50,3029	49,7139	Não
406	0101101001110001	0,8438	0,9540	0,0001	49,9993	0,0948	0,9543	0,9537	50,3002	49,7349	Não
407	1010010101110010	0,7695	0,9540	0,0001	50,0060	0,1011	0,9544	0,9537	50,3288	49,6246	Não
408	0010111110011101	0,7500	0,9540	0,0001	49,9951	0,0981	0,9545	0,9537	50,3063	49,5762	Não
409	1101001010111011	0,8007	0,9540	0,0001	49,9952	0,0979	0,9544	0,9537	50,3216	49,6944	Não
410	0011010110110010	0,8750	0,9540	0,0001	50,0029	0,0999	0,9544	0,9537	50,3906	49,6674	Não
411	1100111110011011	0,6014	0,9540	0,0001	50,0026	0,0942	0,9544	0,9537	50,3433	49,7261	Não
412	1110110001100000	0,8438	0,9540	0,0001	50,0003	0,0989	0,9545	0,9537	50,3262	49,6815	Não
413	1010101001111101	0,7131	0,9540	0,0001	50,0025	0,0960	0,9544	0,9537	50,3140	49,7131	Não
414	1110101100000110	0,8632	0,9540	0,0001	50,0020	0,1007	0,9545	0,9538	50,2869	49,6700	Não
415	0111000011111000	0,7382	0,9540	0,0001	50,0010	0,0982	0,9544	0,9536	50,2777	49,6784	Não
416	0000000101000101	0,8007	0,9540	0,0001	49,9994	0,0943	0,9544	0,9536	50,3422	49,6490	Não

417	1011011101110010	0,8320	0,9540	0,0001	50,0013	0,0989	0,9544	0,9536	50,3201	49,7154	Não
418	1001101011100100	0,8438	0,9540	0,0001	50,0014	0,0928	0,9544	0,9537	50,3231	49,6479	Não
419	0111101101000001	0,9688	0,9540	0,0001	49,9982	0,0975	0,9544	0,9537	50,3048	49,6624	Não
420	1001011111011110	0,7146	0,9540	0,0001	49,9994	0,0969	0,9544	0,9537	50,2922	49,6834	Não
421	1110010000100110	0,8632	0,9540	0,0001	49,9983	0,0996	0,9544	0,9537	50,3361	49,7135	Não
422	1110111001101000	0,8125	0,9540	0,0001	50,0021	0,0968	0,9543	0,9538	50,3647	49,6990	Não
423	1001111101110001	0,8438	0,9540	0,0001	49,9957	0,0944	0,9544	0,9537	50,2613	49,6815	Não
424	0000101001010111	0,7382	0,9540	0,0001	49,9990	0,1004	0,9544	0,9537	50,3189	49,6460	Não
425	1001011101010101	0,8007	0,9540	0,0001	50,0030	0,0985	0,9544	0,9537	50,3052	49,6880	Não
426	1110001111011000	0,8438	0,9540	0,0001	49,9954	0,0993	0,9544	0,9537	50,3090	49,6288	Não
427	1001110101100101	0,8320	0,9540	0,0001	50,0032	0,1000	0,9543	0,9537	50,3193	49,7025	Não
428	1010000000101010	0,6875	0,9540	0,0001	50,0006	0,0955	0,9544	0,9537	50,2842	49,6914	Não
429	0011100010100000	0,7561	0,9540	0,0001	49,9962	0,0981	0,9544	0,9537	50,3063	49,7128	Não
430	0001100001100110	0,7577	0,9540	0,0001	49,9931	0,0981	0,9544	0,9537	50,2838	49,6723	Não
431	1100011110110001	0,6875	0,9540	0,0001	49,9996	0,0972	0,9543	0,9537	50,2666	49,6109	Não
432	0001011001010011	0,8320	0,9540	0,0001	50,0038	0,0976	0,9544	0,9537	50,3315	49,7128	Não
433	0111101100011011	0,7264	0,9540	0,0001	49,9949	0,0967	0,9544	0,9537	50,3223	49,6960	Não
434	0101111010000010	0,8438	0,9540	0,0001	50,0040	0,0968	0,9544	0,9537	50,3307	49,6548	Não
435	1100011011100100	0,9063	0,9540	0,0001	49,9959	0,0984	0,9544	0,9537	50,3464	49,6307	Não
436	0100111011111010	0,8007	0,9540	0,0001	49,9992	0,0933	0,9543	0,9537	50,3384	49,6986	Não
437	0000000000111111	0,7443	0,9540	0,0001	49,9999	0,0968	0,9543	0,9537	50,3361	49,6708	Não
438	0110001010010001	0,8750	0,9540	0,0001	50,0021	0,0996	0,9544	0,9537	50,3021	49,7017	Não
439	0001010010001101	0,8438	0,9540	0,0001	49,9961	0,0993	0,9544	0,9537	50,3208	49,6727	Não
440	1011110000001001	0,8750	0,9540	0,0001	50,0023	0,0973	0,9544	0,9537	50,2975	49,6620	Não
441	1111011111010111	0,6875	0,9467	0,0120	52,7098	1,7954	0,9542	0,8567	60,5885	49,9611	Sim
442	1101001111101111	0,6327	0,9540	0,0001	50,0003	0,0965	0,9544	0,9537	50,3876	49,6834	Não
443	0001101111100000	0,7813	0,9540	0,0001	49,9974	0,0961	0,9544	0,9537	50,3418	49,6937	Não
444	1011100100110101	0,8438	0,9540	0,0001	49,9907	0,1003	0,9544	0,9537	50,3513	49,6628	Não
445	0000110010011101	0,8438	0,9540	0,0001	50,0042	0,0994	0,9544	0,9537	50,3006	49,7257	Não
446	0101100010110110	0,8750	0,9540	0,0001	49,9987	0,0959	0,9544	0,9537	50,2987	49,7192	Não
447	0100001110100101	0,8320	0,9540	0,0001	50,0016	0,0998	0,9544	0,9537	50,3086	49,7074	Não
448	1110010101001010	0,7695	0,9540	0,0001	50,0054	0,0976	0,9543	0,9537	50,3113	49,6727	Não
449	0001010110111100	0,8438	0,9540	0,0001	50,0024	0,0986	0,9544	0,9537	50,3254	49,6544	Não
450	1110111001111110	0,8007	0,9540	0,0001	49,9974	0,0987	0,9544	0,9537	50,3708	49,7234	Não
451	0011001001010110	0,8438	0,9540	0,0001	49,9991	0,0965	0,9544	0,9537	50,3117	49,7040	Não
452	0011000010100111	0,8320	0,9540	0,0001	49,9982	0,0965	0,9544	0,9537	50,2941	49,7150	Não
453	0010000110111010	0,8632	0,9540	0,0001	49,9973	0,0971	0,9543	0,9537	50,2579	49,6777	Não
454	1100010001101010	0,8007	0,9540	0,0001	50,0009	0,1012	0,9544	0,9537	50,3071	49,6407	Não
455	0101101101101110	0,7070	0,9540	0,0001	49,9928	0,1019	0,9544	0,9537	50,3181	49,6002	Não
456	0100000101000000	0,5000	0,9538	0,0007	49,9942	0,0996	0,9544	0,9456	50,2754	49,6536	Sim
457	0111001000010010	0,8632	0,9540	0,0001	49,9984	0,0951	0,9544	0,9537	50,3281	49,6906	Não
458	0011011010011101	0,8320	0,9540	0,0001	50,0003	0,0933	0,9544	0,9537	50,2975	49,7475	Não
459	1001010110010001	0,9375	0,9540	0,0001	50,0054	0,1006	0,9544	0,9537	50,3365	49,6700	Não
460	0010011001101100	0,7577	0,9540	0,0001	50,0016	0,0928	0,9544	0,9537	50,3632	49,7257	Não
461	0010011101010001	0,8632	0,9540	0,0001	50,0051	0,0946	0,9543	0,9537	50,3563	49,6761	Não
462	0010110010011110	0,7695	0,9540	0,0001	50,0005	0,0996	0,9543	0,9537	50,3109	49,6494	Não
463	0101101011011010	0,7889	0,9540	0,0001	49,9942	0,0966	0,9543	0,9537	50,3357	49,6788	Não
464	0110111110101011	0,6716	0,9540	0,0001	50,0002	0,0960	0,9543	0,9538	50,2789	49,6899	Não
465	0001110110001001	0,8320	0,9540	0,0001	49,9992	0,0947	0,9544	0,9536	50,2945	49,6601	Não
466	1011000000010001	0,8438	0,9540	0,0001	50,0013	0,0961	0,9544	0,9537	50,3101	49,6368	Não
467	0110101100011000	0,8438	0,9540	0,0001	50,0016	0,0973	0,9543	0,9537	50,2934	49,6807	Não
468	1101000001111000	0,8632	0,9540	0,0001	50,0049	0,1006	0,9543	0,9537	50,3471	49,7410	Não
469	1010100010100001	0,8007	0,9540	0,0001	49,9996	0,1031	0,9544	0,9537	50,3601	49,5697	Não
470	0011101111010100	0,8750	0,9540	0,0001	50,0035	0,0971	0,9544	0,9538	50,3330	49,6231	Não
471	0101001100000111	0,8438	0,9540	0,0001	50,0048	0,1033	0,9543	0,9537	50,3136	49,7166	Não
472	1111010101111011	0,8007	0,9540	0,0001	49,9983	0,0967	0,9544	0,9537	50,3086	49,7028	Não
473	1000010111011110	0,8125	0,9540	0,0001	50,0035	0,1017	0,9544	0,9537	50,3090	49,7200	Não
474	1111111110001111	0,6929	0,9540	0,0001	49,9953	0,0982	0,9543	0,9537	50,3551	49,7124	Não
475	1101110011111100	0,8438	0,9540	0,0001	49,9965	0,0971	0,9544	0,9537	50,2861	49,6651	Não
476	1001110110110110	0,8750	0,9540	0,0001	50,0006	0,0976	0,9544	0,9537	50,2823	49,6647	Não
477	1001001001000000	0,6075	0,9540	0,0001	50,0021	0,0984	0,9543	0,9537	50,3120	49,6323	Não
478	0101001001000001	0,8320	0,9540	0,0001	50,0002	0,0984	0,9544	0,9537	50,3304	49,6109	Não
479	0101001101001100	0,8632	0,9540	0,0001	49,9952	0,0984	0,9543	0,9537	50,3223	49,6532	Não
480	1110100110000110	0,9688	0,9540	0,0001	49,9973	0,0981	0,9545	0,9536	50,2796	49,7261	Não
481	0100000011100000	0,7561	0,9540	0,0001	49,9986	0,1017	0,9544	0,9537	50,3258	49,6868	Não
482	1101011110110011	0,7500	0,9540	0,0001	50,0019	0,0971	0,9543	0,9537	50,3513	49,7517	Não
483	1110001101011101	0,8320	0,9540	0,0001	50,0030	0,0959	0,9544	0,9537	50,3815	49,6632	Não
484	1010101011000100	0,9375	0,9540	0,0001	49,9993	0,0998	0,9544	0,9536	50,3174	49,6758	Não
485	0010011100001000	0,8438	0,9540	0,0001	50,0000	0,1002	0,9544	0,9537	50,2991	49,6319	Não
486	1010000000000010	0,6875	0,9540	0,0001	50,0060	0,0974	0,9544	0,9537	50,3677	49,7192	Não
487	1101100001100010	0,8750	0,9540	0,0001	50,0099	0,0989	0,9544	0,9536	50,2941	49,6689	Não
488	0111010101111110	0,8125	0,9540	0,0001	49,9960	0,0950	0,9543	0,9537	50,3494	49,7002	Não
489	1101010000010011	0,9063	0,9540	0,0001	50,0001	0,0948	0,9544	0,9537	50,3002	49,6849	Não
490	1101111000110000	0,8125	0,9540	0,0001	50,0020	0,0951	0,9544	0,9537	50,2838	49,7299	Não
491	1100001011110000	0,8438	0,9540	0,0001	49,9964	0,1012	0,9544	0,9537	50,3563	49,6616	Não
492	1001110100100000	0,8007	0,9540	0,0001	50,0019	0,0980	0,9543	0,9537	50,3136	49,6670	Não
493	1110011100101110	0,7500	0,9540	0,0001	50,0061	0,0958	0,9544	0,9537	50,3410	49,7406	Não
494	0010101111100010	0,8438	0,9540	0,0001	49,9977	0,0973	0,9544	0,9538	50,4135	49,6437	Não
495	1010000000100111	0,8125	0,9540	0,0001	50,0015	0,0945	0,9544	0,9536	50,3284	49,6922	Não
496	1010010000100011	0,8750	0,9540	0,0001	49,9987	0,1001	0,9544	0,9537	50,3815	49,6716	Não

497	1000010100101100	0,8750	0,9540	0,0001	50,0010	0,0946	0,9543	0,9537	50,3281	49,6670	Não
498	1100001110011001	0,8125	0,9540	0,0001	49,9981	0,1010	0,9544	0,9537	50,2846	49,6826	Não
499	0100110100010001	0,8750	0,9540	0,0001	50,0048	0,0995	0,9545	0,9537	50,3067	49,6662	Não
500	1101010111011001	0,8125	0,9540	0,0001	49,9989	0,0978	0,9544	0,9537	50,2865	49,6479	Não

Tabela C.2: Resultados para o teste com o modelo de sensitividade fixa

C.2 Resultados do modelo com rotação da sensitividade

A	B	C	D	E	F	G	H	I	J	K	L
1	1000000000000000	0,0000	0,8241	0,0906	52,0019	1,2698	0,9526	0,4918	55,9185	40,5144	Sim
2	1110111111111111	0,0000	0,7133	0,1049	63,5911	5,5533	0,9304	0,3688	81,8707	51,8982	Sim
3	1111111100010000	0,6372	0,9540	0,0001	50,0027	0,0984	0,9543	0,9537	50,2628	49,5995	Não
4	0000100011111111	0,6372	0,9540	0,0001	49,9988	0,0952	0,9544	0,9537	50,2808	49,6861	Não
5	1010101010101110	0,2500	0,9540	0,0001	49,9953	0,0994	0,9544	0,9538	50,2991	49,6742	Não
6	0100010101010101	0,2500	0,9540	0,0001	50,0006	0,0956	0,9544	0,9536	50,3677	49,7272	Não
7	1100010011001100	0,5000	0,9540	0,0001	50,0013	0,0946	0,9544	0,9537	50,2693	49,7383	Não
8	1110011110001100	0,7264	0,9540	0,0001	49,9992	0,0986	0,9543	0,9536	50,3735	49,7021	Não
9	1111000001110000	0,7500	0,9540	0,0001	50,0012	0,0950	0,9544	0,9537	50,2815	49,6639	Não
10	0111110011010111	0,7771	0,9540	0,0001	49,9972	0,0968	0,9543	0,9537	50,2701	49,6731	Não
11	1111011010010101	0,8125	0,9540	0,0001	50,0024	0,0993	0,9543	0,9537	50,3204	49,6117	Não
12	0011001011101000	0,9063	0,9540	0,0001	50,0019	0,0961	0,9544	0,9537	50,2956	49,6853	Não
13	0101001010011000	0,8320	0,9540	0,0001	49,9964	0,1003	0,9544	0,9537	50,3475	49,6487	Não
14	1100001010010111	0,8750	0,9540	0,0001	49,9980	0,0972	0,9544	0,9537	50,2666	49,6674	Não
15	1101101001101001	0,8320	0,9540	0,0001	49,9969	0,0988	0,9545	0,9537	50,4456	49,7040	Não
16	1111011011100110	0,7771	0,9540	0,0001	49,9965	0,0951	0,9544	0,9537	50,3300	49,7116	Não
17	1110111010111000	0,7889	0,9540	0,0001	49,9972	0,0951	0,9543	0,9537	50,3025	49,6490	Não
18	0110000110100011	0,8438	0,9540	0,0001	50,0000	0,1013	0,9545	0,9537	50,3201	49,6361	Não
19	1110011010100000	0,8438	0,9540	0,0001	49,9973	0,0998	0,9543	0,9537	50,2800	49,6735	Não
20	0110111100110011	0,7459	0,9540	0,0001	49,9959	0,0997	0,9544	0,9537	50,2979	49,6330	Não
21	1001010010011110	0,8750	0,9540	0,0001	49,9964	0,0981	0,9544	0,9537	50,2987	49,6891	Não
22	1100010011001110	0,8750	0,9541	0,0001	50,0026	0,0959	0,9544	0,9537	50,3185	49,7097	Não
23	0110101111001011	0,7146	0,9540	0,0001	49,9994	0,0964	0,9544	0,9537	50,3262	49,7131	Não
24	1011010000100110	0,7695	0,9540	0,0001	49,9945	0,0952	0,9543	0,9537	50,2720	49,6925	Não
25	1111101011101100	0,7146	0,9540	0,0001	50,0038	0,0938	0,9543	0,9537	50,3235	49,6498	Não
26	0010101100000101	0,9688	0,9540	0,0001	49,9970	0,0977	0,9543	0,9537	50,3433	49,6643	Não
27	0111100010001100	0,8125	0,9540	0,0001	49,9984	0,0982	0,9543	0,9536	50,2480	49,6803	Não
28	0001101010111110	0,9375	0,9540	0,0001	50,0008	0,0994	0,9543	0,9537	50,2834	49,6849	Não
29	1011001100101001	0,8750	0,9540	0,0001	50,0006	0,0961	0,9543	0,9537	50,3090	49,6735	Não
30	0010110001101000	0,8125	0,9540	0,0001	50,0040	0,0977	0,9544	0,9537	50,2937	49,6864	Não
31	0000101010011000	0,7561	0,9540	0,0001	50,0035	0,0949	0,9543	0,9537	50,2995	49,6593	Não
32	0011111111000001	0,7873	0,9540	0,0001	49,9993	0,1008	0,9543	0,9537	50,2869	49,6796	Não
33	1101011011110011	0,8750	0,9540	0,0001	49,9958	0,0995	0,9544	0,9537	50,3410	49,6483	Não
34	1110100110100011	0,8320	0,9540	0,0001	50,0007	0,0989	0,9544	0,9537	50,3326	49,7040	Não
35	0000100011110001	0,7889	0,9540	0,0001	49,9943	0,0962	0,9543	0,9537	50,2617	49,6769	Não
36	1111001110001111	0,8186	0,9540	0,0001	50,0010	0,0989	0,9544	0,9537	50,2972	49,6655	Não
37	0010101110010100	0,8632	0,9540	0,0001	50,0009	0,0984	0,9544	0,9536	50,3967	49,7322	Não
38	0010101000001110	0,7577	0,9540	0,0001	50,0029	0,0964	0,9543	0,9537	50,2960	49,6998	Não
39	0001001000101000	0,6563	0,9540	0,0001	50,0046	0,0952	0,9544	0,9537	50,3246	49,6731	Não
40	0101001010110011	0,7695	0,9540	0,0001	49,9979	0,0947	0,9544	0,9537	50,2705	49,7181	Não
41	1100011001010101	0,8438	0,9540	0,0001	50,0046	0,0968	0,9544	0,9537	50,2708	49,6613	Não
42	0011110000110110	0,9063	0,9540	0,0001	49,9934	0,0957	0,9544	0,9537	50,2739	49,7078	Não
43	1010010011111110	0,8125	0,9540	0,0001	49,9986	0,0962	0,9544	0,9537	50,3105	49,6986	Não
44	0110101101000111	0,8320	0,9540	0,0001	50,0067	0,0985	0,9544	0,9537	50,3002	49,6773	Não
45	1011110100011111	0,8320	0,9540	0,0001	50,0029	0,0995	0,9544	0,9537	50,2865	49,6716	Não
46	1011011101001100	0,7889	0,9540	0,0001	50,0017	0,0967	0,9544	0,9537	50,3136	49,6826	Não
47	0001100000111011	0,8632	0,9540	0,0001	50,0030	0,0953	0,9544	0,9537	50,3510	49,6567	Não
48	0000000011011111	0,8632	0,9540	0,0001	49,9969	0,0969	0,9544	0,9537	50,3029	49,7124	Não
49	0001111101100011	0,9063	0,9540	0,0001	49,9986	0,0956	0,9543	0,9537	50,3201	49,7025	Não
50	0000010001100110	0,8438	0,9540	0,0001	49,9992	0,0985	0,9544	0,9537	50,3159	49,6708	Não
51	1001000111111000	0,8320	0,9540	0,0001	50,0044	0,0944	0,9544	0,9537	50,3475	49,6651	Não
52	1101010110101111	0,6875	0,9540	0,0001	50,0038	0,0988	0,9544	0,9537	50,2876	49,6674	Não
53	0111110111111101	0,5000	0,9539	0,0006	50,0668	0,1917	0,9544	0,9429	52,5921	49,6719	Sim
54	0011000000010010	0,7577	0,9540	0,0001	49,9945	0,0990	0,9544	0,9537	50,3235	49,6929	Não
55	1001001001001001	0,6757	0,9540	0,0001	49,9949	0,0931	0,9544	0,9537	50,3002	49,6563	Não
56	1111111001011100	0,8438	0,9540	0,0001	50,0044	0,0946	0,9544	0,9537	50,3307	49,6101	Não
57	1100000100100001	0,8320	0,9540	0,0001	49,9986	0,0974	0,9544	0,9536	50,3136	49,6674	Não
58	1110011010000010	0,8438	0,9540	0,0001	49,9992	0,1008	0,9544	0,9537	50,3159	49,6681	Não
59	0100111111111110	0,7873	0,9540	0,0001	49,9979	0,0994	0,9544	0,9537	50,2899	49,6723	Não

60	0000100000101000	0,6875	0,9540	0,0001	50,0022	0,1007	0,9543	0,9537	50,3403	49,7265	Não
61	1011110100101100	0,7695	0,9540	0,0001	50,0059	0,1003	0,9544	0,9538	50,2918	49,6410	Não
62	1101011101111111	0,7146	0,9540	0,0001	49,9976	0,0982	0,9544	0,9537	50,2987	49,6853	Não
63	1010011100000010	0,8007	0,9540	0,0001	49,9974	0,0957	0,9543	0,9537	50,3254	49,6956	Não
64	0001100011111110	0,8750	0,9540	0,0001	49,9983	0,0937	0,9543	0,9537	50,2586	49,7135	Não
65	1111100110111110	0,8438	0,9540	0,0001	49,9975	0,0979	0,9544	0,9538	50,2754	49,6990	Não
66	0000000000001101	0,7264	0,9540	0,0001	49,9949	0,0982	0,9544	0,9537	50,3037	49,6857	Não
67	1000011001111011	0,8438	0,9540	0,0001	49,9978	0,0922	0,9543	0,9536	50,3590	49,6979	Não
68	1110010111011101	0,8007	0,9540	0,0001	50,0036	0,1036	0,9543	0,9537	50,3273	49,6223	Não
69	0000110011000110	0,7695	0,9540	0,0001	49,9954	0,1003	0,9544	0,9537	50,3334	49,6433	Não
70	1111101101101111	0,6250	0,9540	0,0001	50,0007	0,0981	0,9543	0,9537	50,3361	49,6883	Não
71	1011100001111001	0,8438	0,9540	0,0001	50,0040	0,0992	0,9544	0,9537	50,2838	49,7387	Não
72	1101101110111000	0,7771	0,9540	0,0001	50,0059	0,0990	0,9543	0,9537	50,2716	49,6761	Não
73	1001111010101010	0,7188	0,9540	0,0001	50,0019	0,0979	0,9544	0,9537	50,3113	49,7181	Não
74	0100011110110101	0,8750	0,9540	0,0001	49,9996	0,0995	0,9544	0,9537	50,2747	49,6513	Não
75	0011100011101000	0,8125	0,9540	0,0001	50,0023	0,0971	0,9544	0,9537	50,3201	49,7013	Não
76	1011001010000000	0,8750	0,9540	0,0001	50,0032	0,1023	0,9543	0,9537	50,3513	49,7334	Não
77	1011110010111000	0,8632	0,9540	0,0001	49,9985	0,0925	0,9543	0,9537	50,3193	49,7192	Não
78	1010010010110110	0,7146	0,9540	0,0001	49,9983	0,0954	0,9544	0,9537	50,3468	49,7143	Não
79	0110011000110010	0,6952	0,9540	0,0001	49,9961	0,0970	0,9543	0,9537	50,3399	49,6735	Não
80	0001011100010110	0,8632	0,9540	0,0001	49,9944	0,0965	0,9544	0,9537	50,2872	49,6571	Não
81	0110010010011100	0,8750	0,9540	0,0001	49,9986	0,0972	0,9544	0,9537	50,3113	49,6498	Não
82	1110100101110111	0,7771	0,9540	0,0001	49,9998	0,0978	0,9544	0,9536	50,3212	49,7437	Não
83	0000001001001101	0,8945	0,9540	0,0001	49,9999	0,0966	0,9543	0,9537	50,2831	49,6902	Não
84	1001110111100100	0,9063	0,9540	0,0001	50,0011	0,0998	0,9544	0,9537	50,3277	49,7143	Não
85	1101001100111100	0,8438	0,9540	0,0001	49,9959	0,0997	0,9544	0,9537	50,3418	49,6880	Não
86	1101001101010000	0,8320	0,9540	0,0001	50,0017	0,0971	0,9544	0,9537	50,2934	49,7265	Não
87	1111010100001101	0,8438	0,9540	0,0001	49,9976	0,0962	0,9544	0,9537	50,2804	49,6536	Não
88	1100000000001110	0,7873	0,9540	0,0001	49,9988	0,1034	0,9544	0,9537	50,3815	49,6429	Não
89	1011111000111000	0,8320	0,9540	0,0001	50,0062	0,0962	0,9543	0,9537	50,3525	49,7269	Não
90	1010110010111000	0,8320	0,9540	0,0001	49,9971	0,0981	0,9544	0,9537	50,3075	49,7009	Não
91	1100101000101101	0,8750	0,9540	0,0001	50,0013	0,0984	0,9544	0,9536	50,3242	49,7150	Não
92	0001001001100010	0,6250	0,9540	0,0001	49,9984	0,0956	0,9544	0,9537	50,3063	49,6475	Não
93	0110010010110101	0,7146	0,9540	0,0001	50,0030	0,0987	0,9544	0,9537	50,3723	49,7108	Não
94	1101101010111110	0,8320	0,9540	0,0001	49,9993	0,0976	0,9543	0,9537	50,2541	49,6799	Não
95	1010011101001111	0,8750	0,9540	0,0001	49,9991	0,0981	0,9544	0,9537	50,2972	49,6273	Não
96	1101111000110001	0,8750	0,9540	0,0001	49,9954	0,0994	0,9543	0,9537	50,3353	49,6964	Não
97	0100110111111110	0,7382	0,9540	0,0001	49,9950	0,0957	0,9544	0,9537	50,3349	49,7341	Não
98	0101111011001011	0,8750	0,9540	0,0001	49,9979	0,1001	0,9544	0,9537	50,3204	49,6498	Não
99	0111010110001101	0,8750	0,9540	0,0001	49,9998	0,1004	0,9544	0,9537	50,3494	49,7261	Não
100	1100010001011110	0,8125	0,9540	0,0001	50,0016	0,0968	0,9544	0,9537	50,3170	49,7040	Não
101	0011010110111011	0,8320	0,9540	0,0001	49,9972	0,0976	0,9543	0,9537	50,2956	49,6826	Não
102	0100001110101010	0,8632	0,9540	0,0001	49,9998	0,0968	0,9544	0,9537	50,2934	49,6845	Não
103	1101001110001110	0,8438	0,9540	0,0001	49,9976	0,0967	0,9544	0,9537	50,3292	49,6887	Não
104	0100010101110011	0,8438	0,9540	0,0001	50,0022	0,0955	0,9544	0,9537	50,2911	49,6708	Não
105	0011011101001001	0,7146	0,9540	0,0001	49,9970	0,1003	0,9544	0,9537	50,2899	49,6838	Não
106	0101011001101110	0,7500	0,9540	0,0001	49,9975	0,0977	0,9544	0,9537	50,3025	49,7311	Não
107	1001111011000000	0,8438	0,9540	0,0001	49,9993	0,1015	0,9544	0,9537	50,3040	49,6788	Não
108	1111011001010101	0,8007	0,9540	0,0001	50,0029	0,0967	0,9544	0,9537	50,2644	49,7131	Não
109	1111111011111100	0,4054	0,9539	0,0007	50,0008	0,0976	0,9544	0,9437	50,2552	49,7208	Não
110	0010001010110110	0,8632	0,9540	0,0001	50,0009	0,0982	0,9544	0,9537	50,3204	49,6937	Não
111	0110111001001000	0,8320	0,9540	0,0001	50,0013	0,0978	0,9544	0,9537	50,2666	49,7013	Não
112	1111110001000110	0,8007	0,9540	0,0001	49,9992	0,0971	0,9543	0,9536	50,2789	49,6700	Não
113	1100110010111000	0,8007	0,9540	0,0001	50,0052	0,1016	0,9544	0,9537	50,3010	49,6738	Não
114	0001011001110010	0,8750	0,9540	0,0001	50,0000	0,0988	0,9544	0,9537	50,3414	49,7025	Não
115	0000010001001100	0,7695	0,9540	0,0001	50,0016	0,0998	0,9545	0,9537	50,3044	49,7128	Não
116	0111001101111011	0,7771	0,9540	0,0001	50,0036	0,1021	0,9544	0,9536	50,3113	49,6754	Não
117	1010000011100100	0,8438	0,9540	0,0001	50,0004	0,0971	0,9544	0,9537	50,2934	49,6933	Não
118	1000110000001100	0,7264	0,9540	0,0001	49,9994	0,0977	0,9544	0,9537	50,3365	49,6716	Não
119	1101001011011011	0,8750	0,9540	0,0001	50,0021	0,0996	0,9544	0,9537	50,3757	49,6613	Não
120	0011100111001000	0,9063	0,9540	0,0001	49,9987	0,0992	0,9544	0,9537	50,3262	49,7135	Não
121	1111100101100110	0,8320	0,9540	0,0001	50,0036	0,1022	0,9544	0,9537	50,3624	49,7044	Não
122	0001100111000100	0,7577	0,9540	0,0001	49,9958	0,0994	0,9543	0,9536	50,3002	49,6655	Não
123	1111011111010000	0,8750	0,9540	0,0001	49,9994	0,0972	0,9544	0,9537	50,3128	49,6853	Não
124	1110011010110001	0,8320	0,9540	0,0001	49,9986	0,0959	0,9544	0,9537	50,3151	49,6758	Não
125	1010100000110011	0,9063	0,9540	0,0001	49,9961	0,1023	0,9544	0,9537	50,3143	49,6880	Não
126	1101010010101001	0,7500	0,9540	0,0001	49,9971	0,0988	0,9544	0,9537	50,3063	49,6620	Não
127	1100000111101001	0,9063	0,9540	0,0001	49,9969	0,0956	0,9543	0,9537	50,3109	49,6758	Não
128	1000010011011001	0,8438	0,9540	0,0001	49,9959	0,0928	0,9544	0,9537	50,2728	49,6674	Não
129	0111001011000001	0,8320	0,9540	0,0001	49,9966	0,0967	0,9544	0,9536	50,3235	49,6368	Não
130	1011101001100101	0,9063	0,9540	0,0001	49,9955	0,0973	0,9544	0,9536	50,3040	49,6952	Não
131	1100011101001001	0,8750	0,9540	0,0001	50,0009	0,0947	0,9544	0,9538	50,3033	49,6006	Não
132	1101100011111110	0,8438	0,9540	0,0001	49,9957	0,1005	0,9544	0,9537	50,3281	49,6471	Não
133	0000110101111010	0,8438	0,9540	0,0001	49,9988	0,0937	0,9544	0,9537	50,2625	49,6506	Não
134	1101110010001011	0,8007	0,9540	0,0001	50,0004	0,0976	0,9544	0,9537	50,3075	49,6815	Não
135	0111100100010100	0,8438	0,9540	0,0001	50,0046	0,0942	0,9544	0,9537	50,3098	49,7231	Não
136	0101111000100111	0,8438	0,9540	0,0001	50,0042	0,0981	0,9543	0,9537	50,2762	49,7097	Não
137	1110111000010110	0,8750	0,9540	0,0001	49,9986	0,0961	0,9544	0,9537	50,2926	49,6082	Não
138	0110100101000010	0,7146	0,9540	0,0001	50,0008	0,0961	0,9544	0,9537	50,3372	49,6758	Não
139	0000001101011100	0,7131	0,9540	0,0001	49,9980	0,0946	0,9544	0,9537	50,3433	49,7105	Não

140	1111111100000101	0,8438	0,9540	0,0001	50,0003	0,0961	0,9544	0,9537	50,3044	49,7082	Não
141	0001011010101010	0,8007	0,9540	0,0001	49,9928	0,1008	0,9544	0,9537	50,2846	49,6899	Não
142	1100101011011100	0,7500	0,9540	0,0001	49,9992	0,0949	0,9544	0,9537	50,3845	49,6674	Não
143	0110110001011010	0,8320	0,9540	0,0001	49,9928	0,0949	0,9544	0,9537	50,2850	49,6529	Não
144	1011101000111001	0,8320	0,9540	0,0001	50,0017	0,0980	0,9543	0,9537	50,3052	49,7532	Não
145	0010100110001001	0,8438	0,9540	0,0001	50,0031	0,1003	0,9544	0,9536	50,2865	49,7189	Não
146	1100111001100000	0,7577	0,9540	0,0001	49,9995	0,0995	0,9544	0,9537	50,3895	49,6983	Não
147	0010111101110101	0,8750	0,9540	0,0001	50,0041	0,0990	0,9544	0,9537	50,2884	49,7200	Não
148	0010111001011001	0,8320	0,9540	0,0001	50,0028	0,0986	0,9544	0,9537	50,3349	49,6815	Não
149	0101111110011111	0,6304	0,9540	0,0001	49,9985	0,0970	0,9543	0,9537	50,3372	49,7040	Não
150	0010100010110000	0,7248	0,9540	0,0001	49,9970	0,0951	0,9543	0,9537	50,2468	49,7150	Não
151	1000000001100111	0,7813	0,9540	0,0001	50,0013	0,0979	0,9544	0,9537	50,3212	49,7185	Não
152	1111100010001101	0,8320	0,9540	0,0001	50,0006	0,0971	0,9544	0,9537	50,2827	49,6941	Não
153	0100111010111001	0,8007	0,9540	0,0001	50,0017	0,0995	0,9544	0,9537	50,3269	49,6670	Não
154	1001011101111000	0,8438	0,9540	0,0001	50,0041	0,0972	0,9544	0,9538	50,2781	49,7055	Não
155	1100111111100110	0,8438	0,9540	0,0001	49,9965	0,0977	0,9544	0,9537	50,2708	49,6834	Não
156	1101000010101110	0,8750	0,9540	0,0001	50,0022	0,0969	0,9544	0,9537	50,2708	49,6544	Não
157	1111011101000010	0,8320	0,9540	0,0001	49,9968	0,0951	0,9544	0,9537	50,3105	49,6994	Não
158	1100110111110001	0,6936	0,9540	0,0001	50,0003	0,0946	0,9544	0,9538	50,2747	49,6742	Não
159	0000001101110000	0,5992	0,9540	0,0001	49,9974	0,0979	0,9544	0,9537	50,3246	49,6986	Não
160	1000110001110000	0,8750	0,9540	0,0001	49,9987	0,0979	0,9543	0,9537	50,3319	49,6765	Não
161	0000010011101010	0,9688	0,9540	0,0001	49,9953	0,0961	0,9544	0,9537	50,3101	49,6853	Não
162	0101101110110100	0,8750	0,9540	0,0001	50,0047	0,0958	0,9544	0,9537	50,3307	49,6807	Não
163	0000100000101101	0,8750	0,9540	0,0001	50,0047	0,0995	0,9544	0,9537	50,3166	49,6826	Não
164	0011110010111000	0,8945	0,9540	0,0001	50,0031	0,0985	0,9544	0,9537	50,3426	49,6727	Não
165	0110110011001011	0,8632	0,9540	0,0001	50,0016	0,0937	0,9544	0,9537	50,3037	49,7017	Não
166	0111010111100110	0,7695	0,9540	0,0001	50,0036	0,0989	0,9544	0,9537	50,3628	49,7215	Não
167	0110101011011011	0,7146	0,9540	0,0001	49,9985	0,0995	0,9544	0,9536	50,3780	49,7200	Não
168	1001010100110011	0,9063	0,9540	0,0001	49,9961	0,0971	0,9544	0,9537	50,3284	49,6490	Não
169	1111000010010001	0,8438	0,9540	0,0001	49,9978	0,0954	0,9544	0,9537	50,2892	49,6956	Não
170	0000100111010101	0,8632	0,9540	0,0001	50,0004	0,0987	0,9543	0,9537	50,2666	49,5766	Não
171	0101010001001001	0,5434	0,9540	0,0001	49,9971	0,0975	0,9544	0,9537	50,3399	49,6994	Não
172	1110010011111100	0,7695	0,9540	0,0001	50,0015	0,0973	0,9544	0,9537	50,2716	49,6292	Não
173	0101001101010110	0,8125	0,9540	0,0001	49,9986	0,0956	0,9544	0,9537	50,3326	49,7124	Não
174	0010001001111011	0,7813	0,9540	0,0001	49,9999	0,0986	0,9545	0,9537	50,3216	49,7192	Não
175	1110001110111011	0,8438	0,9540	0,0001	50,0061	0,0961	0,9544	0,9537	50,3407	49,7009	Não
176	0111111101111010	0,7813	0,9540	0,0001	49,9969	0,0977	0,9544	0,9537	50,3494	49,7017	Não
177	1101100000011110	0,8320	0,9540	0,0001	49,9957	0,0970	0,9544	0,9537	50,2815	49,6700	Não
178	0101000011101001	0,8320	0,9540	0,0001	49,9978	0,0979	0,9544	0,9536	50,3250	49,6925	Não
179	1110100011101111	0,7248	0,9540	0,0001	50,0017	0,0978	0,9544	0,9537	50,3181	49,6590	Não
180	0110001111011001	0,8750	0,9540	0,0001	49,9970	0,1021	0,9544	0,9537	50,3685	49,6681	Não
181	1101111110101111	0,7561	0,9540	0,0001	50,0014	0,0975	0,9544	0,9538	50,3452	49,6933	Não
182	1001001010110111	0,8438	0,9540	0,0001	49,9974	0,0977	0,9544	0,9537	50,3075	49,6418	Não
183	1100010001010110	0,8320	0,9540	0,0001	50,0019	0,1012	0,9544	0,9537	50,4005	49,6666	Não
184	1101011000101001	0,9375	0,9540	0,0001	50,0005	0,0980	0,9544	0,9537	50,2831	49,6750	Não
185	1101110011010101	0,8750	0,9540	0,0001	49,9994	0,0967	0,9544	0,9537	50,3124	49,6937	Não
186	0000110110011011	0,7771	0,9540	0,0001	49,9973	0,0989	0,9544	0,9536	50,3178	49,6952	Não
187	1000101011000011	0,8125	0,9540	0,0001	50,0004	0,1003	0,9544	0,9537	50,3281	49,6662	Não
188	1100000101000011	0,7561	0,9540	0,0001	50,0044	0,0966	0,9544	0,9537	50,4017	49,6986	Não
189	1011011010010110	0,8202	0,9540	0,0001	50,0002	0,0995	0,9544	0,9537	50,3258	49,6460	Não
190	0100110001101001	0,8320	0,9540	0,0001	50,0031	0,1021	0,9544	0,9537	50,2712	49,6811	Não
191	1101101100101101	0,7070	0,9540	0,0001	50,0018	0,0949	0,9543	0,9537	50,2678	49,6441	Não
192	1010111011001111	0,8125	0,9540	0,0001	50,0054	0,0965	0,9544	0,9537	50,3448	49,6376	Não
193	1110001110101000	0,8750	0,9540	0,0001	50,0037	0,0949	0,9543	0,9537	50,2750	49,7589	Não
194	0100011101100101	0,8438	0,9540	0,0001	50,0021	0,0942	0,9544	0,9537	50,3056	49,6979	Não
195	1010011100100111	0,6875	0,9540	0,0001	50,0037	0,0964	0,9544	0,9537	50,2941	49,6761	Não
196	0001100001110110	0,7264	0,9540	0,0001	49,9971	0,0971	0,9543	0,9537	50,3883	49,7078	Não
197	0110101111001111	0,7146	0,9540	0,0001	50,0034	0,0982	0,9544	0,9538	50,3048	49,6872	Não
198	1010000111101010	0,8750	0,9540	0,0001	49,9957	0,1011	0,9544	0,9537	50,3086	49,7116	Não
199	1100000011111101	0,8632	0,9540	0,0001	49,9963	0,0961	0,9544	0,9537	50,2911	49,6597	Não
200	1110110010011001	0,9063	0,9540	0,0001	50,0008	0,0981	0,9543	0,9537	50,3445	49,7017	Não
201	0101110110101110	0,8438	0,9540	0,0001	49,9994	0,0952	0,9543	0,9538	50,3242	49,7047	Não
202	0010111000001110	0,8750	0,9540	0,0001	50,0017	0,0957	0,9543	0,9537	50,4169	49,7379	Não
203	1110111011111100	0,5778	0,9540	0,0001	50,0007	0,0964	0,9544	0,9537	50,3319	49,7536	Não
204	1001010110101011	0,8320	0,9540	0,0001	49,9970	0,0971	0,9545	0,9537	50,3326	49,7086	Não
205	0010100011011100	0,9063	0,9540	0,0001	50,0028	0,1008	0,9543	0,9537	50,3189	49,6891	Não
206	0110110010011110	0,8438	0,9540	0,0001	50,0062	0,0951	0,9544	0,9537	50,2720	49,6998	Não
207	0110111110000010	0,8438	0,9540	0,0001	50,0003	0,1003	0,9544	0,9537	50,3765	49,6151	Não
208	1011011001011100	0,8438	0,9540	0,0001	49,9966	0,0938	0,9544	0,9538	50,3094	49,7116	Não
209	0001000101110100	0,8007	0,9540	0,0001	49,9978	0,0998	0,9544	0,9537	50,3815	49,5583	Não
210	0001011001000111	0,9063	0,9540	0,0001	49,9978	0,0972	0,9544	0,9537	50,3559	49,7059	Não
211	0100100100111100	0,7577	0,9540	0,0001	50,0021	0,0987	0,9544	0,9537	50,3071	49,6620	Não
212	0100000000001100	0,6617	0,9540	0,0001	49,9977	0,0987	0,9544	0,9537	50,2945	49,6891	Não
213	0110111000000110	0,8750	0,9540	0,0001	49,9988	0,0994	0,9543	0,9537	50,3098	49,5975	Não
214	0000001000010000	0,3278	0,9469	0,0109	50,0084	0,1410	0,9543	0,8703	51,2215	49,4030	Sim
215	0000100010011000	0,7500	0,9540	0,0001	49,9991	0,0951	0,9544	0,9537	50,2453	49,6880	Não
216	0101011111011001	0,9063	0,9540	0,0001	49,9982	0,0974	0,9543	0,9537	50,3242	49,7040	Não
217	0000110101111011	0,9063	0,9540	0,0001	50,0053	0,0974	0,9544	0,9537	50,3830	49,7593	Não
218	0111001100101101	0,8320	0,9540	0,0001	49,9926	0,0958	0,9544	0,9537	50,3063	49,6941	Não
219	1011000101111011	0,8750	0,9540	0,0001	50,0018	0,0981	0,9544	0,9538	50,2937	49,6197	Não

220	0000100110010100	0,7577	0,9540	0,0001	49,9989	0,0981	0,9543	0,9538	50,3986	49,6998	Não
221	0001000010110101	0,8438	0,9540	0,0001	50,0015	0,0988	0,9544	0,9537	50,3658	49,7173	Não
222	0101101011011110	0,9063	0,9540	0,0001	49,9974	0,0995	0,9543	0,9536	50,3174	49,6872	Não
223	1011100001100101	0,8320	0,9540	0,0001	50,0030	0,1004	0,9545	0,9537	50,3056	49,7116	Não
224	1111011000100010	0,9063	0,9540	0,0001	50,0012	0,1001	0,9544	0,9537	50,2972	49,6418	Não
225	0100111100111010	0,8438	0,9540	0,0001	49,9987	0,0991	0,9544	0,9537	50,2888	49,6613	Não
226	1011010111111011	0,8007	0,9540	0,0001	49,9984	0,0974	0,9544	0,9538	50,3204	49,7322	Não
227	1101001101100101	0,9063	0,9540	0,0001	49,9955	0,1000	0,9544	0,9537	50,3136	49,7013	Não
228	0101010011010100	0,6250	0,9540	0,0001	50,0047	0,0989	0,9544	0,9536	50,3071	49,7189	Não
229	0110100011110111	0,9063	0,9540	0,0001	49,9994	0,0988	0,9544	0,9537	50,3323	49,7303	Não
230	0001111000000010	0,8320	0,9540	0,0001	49,9984	0,1005	0,9544	0,9537	50,3170	49,7211	Não
231	0010100011101011	0,8007	0,9540	0,0001	50,0006	0,0994	0,9544	0,9537	50,3208	49,6593	Não
232	1000011011111000	0,9063	0,9540	0,0001	49,9992	0,0971	0,9543	0,9538	50,3258	49,6826	Não
233	0011101110000101	0,8632	0,9540	0,0001	50,0006	0,0977	0,9544	0,9537	50,2720	49,6426	Não
234	1110100011101000	0,8007	0,9540	0,0001	49,9998	0,0962	0,9544	0,9537	50,3647	49,6819	Não
235	0101001111111101	0,7695	0,9540	0,0001	50,0018	0,0966	0,9544	0,9537	50,3162	49,7086	Não
236	1000000001110001	0,6875	0,9540	0,0001	50,0010	0,0970	0,9543	0,9537	50,3475	49,6147	Não
237	1111100110111000	0,7695	0,9540	0,0001	49,9964	0,0985	0,9543	0,9537	50,3212	49,6643	Não
238	1101101001110000	0,8750	0,9540	0,0001	50,0013	0,0985	0,9544	0,9537	50,3357	49,6834	Não
239	0010111101101010	0,9063	0,9540	0,0001	50,0015	0,0965	0,9544	0,9537	50,3082	49,6353	Não
240	0000111101100000	0,6952	0,9540	0,0001	50,0055	0,1002	0,9544	0,9536	50,3326	49,7253	Não
241	0100001111001011	0,8945	0,9540	0,0001	49,9970	0,0992	0,9544	0,9537	50,2998	49,6647	Não
242	0000101100010000	0,7561	0,9540	0,0001	50,0012	0,0972	0,9544	0,9537	50,3246	49,6849	Não
243	1011111011110111	0,7146	0,9540	0,0001	50,0001	0,0949	0,9544	0,9537	50,3910	49,6082	Não
244	0110110110011111	0,7771	0,9540	0,0001	49,9974	0,0974	0,9544	0,9537	50,3128	49,6944	Não
245	0101110111101011	0,8750	0,9540	0,0001	49,9978	0,1018	0,9545	0,9537	50,3536	49,6475	Não
246	1010111110001001	0,8320	0,9541	0,0001	50,0051	0,0965	0,9544	0,9538	50,2823	49,7238	Não
247	1011110101111010	0,6875	0,9540	0,0001	49,9984	0,0936	0,9544	0,9536	50,3078	49,7089	Não
248	0011101011001010	0,8320	0,9540	0,0001	49,9994	0,0982	0,9545	0,9537	50,3189	49,7250	Não
249	0110101010100101	0,7695	0,9540	0,0001	50,0020	0,0981	0,9544	0,9537	50,3193	49,5991	Não
250	0110100000100100	0,8438	0,9540	0,0001	49,9976	0,0997	0,9543	0,9537	50,3574	49,6906	Não
251	1100001111011011	0,8632	0,9540	0,0001	49,9969	0,0975	0,9544	0,9537	50,3208	49,6807	Não
252	1011100110110110	0,8320	0,9540	0,0001	50,0077	0,0981	0,9544	0,9537	50,3914	49,6773	Não
253	1011000001010011	0,8632	0,9540	0,0001	50,0016	0,1014	0,9544	0,9537	50,2754	49,7059	Não
254	0110101101110010	0,7771	0,9540	0,0001	50,0032	0,0979	0,9543	0,9538	50,3544	49,6414	Não
255	0111000001010100	0,8125	0,9541	0,0001	49,9929	0,0979	0,9544	0,9537	50,3250	49,7173	Não
256	1110110100000110	0,8632	0,9540	0,0001	49,9985	0,0981	0,9543	0,9537	50,2869	49,7021	Não
257	1000011100000011	0,6936	0,9540	0,0001	49,9997	0,0972	0,9544	0,9537	50,3288	49,6490	Não
258	0110110100000001	0,8438	0,9540	0,0001	50,0017	0,0958	0,9545	0,9537	50,2594	49,7337	Não
259	1001100100101101	0,8007	0,9540	0,0001	49,9971	0,1018	0,9544	0,9537	50,3296	49,6948	Não
260	1110111011110010	0,8007	0,9540	0,0001	49,9973	0,0977	0,9544	0,9537	50,3868	49,7181	Não
261	0000110000011110	0,7382	0,9540	0,0001	50,0012	0,0956	0,9544	0,9537	50,2865	49,6288	Não
262	0000111001011101	0,9063	0,9540	0,0001	50,0028	0,1003	0,9543	0,9537	50,3189	49,6704	Não
263	0000010110110010	0,8750	0,9540	0,0001	49,9966	0,0955	0,9544	0,9537	50,3418	49,7192	Não
264	1100011101111010	0,7264	0,9540	0,0001	49,9925	0,1011	0,9544	0,9537	50,3242	49,6845	Não
265	1101001110000011	0,8125	0,9540	0,0001	49,9964	0,0959	0,9543	0,9537	50,2720	49,6696	Não
266	1010110010101001	0,7146	0,9540	0,0001	50,0000	0,0988	0,9544	0,9537	50,3296	49,6864	Não
267	0000011110100101	0,9063	0,9540	0,0001	49,9957	0,0995	0,9544	0,9537	50,3399	49,6960	Não
268	1110010100001001	0,9375	0,9540	0,0001	50,0021	0,0985	0,9543	0,9536	50,4089	49,6857	Não
269	0111001001101000	0,8320	0,9540	0,0001	49,9991	0,0907	0,9544	0,9537	50,3235	49,7478	Não
270	0011110100101100	0,9063	0,9540	0,0001	49,9985	0,0940	0,9544	0,9537	50,3235	49,7196	Não
271	1010100110011101	0,8438	0,9540	0,0001	50,0010	0,0954	0,9543	0,9537	50,3532	49,7036	Não
272	0111011000010111	0,9063	0,9540	0,0001	50,0033	0,0972	0,9544	0,9537	50,3353	49,7067	Não
273	0111110100101010	0,8320	0,9540	0,0001	50,0003	0,0970	0,9544	0,9536	50,3513	49,7044	Não
274	0110100110101101	0,8320	0,9540	0,0001	49,9970	0,0939	0,9543	0,9537	50,2640	49,7234	Não
275	0011100011001001	0,8320	0,9540	0,0001	49,9976	0,0973	0,9543	0,9538	50,4116	49,6834	Não
276	1000001110101101	0,8438	0,9540	0,0001	50,0027	0,0992	0,9544	0,9537	50,3201	49,6407	Não
277	0110111100100111	0,8750	0,9540	0,0001	49,9989	0,0975	0,9544	0,9537	50,2888	49,6891	Não
278	1100000111010000	0,8125	0,9540	0,0001	49,9975	0,0980	0,9544	0,9537	50,3567	49,6113	Não
279	1011110010001101	0,9063	0,9540	0,0001	50,0019	0,1013	0,9544	0,9537	50,2850	49,6967	Não
280	1000000010000110	0,7500	0,9540	0,0001	49,9989	0,0969	0,9544	0,9537	50,2892	49,7147	Não
281	1010000100101010	0,7500	0,9540	0,0001	49,9984	0,0961	0,9544	0,9537	50,2831	49,6517	Não
282	0000011111101101	0,8007	0,9540	0,0001	50,0012	0,0976	0,9544	0,9537	50,3246	49,7120	Não
283	1110011110110110	0,8438	0,9541	0,0001	49,9986	0,1006	0,9544	0,9536	50,3090	49,6799	Não
284	1011101011101000	0,6250	0,9540	0,0001	49,9993	0,0946	0,9544	0,9537	50,2438	49,6941	Não
285	1100010000011111	0,8125	0,9540	0,0001	49,9967	0,0982	0,9544	0,9537	50,3204	49,6452	Não
286	1100101011001101	0,8438	0,9540	0,0001	50,0045	0,0964	0,9544	0,9537	50,3422	49,7189	Não
287	0110011000110110	0,8007	0,9540	0,0001	49,9977	0,0985	0,9544	0,9537	50,3338	49,6086	Não
288	1010100000101000	0,8320	0,9540	0,0001	49,9984	0,0963	0,9544	0,9537	50,2804	49,7189	Não
289	1011010110010011	0,8750	0,9540	0,0001	49,9990	0,0965	0,9544	0,9537	50,2712	49,7234	Não
290	1000111100111101	0,8007	0,9540	0,0001	49,9966	0,0964	0,9544	0,9537	50,3136	49,6700	Não
291	0011010110001010	0,8007	0,9540	0,0001	49,9993	0,0988	0,9544	0,9537	50,2869	49,6712	Não
292	1010011111011100	0,8007	0,9540	0,0001	49,9940	0,0991	0,9544	0,9537	50,3437	49,5960	Não
293	0011100111001001	0,8125	0,9540	0,0001	50,0016	0,0976	0,9544	0,9537	50,3105	49,7227	Não
294	1000111011101111	0,7577	0,9540	0,0001	49,9969	0,0994	0,9543	0,9536	50,3281	49,7105	Não
295	1100010011101010	0,8438	0,9540	0,0001	50,0005	0,1013	0,9544	0,9536	50,3216	49,6246	Não
296	1011100010011001	0,8750	0,9540	0,0001	50,0006	0,0948	0,9544	0,9537	50,3311	49,7173	Não
297	0101110010100001	0,9063	0,9540	0,0001	49,9979	0,0934	0,9544	0,9535	50,2655	49,6960	Não
298	0001010111000001	0,7264	0,9540	0,0001	49,9973	0,0980	0,9544	0,9537	50,2735	49,6689	Não
299	1100000000111110	0,7873	0,9540	0,0001	50,0011	0,0961	0,9544	0,9537	50,2800	49,6609	Não

300	1111000010111011	0,8750	0,9540	0,0001	49,9987	0,1032	0,9544	0,9537	50,3094	49,6548	Não
301	0101101010101101	0,6875	0,9540	0,0001	49,9981	0,0971	0,9543	0,9537	50,2930	49,7009	Não
302	1111101011101010	0,8438	0,9540	0,0001	50,0014	0,0989	0,9544	0,9537	50,2998	49,6666	Não
303	1011100101101110	0,8007	0,9540	0,0001	49,9970	0,0960	0,9544	0,9536	50,2800	49,6872	Não
304	1000010000111101	1,0000	0,9540	0,0001	49,9987	0,0972	0,9544	0,9538	50,3048	49,7215	Não
305	0001111010110110	0,7889	0,9540	0,0001	50,0027	0,0954	0,9544	0,9537	50,3223	49,7284	Não
306	0101101111101100	0,9063	0,9540	0,0001	50,0011	0,0958	0,9544	0,9537	50,3544	49,6899	Não
307	0011111011011011	0,8438	0,9540	0,0001	49,9949	0,0971	0,9544	0,9537	50,2563	49,6670	Não
308	1101101011110010	0,8750	0,9540	0,0001	50,0027	0,1040	0,9544	0,9537	50,3479	49,6971	Não
309	0001110101000001	0,8750	0,9540	0,0001	49,9974	0,0993	0,9544	0,9537	50,2964	49,6628	Não
310	1010001111111111	0,6250	0,9540	0,0001	50,0030	0,0982	0,9544	0,9537	50,4234	49,6727	Não
311	0010010110100101	0,7500	0,9540	0,0001	49,9990	0,0939	0,9544	0,9537	50,3376	49,7269	Não
312	1110010000111001	0,8750	0,9540	0,0001	49,9981	0,1032	0,9544	0,9537	50,3750	49,6811	Não
313	0111101100001011	0,7889	0,9540	0,0001	50,0012	0,1003	0,9544	0,9538	50,3017	49,7246	Não
314	1001011000111110	0,9063	0,9540	0,0001	49,9960	0,0993	0,9543	0,9537	50,3056	49,6407	Não
315	1000001101100001	0,8320	0,9540	0,0001	50,0034	0,0973	0,9544	0,9537	50,3002	49,6708	Não
316	1000010111011001	0,8438	0,9540	0,0001	49,9966	0,0963	0,9544	0,9537	50,2739	49,5773	Não
317	0100011010010111	0,9688	0,9540	0,0001	49,9976	0,1020	0,9545	0,9537	50,2979	49,6983	Não
318	1000101111111100	0,8750	0,9540	0,0001	50,0022	0,0979	0,9543	0,9537	50,2876	49,7002	Não
319	0001001101111001	0,7771	0,9540	0,0001	49,9951	0,0995	0,9543	0,9537	50,3056	49,6372	Não
320	0011001001001011	0,8632	0,9540	0,0001	50,0010	0,0961	0,9544	0,9538	50,3140	49,7322	Não
321	1011101100011111	0,6929	0,9540	0,0001	49,9984	0,0990	0,9544	0,9537	50,3674	49,7028	Não
322	1111110111110110	0,4917	0,9540	0,0001	50,0000	0,0966	0,9544	0,9537	50,3281	49,7040	Não
323	1100101001110010	0,8438	0,9540	0,0001	50,0010	0,0998	0,9544	0,9537	50,2724	49,6738	Não
324	1011111010001001	0,9063	0,9540	0,0001	49,9988	0,0968	0,9543	0,9537	50,3536	49,7173	Não
325	0011011001001010	0,7577	0,9540	0,0001	49,9985	0,0968	0,9544	0,9537	50,2922	49,6994	Não
326	1011101110001101	0,8438	0,9540	0,0001	49,9990	0,0967	0,9544	0,9537	50,3662	49,6975	Não
327	0101110000100110	0,7695	0,9540	0,0001	49,9992	0,0983	0,9545	0,9537	50,3311	49,7017	Não
328	0001111010101011	0,8632	0,9540	0,0001	50,0025	0,0973	0,9543	0,9537	50,3353	49,7452	Não
329	1001010110001001	0,8320	0,9540	0,0001	50,0004	0,0968	0,9544	0,9537	50,3746	49,6666	Não
330	1110101100001101	0,8320	0,9540	0,0001	49,9963	0,1002	0,9544	0,9537	50,3132	49,7280	Não
331	1010010001101101	0,6757	0,9541	0,0001	49,9933	0,0923	0,9544	0,9538	50,2853	49,7082	Não
332	1011100001101001	0,9063	0,9540	0,0001	50,0016	0,1027	0,9544	0,9537	50,2834	49,6761	Não
333	0011011110000101	0,9063	0,9540	0,0001	50,0032	0,0939	0,9545	0,9537	50,3132	49,7147	Não
334	0101000001101011	0,8320	0,9540	0,0001	49,9980	0,0932	0,9543	0,9537	50,2712	49,7200	Não
335	0101001011001010	0,8320	0,9540	0,0001	50,0012	0,0988	0,9544	0,9538	50,3246	49,7318	Não
336	1111001001101110	0,8750	0,9540	0,0001	49,9961	0,0990	0,9544	0,9537	50,3090	49,7101	Não
337	1100100000000110	0,5938	0,9540	0,0001	50,0007	0,0964	0,9544	0,9537	50,3128	49,6784	Não
338	0010100100111110	0,7889	0,9540	0,0001	49,9991	0,0967	0,9543	0,9536	50,3452	49,6738	Não
339	0000000111010110	0,8632	0,9540	0,0001	50,0015	0,1000	0,9543	0,9537	50,2766	49,7078	Não
340	0101000111010000	0,9375	0,9540	0,0001	50,0031	0,1010	0,9544	0,9536	50,3353	49,6876	Não
341	1100001001111111	0,6929	0,9540	0,0001	49,9985	0,0998	0,9544	0,9537	50,3265	49,6864	Não
342	1000110011001001	0,8750	0,9540	0,0001	50,0009	0,0990	0,9544	0,9537	50,3506	49,6841	Não
343	1101000000001001	0,7873	0,9540	0,0001	50,0008	0,1018	0,9544	0,9538	50,2590	49,6700	Não
344	1110001100100110	0,8007	0,9540	0,0001	49,9948	0,1003	0,9544	0,9537	50,2800	49,6372	Não
345	0001001001000100	0,6563	0,9540	0,0001	50,0014	0,0994	0,9544	0,9537	50,2762	49,6777	Não
346	1111100111110010	0,8438	0,9540	0,0001	49,9976	0,1007	0,9544	0,9537	50,3071	49,6685	Não
347	1011100111010111	0,6716	0,9540	0,0001	50,0035	0,0978	0,9543	0,9537	50,4242	49,7238	Não
348	1101000101100000	0,7889	0,9540	0,0001	49,9996	0,0999	0,9544	0,9537	50,3284	49,7253	Não
349	1010000011000000	0,6304	0,9540	0,0001	49,9936	0,0968	0,9544	0,9537	50,2724	49,6441	Não
350	0111001010001010	0,8438	0,9540	0,0001	49,9944	0,0998	0,9544	0,9537	50,2838	49,6750	Não
351	0011001110110010	0,8750	0,9540	0,0001	49,9982	0,0976	0,9544	0,9537	50,3441	49,6449	Não
352	0000000010110111	0,6952	0,9540	0,0001	49,9976	0,0982	0,9544	0,9537	50,3521	49,7059	Não
353	0101111000011000	0,8125	0,9540	0,0001	50,0008	0,0958	0,9544	0,9537	50,3777	49,6899	Não
354	0010110110100010	0,8125	0,9540	0,0001	49,9965	0,0962	0,9544	0,9537	50,3208	49,7108	Não
355	1001010010011100	0,8750	0,9540	0,0001	49,9994	0,0966	0,9544	0,9537	50,3437	49,6166	Não
356	0010110011010111	0,7577	0,9540	0,0001	50,0018	0,0959	0,9544	0,9536	50,2876	49,6376	Não
357	1111001000001100	0,8438	0,9540	0,0001	49,9976	0,0979	0,9544	0,9538	50,3094	49,6468	Não
358	1010011111100111	0,7500	0,9540	0,0001	50,0031	0,0971	0,9545	0,9537	50,2884	49,7231	Não
359	1010110000101100	0,9375	0,9540	0,0001	49,9993	0,0947	0,9544	0,9537	50,2602	49,6376	Não
360	0110111010011011	0,6563	0,9540	0,0001	50,0051	0,0969	0,9543	0,9537	50,3037	49,7238	Não
361	0101000111000010	0,8632	0,9540	0,0001	50,0024	0,0953	0,9544	0,9538	50,2785	49,7086	Não
362	0111010001010001	0,8438	0,9540	0,0001	50,0043	0,0976	0,9544	0,9537	50,3147	49,7013	Não
363	1110010110111100	0,8438	0,9540	0,0001	49,9973	0,0979	0,9544	0,9537	50,2918	49,6536	Não
364	1111000001001010	0,8438	0,9540	0,0001	49,9993	0,0987	0,9544	0,9537	50,3277	49,6853	Não
365	1011011010010101	0,7500	0,9540	0,0001	49,9991	0,0989	0,9543	0,9537	50,3517	49,7002	Não
366	1101011101111010	0,6716	0,9540	0,0001	50,0027	0,0944	0,9544	0,9537	50,3414	49,7211	Não
367	0111001001111001	0,7500	0,9540	0,0001	50,0008	0,0946	0,9544	0,9537	50,3315	49,6887	Não
368	1010001110100000	0,8125	0,9540	0,0001	49,9928	0,0985	0,9544	0,9537	50,3853	49,7013	Não
369	1010000111001101	0,8007	0,9541	0,0001	50,0002	0,0927	0,9544	0,9538	50,2613	49,6895	Não
370	1011001110100011	0,9375	0,9540	0,0001	49,9995	0,0970	0,9544	0,9537	50,3754	49,6452	Não
371	0110011101000000	0,7813	0,9540	0,0001	49,9949	0,0974	0,9543	0,9538	50,2960	49,6620	Não
372	0101110111000011	0,8632	0,9540	0,0001	49,9986	0,0990	0,9544	0,9537	50,3586	49,6643	Não
373	0001101101111000	0,8438	0,9540	0,0001	49,9954	0,0951	0,9544	0,9537	50,3326	49,7147	Não
374	0001100101000111	0,8632	0,9540	0,0001	50,0035	0,1014	0,9544	0,9538	50,3372	49,6422	Não
375	0100000110101111	0,8632	0,9540	0,0001	50,0004	0,0994	0,9544	0,9537	50,3128	49,6456	Não
376	1110010110011100	0,8438	0,9540	0,0001	49,9995	0,0976	0,9544	0,9537	50,3448	49,7402	Não
377	0111011011101010	0,8438	0,9540	0,0001	49,9971	0,0979	0,9544	0,9538	50,3086	49,6609	Não
378	0000111001000001	0,7500	0,9540	0,0001	50,0001	0,0951	0,9543	0,9537	50,2880	49,6380	Não
379	0010110100111111	0,7500	0,9540	0,0001	49,9976	0,0992	0,9544	0,9537	50,3147	49,6700	Não

380	1101010101111111	0,7131	0,9540	0,0001	50,0041	0,0955	0,9544	0,9537	50,3468	49,6624	Não
381	1000010001011011	0,8750	0,9540	0,0001	49,9999	0,0987	0,9544	0,9537	50,2766	49,6964	Não
382	0011011010110111	0,7146	0,9540	0,0001	50,0012	0,0976	0,9544	0,9537	50,2953	49,7192	Não
383	0111111110111110	0,5000	0,9540	0,0001	49,9977	0,0948	0,9544	0,9537	50,2949	49,6197	Não
384	1011110111000000	0,7889	0,9540	0,0001	49,9989	0,1000	0,9544	0,9537	50,3361	49,6830	Não
385	0000101110001011	0,8320	0,9540	0,0001	50,0038	0,0962	0,9544	0,9536	50,3777	49,6979	Não
386	0000100011011111	0,9063	0,9540	0,0001	50,0012	0,0945	0,9544	0,9537	50,3521	49,7200	Não
387	0110111000101100	0,8125	0,9540	0,0001	50,0081	0,0974	0,9544	0,9537	50,3281	49,7063	Não
388	0100101000001110	0,8438	0,9540	0,0001	50,0041	0,0970	0,9544	0,9537	50,2754	49,6727	Não
389	1000011101111000	0,9063	0,9540	0,0001	49,9999	0,1003	0,9544	0,9537	50,3193	49,6548	Não
390	0000011100010000	0,7264	0,9540	0,0001	50,0022	0,1040	0,9544	0,9536	50,3929	49,6037	Não
391	1101110111011100	0,7500	0,9540	0,0001	50,0085	0,0944	0,9544	0,9538	50,3586	49,6708	Não
392	1011011101100111	0,6250	0,9540	0,0001	50,0033	0,0969	0,9544	0,9537	50,3395	49,7307	Não
393	0010011010010000	0,8320	0,9540	0,0001	49,9986	0,0943	0,9544	0,9537	50,2888	49,6235	Não
394	1100110110001110	0,7695	0,9540	0,0001	49,9958	0,0994	0,9543	0,9537	50,3368	49,6998	Não
395	1111000100101110	0,8750	0,9540	0,0001	50,0030	0,0943	0,9543	0,9537	50,3502	49,6758	Não
396	1011011110000000	0,7873	0,9540	0,0001	50,0019	0,0986	0,9544	0,9537	50,3567	49,6666	Não
397	1100011100011111	0,8125	0,9540	0,0001	50,0032	0,0952	0,9544	0,9536	50,2880	49,6990	Não
398	0101101100111111	0,7500	0,9540	0,0001	50,0048	0,0967	0,9544	0,9537	50,2979	49,6475	Não
399	0010100000110010	0,8750	0,9540	0,0001	49,9985	0,0975	0,9543	0,9537	50,2903	49,6655	Não
400	0001000000101111	0,8632	0,9541	0,0001	49,9960	0,0963	0,9544	0,9537	50,2865	49,6822	Não
401	0000010000110000	0,7500	0,9540	0,0001	50,0008	0,0975	0,9544	0,9537	50,3162	49,6841	Não
402	0111001011001101	0,7577	0,9540	0,0001	50,0009	0,1031	0,9544	0,9537	50,2827	49,6655	Não
403	1011010010101110	0,7577	0,9540	0,0001	49,9997	0,0937	0,9543	0,9537	50,2804	49,6876	Não
404	0001100111010011	0,8007	0,9540	0,0001	50,0002	0,0993	0,9544	0,9537	50,3170	49,6925	Não
405	1101000001100011	0,8750	0,9540	0,0001	50,0020	0,0957	0,9544	0,9538	50,3273	49,7395	Não
406	0000101001110001	0,8438	0,9540	0,0001	49,9969	0,0993	0,9544	0,9536	50,3201	49,6735	Não
407	1010110101111010	0,7695	0,9540	0,0001	50,0057	0,0975	0,9544	0,9537	50,3555	49,6941	Não
408	0010111110011101	0,7500	0,9540	0,0001	50,0036	0,1000	0,9544	0,9537	50,2785	49,6891	Não
409	1111001011111011	0,8007	0,9540	0,0001	50,0001	0,0980	0,9544	0,9537	50,3311	49,7280	Não
410	1001010110110010	0,8750	0,9540	0,0001	49,9989	0,1004	0,9544	0,9537	50,2903	49,7013	Não
411	1000111110011111	0,6014	0,9540	0,0001	49,9941	0,0962	0,9544	0,9537	50,2609	49,6887	Não
412	1111110011100000	0,8438	0,9540	0,0001	49,9966	0,0967	0,9544	0,9537	50,3044	49,6941	Não
413	1000101001111111	0,7131	0,9540	0,0001	49,9955	0,1008	0,9544	0,9537	50,3376	49,7120	Não
414	1110101110000010	0,8632	0,9540	0,0001	50,0003	0,0980	0,9544	0,9537	50,2892	49,6922	Não
415	1111000011111100	0,7382	0,9540	0,0001	49,9961	0,0985	0,9543	0,9537	50,3078	49,6212	Não
416	1000100101000101	0,8007	0,9540	0,0001	49,9992	0,1015	0,9544	0,9537	50,2869	49,5857	Não
417	1011011001100010	0,8320	0,9540	0,0001	49,9991	0,1031	0,9544	0,9538	50,3498	49,6288	Não
418	1001111011100101	0,8438	0,9540	0,0001	49,9931	0,0964	0,9543	0,9537	50,2563	49,6567	Não
419	0111001111000001	0,9688	0,9540	0,0001	50,0033	0,0968	0,9543	0,9537	50,3391	49,6967	Não
420	1101010111011110	0,7146	0,9540	0,0001	49,9994	0,0989	0,9544	0,9537	50,3284	49,7108	Não
421	1111010100100110	0,8632	0,9540	0,0001	49,9947	0,0957	0,9544	0,9537	50,3212	49,6502	Não
422	1110110001101010	0,8125	0,9540	0,0001	50,0040	0,1024	0,9543	0,9537	50,3323	49,6986	Não
423	1101111101110101	0,8438	0,9540	0,0001	50,0008	0,0940	0,9544	0,9537	50,3307	49,6952	Não
424	0010001001010111	0,7382	0,9540	0,0001	50,0002	0,0964	0,9544	0,9536	50,3002	49,6674	Não
425	1001011101010101	0,8007	0,9540	0,0001	50,0019	0,0986	0,9544	0,9537	50,3246	49,6872	Não
426	1110001101010000	0,8438	0,9540	0,0001	49,9943	0,0946	0,9544	0,9537	50,3162	49,5899	Não
427	1001110101100101	0,8320	0,9540	0,0001	50,0014	0,0958	0,9544	0,9537	50,3326	49,6941	Não
428	0110000000101010	0,6875	0,9540	0,0001	50,0028	0,0969	0,9544	0,9536	50,3433	49,7391	Não
429	0011000010100100	0,7561	0,9540	0,0001	50,0023	0,0975	0,9543	0,9537	50,2815	49,6761	Não
430	0001100011100100	0,7577	0,9540	0,0001	50,0026	0,0986	0,9544	0,9537	50,3613	49,7410	Não
431	1100011011110001	0,6875	0,9540	0,0001	50,0067	0,0954	0,9544	0,9537	50,3380	49,7154	Não
432	1001011001110011	0,8320	0,9540	0,0001	50,0011	0,0941	0,9544	0,9537	50,2769	49,6746	Não
433	0111101100011011	0,7264	0,9540	0,0001	49,9996	0,0965	0,9544	0,9537	50,3071	49,6780	Não
434	0101001010000010	0,8438	0,9540	0,0001	50,0010	0,0977	0,9543	0,9537	50,2872	49,6906	Não
435	1100001011100110	0,9063	0,9540	0,0001	49,9979	0,0943	0,9544	0,9536	50,2647	49,6826	Não
436	0100111010110010	0,8007	0,9540	0,0001	49,9995	0,0967	0,9543	0,9537	50,3014	49,6967	Não
437	0110000000111111	0,7443	0,9540	0,0001	50,0006	0,0995	0,9544	0,9537	50,3155	49,7047	Não
438	0110011011010001	0,8750	0,9540	0,0001	50,0041	0,0992	0,9544	0,9537	50,3075	49,6731	Não
439	0001110010001100	0,8438	0,9540	0,0001	49,9988	0,0969	0,9544	0,9536	50,3315	49,6197	Não
440	1010110000011001	0,8750	0,9540	0,0001	49,9974	0,0980	0,9544	0,9537	50,3208	49,6407	Não
441	1111011100010111	0,6875	0,9540	0,0001	50,0043	0,0979	0,9544	0,9536	50,3162	49,6830	Não
442	1101011111101101	0,6327	0,9540	0,0001	49,9916	0,0988	0,9544	0,9537	50,3185	49,5796	Não
443	0011111111100000	0,7813	0,9540	0,0001	49,9988	0,1025	0,9543	0,9537	50,3052	49,7253	Não
444	1011100100111001	0,8438	0,9540	0,0001	49,9969	0,0976	0,9544	0,9538	50,3044	49,6918	Não
445	0000010010001101	0,8438	0,9540	0,0001	50,0010	0,0964	0,9544	0,9537	50,3002	49,6593	Não
446	0101000010100110	0,8750	0,9540	0,0001	49,9990	0,0966	0,9544	0,9537	50,2510	49,7089	Não
447	0100001110100101	0,8320	0,9540	0,0001	49,9970	0,1012	0,9544	0,9537	50,3002	49,6361	Não
448	1010010101101010	0,7695	0,9540	0,0001	50,0020	0,0982	0,9543	0,9537	50,3380	49,7219	Não
449	0011110110111100	0,8438	0,9540	0,0001	49,9999	0,0985	0,9544	0,9537	50,3605	49,7002	Não
450	1110110001110110	0,8007	0,9540	0,0001	49,9975	0,0978	0,9543	0,9537	50,3689	49,6796	Não
451	0011011001010100	0,8438	0,9540	0,0001	49,9909	0,0985	0,9543	0,9537	50,3326	49,7162	Não
452	0010010010100111	0,8320	0,9540	0,0001	49,9980	0,0931	0,9544	0,9537	50,2510	49,7089	Não
453	0010000110110000	0,8632	0,9540	0,0001	50,0011	0,0976	0,9544	0,9536	50,3136	49,6792	Não
454	0100010011101010	0,8007	0,9540	0,0001	49,9972	0,0976	0,9544	0,9538	50,2918	49,6582	Não
455	0101111101100110	0,7070	0,9540	0,0001	50,0023	0,0963	0,9543	0,9537	50,2846	49,6815	Não
456	0110000100000000	0,5000	0,9540	0,0001	50,0030	0,1007	0,9544	0,9538	50,3307	49,6235	Não
457	0110101000010010	0,8632	0,9540	0,0001	49,9959	0,0986	0,9544	0,9537	50,2663	49,7158	Não
458	0011011000111101	0,8320	0,9540	0,0001	50,0009	0,0975	0,9544	0,9537	50,3147	49,6902	Não
459	1101011110010001	0,9375	0,9540	0,0001	49,9973	0,0999	0,9544	0,9537	50,3132	49,6902	Não

460	0010011001111101	0,7577	0,9540	0,0001	49,9959	0,0970	0,9544	0,9537	50,2609	49,6544	Não
461	0010111101011001	0,8632	0,9540	0,0001	50,0031	0,0969	0,9544	0,9537	50,3510	49,7040	Não
462	0010110010010010	0,7695	0,9540	0,0001	50,0018	0,0944	0,9544	0,9537	50,3052	49,6758	Não
463	0101111011011000	0,7889	0,9540	0,0001	49,9961	0,0978	0,9544	0,9537	50,3822	49,6433	Não
464	0110101010101011	0,6716	0,9540	0,0001	50,0011	0,0991	0,9543	0,9537	50,3361	49,6059	Não
465	0001110101001001	0,8320	0,9540	0,0001	49,9937	0,0969	0,9544	0,9537	50,2796	49,6975	Não
466	1011000010010101	0,8438	0,9540	0,0001	49,9987	0,0943	0,9544	0,9537	50,2640	49,7490	Não
467	0111101100011100	0,8438	0,9541	0,0001	50,0029	0,0967	0,9544	0,9537	50,3033	49,7189	Não
468	0101001001111000	0,8632	0,9540	0,0001	49,9986	0,1012	0,9544	0,9537	50,2705	49,7097	Não
469	1010100110100000	0,8007	0,9540	0,0001	49,9972	0,0937	0,9544	0,9538	50,2991	49,6826	Não
470	0011100111010101	0,8750	0,9540	0,0001	50,0030	0,0988	0,9544	0,9537	50,3281	49,6773	Não
471	0101011110000111	0,8438	0,9540	0,0001	49,9988	0,1005	0,9544	0,9537	50,3666	49,6807	Não
472	1111000101111001	0,8007	0,9540	0,0001	49,9954	0,0972	0,9544	0,9537	50,2796	49,7128	Não
473	1001010111001110	0,8125	0,9540	0,0001	50,0054	0,0992	0,9544	0,9537	50,4162	49,6258	Não
474	1111111110001001	0,6929	0,9540	0,0001	50,0005	0,0968	0,9544	0,9537	50,3052	49,6609	Não
475	1111110001111100	0,8438	0,9540	0,0001	49,9984	0,0987	0,9544	0,9536	50,3262	49,7021	Não
476	0001110110010110	0,8750	0,9541	0,0001	49,9978	0,1028	0,9544	0,9537	50,2754	49,6624	Não
477	1000001001001000	0,6075	0,9540	0,0001	50,0023	0,0990	0,9544	0,9537	50,2975	49,7101	Não
478	0101101011000001	0,8320	0,9540	0,0001	49,9966	0,0941	0,9544	0,9536	50,2941	49,6231	Não
479	0101011101101100	0,8632	0,9540	0,0001	50,0017	0,0963	0,9544	0,9537	50,2651	49,6983	Não
480	1110100110000000	0,9688	0,9540	0,0001	50,0000	0,0984	0,9544	0,9537	50,2975	49,6510	Não
481	0101000011110000	0,7561	0,9540	0,0001	50,0030	0,0984	0,9544	0,9537	50,3254	49,6422	Não
482	1101111110010011	0,7500	0,9540	0,0001	49,9971	0,0965	0,9543	0,9536	50,3140	49,7005	Não
483	1010001001011101	0,8320	0,9540	0,0001	49,9981	0,0987	0,9544	0,9537	50,3021	49,7391	Não
484	1010101011000100	0,9375	0,9540	0,0001	50,0023	0,0970	0,9544	0,9537	50,2792	49,6410	Não
485	0110011110001000	0,8438	0,9540	0,0001	50,0006	0,0987	0,9543	0,9537	50,3437	49,6693	Não
486	1010000010000000	0,6875	0,9540	0,0001	50,0015	0,0988	0,9544	0,9537	50,3208	49,6830	Não
487	1111100001110010	0,8750	0,9540	0,0001	50,0004	0,0960	0,9544	0,9537	50,2609	49,6498	Não
488	0111010100111100	0,8125	0,9540	0,0001	50,0028	0,0979	0,9544	0,9537	50,3387	49,7070	Não
489	1101110000010010	0,9063	0,9540	0,0001	49,9965	0,0970	0,9544	0,9537	50,2674	49,7028	Não
490	1101110100110000	0,8125	0,9540	0,0001	50,0036	0,0992	0,9544	0,9538	50,3101	49,7047	Não
491	1000001001110000	0,8438	0,9540	0,0001	50,0037	0,0981	0,9544	0,9537	50,3353	49,7181	Não
492	1001110000110000	0,8007	0,9540	0,0001	50,0028	0,0971	0,9544	0,9537	50,2773	49,6708	Não
493	1010011100101111	0,7500	0,9540	0,0001	50,0026	0,0958	0,9544	0,9537	50,3037	49,7005	Não
494	0111101111100010	0,8438	0,9540	0,0001	50,0017	0,0987	0,9544	0,9537	50,3956	49,7051	Não
495	1010000000100111	0,8125	0,9540	0,0001	49,9982	0,0946	0,9544	0,9537	50,2666	49,7253	Não
496	1000010000101011	0,8750	0,9540	0,0001	49,9972	0,1002	0,9544	0,9537	50,3479	49,6796	Não
497	1010010100101110	0,8750	0,9540	0,0001	49,9998	0,0965	0,9544	0,9537	50,2907	49,6925	Não
498	1100001110011001	0,8125	0,9540	0,0001	50,0031	0,0968	0,9544	0,9537	50,3349	49,6300	Não
499	0101110110010001	0,8750	0,9540	0,0001	49,9973	0,0966	0,9544	0,9536	50,2720	49,6651	Não
500	1101010110011101	0,8125	0,9540	0,0001	49,9957	0,0956	0,9544	0,9537	50,2991	49,6696	Não

Tabela C.3: Resultados para o teste com o modelo com rotação da sensitividade