CRIPTOGRAFIA CAÓTICA: TRANSFORMAÇÃO DO GATO DE ARNOLD APLICADO À SEGURANÇA COMPUTACIONAL

Filipi Maciel Rodrigues Jardim[1]; Marina Martins Teixeira[2]; Robert Cristiano Almeida Viana[3]; Thiago de Jesus Oliveira Durães[4]; Neila Marcelle Gualberto Leite[5]

Resumo: A criptografia é uma técnica de codificação e decodificação de mensagens e é amplamente utilizada, tanto como ferramenta militar como civil. Existem várias técnicas de criptografia, dentre as quais pode-se destacar a criptografia caótica. Neste trabalho, são apresentadas as bases matemáticas desta técnica e é desenvolvido um algoritmo em SCILAB para retratar a aplicação de uma técnica de criptografia caótica de imagens chamada de transformação do gato de Arnold.

Palavras–chave: Criptografia.Teoria do Caos. Gato de Arnold.

Introdução

Há séculos a necessidade de decifrar mensagens criptografadas vem instigando a criação de técnicas de codificação e decodificação eficientes e cada vez mais seguras. Usada, inclusive, como estratégia de guerras, os principais códigos desenvolvidos são baseados em princípios matemáticos. Utilizadas tanto como ferramentas militares para segurança nacional como civil, a criptografia é amplamente utilizada nas transações bancárias, na internet para acesso a sites, e-mails e até mesmo em simples mensagens enviadas por celulares. A criptografia caótica, desenvolvida a partir de sistemas caóticos, tem características que vêm sendo estudadas ao longo dos anos, e sua complexidade se baseia na sensibilidade do sistema às condições iniciais dadas, onde uma pequena mudança nos dados de entrada gera um resultado totalmente diferente do esperado. Assim, a criptografia caótica é qualificada como um problema de difícil solução, ao contrário de muitos sistemas criptográficos já desenvolvidos até então [ROSKIN e CASPER]. A transformação do Gato de Arnold é um método de criptografia caótico, que foi desenvolvido pelo matemático russo Vladimir Igorevich Arnold em torno de 1960 [VALDEVINO]. O objetivo desse trabalho é

1 Acadêmico do curso de Ciência da Computação do IFNMG, Campus Montes Claros. Email: filipimacielrj@gmail.com

2 Acadêmico do curso de Ciência da Computação do IFNMG, Campus Montes Claros. Email: mteixeira196@gmail.com

3 Acadêmico do curso de Ciência da Computação do IFNMG, Campus Montes Claros. Email: rcristiano53@gmail.com

4 Acadêmico do curso de Ciência da Computação do IFNMG, Campus Montes Claros. Email:thiagooduraes@gmail.com

5 Docente do IFNMG, Campus Montes Claros. Curso de Ciência da Computação. Email: neilagualberto@gmail.com

retratar a aplicação da transformação do Gato de Arnold no desenvolvimento de um algoritmo, que realiza criptografia caótica de uma imagem.

Metodologia e Descrição do Algoritmo

Para alcançar o objetivo deste trabalho, foi realizada revisão bibliográfica sobre o tema, estudo das bases matemáticas de aritmética modular e álgebra linear que dão suporte à aplicação. Em seguida, desenvolveu-se um algoritmo que será descrito a seguir. O funcionamento do método criado por Arnold é baseado na seguinte definição da aritmética modular: *Seja α um número real, então a notação α mod 1 denota o único número no intervalo [0,1) que difere de α por um número inteiro*. Esta operação pode ser aplicada tanto em números reais quanto em pares ordenados (x, y) de números reais. O par ordenado $(x, y)\ mod\ 1$ denota o par $(x\ mod\ 1, y\ mod\ 1)$, que denota um ponto do quadrado unitário $S = \{(x, y) \mid 0 \leq x < 1, 0 \leq y < 1\}$. A transformação do gato de Arnold é uma aplicação do tipo T: $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ definida pela fórmula: $T : (x, y) \rightarrow (x + y, x + 2y)\ mod\ 1$. Os passos para a transformação são: primeiramente, cisalhamento na direção x com fator 1, seguido de reagrupamento: $(x, y) \rightarrow (x + y, y)\ mod\ 1$; depois, cisalhamento na direção y com fator 1, seguido de reagrupamento: $(x, y) \rightarrow (x, x + y)\ mod\ 1$. Para a representação de uma imagem na forma digital, esta é dividida em quadrados discretos, denominados pixels. Uma imagem definida em um quadrado *S*, possui p^2 pixels (p pixel de largura por p pixels de altura), uniformemente espaçados a cada $1/p$ unidades nas direções x e y. Aplicando a transformação do gato de Arnold, cada ponto de pixel do quadrado S é transformado em outro ponto de pixel de S. Segundo [HOWARD e RORRES, 2012], não existe nenhuma função elementar que relacione o período com a quantidade p de pixels do lado do quadrado *S*. Para a demonstração da transformação do gato de Arnold, foi elaborado um algoritmo, utilizando o software gratuito e de código aberto para computação numérica Scilab [SCILAB] e uma de suas bibliotecas para processamento de imagens, a *Scilab Image and Video Processing toolbox*, SIVP [SIVP]. O dado de entrada do algoritmo é uma imagem de ordem quadrada, que é convertida em uma matriz, na qual cada pixel é representado por um elemento de uma matriz bidimensional. Neste trabalho foi implementada uma função que utiliza o valor de *p* (que representa a quantidade de pixels do lado da imagem) e um ponto arbitrário para determinar o período que representa a quantidade de iteraçãoes necessárias para a transformação do gato de Arnold numa imagem de p^2 pixels. A função aplica sucessivas transformações no ponto pré-estabelecido e conta a quantidade de iterações necessárias para que o ponto retorne à sua posição original. A transformação do gato de Arnold é aplicada em cada uma das matrizes que formam a imagem colorida, e seu tempo de execução depende da quantidade de iterações, que é calculada em função das dimensões da imagem. A cada iteração do algoritmo, o resultado da transformação é atualizado e apresentado na tela, repetindo esse processo até a imagem original ser obtida novamente.

Resultados

O algoritmo implementado foi executado com várias imagens de diferentes tamanhos. O número de iterações é calculado em uma função do algoritmo, que garante o retorno à imagem original ao fim da execução. Pode-se perceber que não existe relação entre o tamanho da imagem e a quantidade de iterações, ou de número de iterações e tempo de execução.

Conclusões

A transformação do gato de Arnold aplicada à criptografia caótica permite que o remetente realize um certo número de iterações em uma imagem, e a envie para um destinatário que irá descriptografá-la realizando o restante da quantidade de iterações necessárias para que a imagem volte à sua forma original. Devido à complexidade e custo da transformação linear realizada no algoritmo, o processo realizado exige alto custo computacional, variando de acordo com as configurações do úsuario e também da dimensão da imagem que pretende criptografar. Por este motivo, conclui-se que, o método desenvolvido por Arnold, apesar do seu custo de execução, é muito eficiente e seguro, e com o avanço da tecnologia e da necessidade de transmissão de dados com total sigilo, se torna uma alternativa para as empresas.

Referências

HOWARD, Anton. RORRES, Chris. Álgebra Linear com Aplicações. 10º edição. Editora Bookman, 2012.

ROSKIN, K. M. and CASPER, J. B. From Chaos To Cryptography. Disposnível em: <http://www.gaianxaos.com/pdf/unsorted/chaos_and_cryptography.pdf>. Acesso em 10 de fevereiro de 2016.

SCILAB: Open Source Software for Numerical Computation. Disponível em: <http://www.scilab.org/scilab/about>. Acessado em 8 de Dezembro de 2015.

SIVP: Scilab Image and Video Processing Toolbox. Disponível em: <http://sivp.sourceforge.net/>. Acesso em 8 de Dezembro de 2015.

VALDEVINO, André. Criptografia Caótica. Disponível em: < https://www.ucb.br/sites/100/103/TCC/22006/AndreValdevino.pdf> . Acesos em 10 de Fevereiro de 2016.