República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(21) BR 102020002072-2 A2

(22) Data do Depósito: 30/01/2020

(43) Data da Publicação Nacional: 10/08/2021

(54) Título: PROCESSO PARA CRIPTOGRAFIA DE IMAGENS ATRAVÉS DA TRANSFORMADA MANOBRÁVEL DE FOURIER EM CORPOS FINITOS

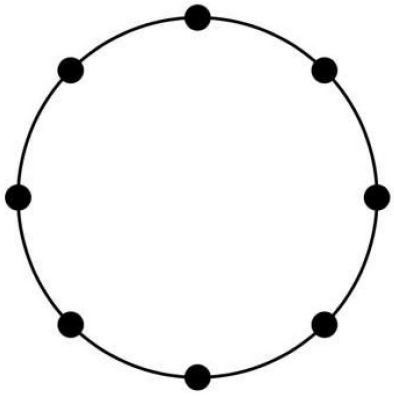
(51) Int. Cl.: H04L 9/32; G06F 21/62; H04L 9/00.

(52) CPC: H04L 9/32; G06F 21/62; H04L 9/00.

(71) Depositante(es): UNIVERSIDADE FEDERAL DE PERNAMBUCO.

(72) Inventor(es): MARCOS A. A. GONDIM; JOSÉ RODRIGUES DE OLIVEIRA NETO; JULIANO BANDEIRA LIMA; FELIPE ALBERTO BARBOSA SIMÃO FERREIRA.

(57) Resumo: PROCESSO PARA CRIPTOGRAFIA DE IMAGENS ATRAVÉS DA TRANSFORMADA MANOBRÁVEL DE FOURIER EM CORPOS FINITOS. A presente invenção introduz a transformada manobrável de Fourier em corpos finitos (TMFCF) propiciando um processo de criptografia de imagens que atende a aspectos de segurança contra ataques, sensibilidade da chave secreta e complexidade computacional. Esta transformada corresponde a generalização da conhecida transformada em corpos finitos, obtida ao aplicar uma rotação de pares de vetores, em um dado corpo finito, da base original da transformada de Fourier em corpos finitos. Nós provemos exemplos ilustrativos acerca da construção da TMFCF e propomos um esquema de criptografia baseado nesta nova transformada; o princípio do método é utilizar os ângulos das referidas rotações como parâmetros secretos. Demostramos que o esquema proposto é resistente contra os principais ataques criptográficos e possui uma menor complexidade computacional comparado a outros métodos publicados na literatura.



PROCESSO PARA CRIPTOGRAFIA DE IMAGENS ATRAVÉS DA TRANSFORMADA MANOBRÁVEL DE FOURIER EM CORPOS FINITOS

CAMPO DA INVENÇÃO

[001] A presente invenção trata um processo de criptografia de imagens através de uma transformada em corpos finitos, mais especificamente a Transformada Manobrável de Fourier em Corpos Finitos (TMFCF), que também é parte integrante desta invenção. A transformada desenvolvida possui aplicação na área de segurança de informação, visando sua utilização em, por exemplo, criptografia de imagens, marca d'água e processamento de sinais no domínio criptografado.

ANTECEDENTES DA INVENÇÃO

[002] Sistemas criptográficos são importantes para garantir a segurança de dados importantes e informações sensíveis que não devem ser reveladas ao público. Na literatura de patentes, pode-se citar, por exemplo, o documento BR 202015018204-5 que propõe um esquema para utilização de imagem cifrada em documentos de identificação pessoal, por exemplo, para evitar fraudes e/ou falsificações. O documento reivindica um esquema para que agentes de fiscalização possam efetuar a leitura da cifra bidimensional e decodifica-la por meio de um aparelho móvel. O método de cifragem em si não é especificado.

[003] No documento de patente BR 112019013130-2 é descrito um método para busca e atualização em estruturas de dados criptografados com objetivo de minimizar ou eliminar o vazamento de informações importantes em servidores potencialmente não confiáveis.

[004] O documento PI 0603105-6, que relata um sistema de criptografia de dados impressos ou exibidos em tela que podem estar embutidos em

imagens. Esta patente não trata da cifragem da imagem em si mas de elementos que possam vir a compor uma imagem. Os dados (caracteres alfanuméricos) são cifrados e substituídos na imagem em questão.

[005] No documento de patente BR 102015019037-9 é descrito um método criptográfico que utiliza a ferramenta matemática conhecida por séries infinitas com razões múltiplas submetendo um arquivo computacional à uma hegemonização dos bytes, conforme apresentado pelos inventores. Este método não trata os dados em um domínio discreto.

[006] No documento de patente BR 112018072515-3 é apresentado um método para realizar criptografia com o uso de curvas elípticas implementadas em múltiplas camadas aritmeticas. Em outro aspecto desta invenção, provê-se um método para realizar comunicação segura entre dispositivos.

[007] No documento de patente BR 112018016559-0 é reivindicado um método de criptografia com o uso de transformadas de múltiplas passagens compactas.

[008] Na literatura acadêmica também existem diversos trabalhos publicados descrevendo métodos criptográficos. No recente trabalho de (Hua e Zhou, 2017), por exemplo, uma cifra de imagem usando embaralhamento baseado em blocos e filtragem de imagem foi introduzido; utilizando máscaras geradas aleatoriamente, a operação de filtragem pode espalhar pequenas alterações na imagem original em todos os pixels da imagem cifrada.

[009] Em (Hua *et al.*, 2018), os autores apresentam um algoritmo para cifragem de imagens baseado no mapa *Logistic-Sine-coupling*; um novo algoritmo de permutação é desenvolvido para rapidamente permutar os pixels da imagem enquanto um algoritmo de difusão é executado para espalhar pequenas mudanças na imagem original por toda imagem cifrada.

[010] Em (*Hua et al.*, 2018), um esquema de cifragem para proteger imagens médicas usando embaralhamento de alta velocidade e difusão adaptativa de pixels é descrito.

[011] O esquema proposto nesta invenção pode ser melhor comparado com aqueles cujo núcleo também é uma transformada linear. A principal ideia por trás desse tipo de esquema é empregar, além de outras ferramentas, uma transformada discreta parametrizável cuja matriz mude de acordo com uma chave secreta. A classe de transformadas mais bem conhecida para este contexto é a classe das transformadas fracionárias. Tais transformadas correspondem a uma generalização da correspondente transformada ordinária, em que uma potência arbitrária da matriz da transformada pode ser calculado.

[012] Em (Annaby, 2016), por exemplo, os autores propuseram um esquema de cifragem de imagens baseando-se em transformadas discretas fracionárias de Fourier geradas por matrizes aleatórias.

[013] Em (Kang e Tao, 2018), uma transformada fracionária de Hartley multiparamétrica com preservação de realidade é definida e um esquema de cifragem para imagens coloridas baseado em tal transformada é proposto. Em (Kang *et al.*, 2018), uma técnica similar baseada em uma transformada angular fracionária discreta multiparamétrica e com preservação de realidade é sugerida e utilizada em um algoritmo de cifragem de imagens.

[014] A invenção proposta neste documento, se baseia em uma transformada manobrável de Fourier em corpos finitos, definida também como segundo objeto desta invenção. Além de cumprir diversos requerimentos de segurança, o esquema de cifragem proposto demonstra-se prover benefícios relacionados a complexidade aritmética, quando comparada a outros esquemas baseados em transformadas fracionárias no domínio dos reais ou dos números complexos. Ainda, trata-se de um

esquema flexível e atinge um desempenho satisfatório com poucos passos de cifragem.

[015] Geralmente, transformadas em corpos finitos são no formato de uma transformada de Fourier em que a N-ésima raiz complexa de uma unidade, utilizada como núcleo da transformada, é substituída pela N-ésima raíz de uma unidade definida em uma estrutura algébrica finita. Desta forma todos os cálculos necessários são realizados por meio de aritmética modular.

[016] A presente invenção é motivada pelo crescente interesse em ferramentas matemáticas e aplicações relacionadas a sinais sobre grafos. Consideramos o fato de que a base de uma transformada de comprimento N, em corpos finitos, no formato da Fourier diagonaliza a Laplaciana $\mathbf{L}(C_N)$ de um grafo cíclico não-direcionado C_N, de N vértices; isso é equivalente a propriedade da convolução cíclica, também válida em cenários de corpos finitos. Nós utilizamos este fato para identificar pares de autovetores da $\mathbf{L}(C_N)$ relacionados ao mesmo autovalor e realizamos uma rotação bidimensional de tais pares. Desta forma, a base da TMFCF é formada por tais pares de autovetores rotacionados em vez dos originalmente utilizados em uma transformada em corpo finito convencional.

[017] De certa forma, a TMFCF pode ser vista como uma extensão do método publicado em (Fracastoro e Magli, 2017), em que é definida uma transformada de Fourier manobrável no domínio dos números complexos. Entretanto, a TMFCF, requer o uso de conceitos inerentemente relacionados a estrutura algébrica em que é definida (a noção do arco de um elemento em um corpo finito, por exemplo).

[018] A seguir são descritos alguns conceitos importantes para o entendimento da transformada manobrável de Fourier em corpos finitos: a transformada de Fourier e trigonometria em corpos finitos (Blahut, 2010;

Lima e Campello Souza, 2011). Além disso também é caracterizada uma rotação bidimensional em um corpo finito. Considere que $\mathbb{F}_p$ denota um corpo com p elementos e que p é um número primo.

[019] Seja $\omega \in \mathbb{F}_p$ um elemento de ordem multiplicativa $\mathrm{ord}(\omega) = N$. A transformada de Fourier em corpos finitos (TFCF) de $\boldsymbol{x} = [x(n)] \in \mathbb{F}_p^N$ é a sequência $\boldsymbol{X} = [X(k)] \in \mathbb{F}_p^N$ com componentes

$$X(k) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n)\, \omega^{kn}, \qquad k = 0,1, \dots, N-1.$$

Na forma matricial, pode-se ter $\boldsymbol{X} = \boldsymbol{F}\boldsymbol{x}$, em que

$$\boldsymbol{F} = [F(k,n)], \qquad F(k,n) = \frac{1}{\sqrt{N}} \omega^{kn}.$$

Sua inversa é calculada por

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k) \omega^{-kn}.$$

[020] É um fato conhecido que, analogamente à transformada discreta de Fourier, a transformada de Fourier em corpos finitos respeita o teorema da convolução cíclica (Blahut, 2010). De forma equivalente, a matriz $\boldsymbol{F}$ em $\mathbb{F}_p$ diagonaliza qualquer matriz circulante com elementos pertencentes ao mesmo corpo.

[021] Seja $\alpha \in \mathbb{F}_p$ um elemento de ordem multiplicativa $\mathrm{ord}(\alpha)$ e $i = \sqrt{-1} (\mathrm{mod}\, p)$. As funções cosseno e seno em corpos finitos relacionadas ao arco do elemento α^θ, $\theta = 0,1, \dots, \mathrm{ord}(\alpha) - 1$, são dadas respectivamente por

$$\cos_\alpha(\theta) = \frac{\alpha^\theta + \alpha^{-\theta}}{2}$$

e

$$\mathrm{sen}_\alpha(\theta) = \frac{\alpha^\theta - \alpha^{-\theta}}{2i}.$$

[022] Utilizando as funções de cosseno e seno em corpos finitos é possível definir um operador de rotação em um corpo finito como

$$\mathrm{R}_{\alpha}(\theta) = \begin{bmatrix} \cos_{\alpha}(\theta) & \mathrm{sen}_{\alpha}(\theta) \\ \text{-}\mathrm{sen}_{\alpha}(\theta) & \cos_{\alpha}(\theta) \end{bmatrix}.$$

É necessário especificar o elemento α na expressão anterior, pois cossenos e senos em corpos finitos calculados em respeito a diferentes elementos podem resultar em valores distintos.

OBJETIVO DA INVENÇÃO

[023] O objetivo da invenção é criptografar imagens por meio de um processo bem estabelecido de passos e com base na definição da transformada manobrável de Fourier em corpos finitos.

SUMÁRIO DA INVENÇÃO

[024] É um dos objetos da presente invenção propiciar um processo para criptografia de imagens. Neste processo, blocos da imagem original são transformados no domínio da transformada manobrável de Fourier em corpos finitos com base em uma sequência de ângulos definidos por um gerador de números pseudoaleatórios baseado em teoria do caos. A chave utilizada para gerar esta sequência de ângulos é utilizada como a chave secreta da cifra aplicada. O processo compreende as seguintes etapas: (1) divida a imagem em blocos de igual dimensão; (2) use a chave secreta para gerar uma sequência de ângulos; (3) calcule a transformada bidimensional de cada bloco; (4) obtenha uma imagem intermediária formada pelos blocos transformados; (5) embaralhe os pixels da imagem intermediária; (6) divida a imagem embaralhada no passo 5 em blocos de igual dimensão; (7) calcule a transformada bidimensional de cada bloco para obter a imagem cifrada.

[025] É um adicional objeto da presente invenção propiciar um processo para o cálculo da transformada manobrável de Fourier em corpos finitos.

[026] Estes objetos da presente invenção serão melhor compreendidos e valorizados a partir da descrição detalhada da invenção e de seus exemplos que têm como objetivo apenas ilustrar um dos inúmeros meios de se realizar a invenção, não limitando portanto seu escopo.

BREVE DESCRIÇÃO DAS FIGURAS

[027] A Figura 1 apresenta um grafo cíclico.

[028] A Figura 2 apresenta o grafo em rede toroidal $\mathcal{T}_{20,20}$.

[029] A Figura 3 apresenta um diagrama de blocos do esquema de cifragem proposto. Os números brancos dentro dos círculos pretos indicam a ordem de execução dos passos para obter a imagem cifrada I_c a partir da correspondente imagem original I.

[030] A Figura 4 apresenta cinco exemplos de imagens utilizadas em nossos experimentos; da esquerda para a direita, as colunas correspondem, respectivamente, a imagem original, a imagem cifrada, ao histograma original e ao histograma após cifragem.

BREVE DESCRIÇÃO DAS TABELAS

[031] A Tabela 1 apresenta resultados experimentais quanto ao coeficiente de correlação ($|r|$), entropia normalizada ($|\overline{H}|$), NPCR_d e UACI_d (testes de ataque diferencial) e NPCR_s (teste de sensibilidade da sequência secreta); o símbolo ($'$) é usado para imagens cifradas.

[032] A Tabela 2 apresenta resultados acerca de uma comparação com métodos existentes. São apresentados valores do comprimento da chave secreta, coeficiente de correlação (r), NPCR_d e UACI_d (teste de ataque diferencial), e entropia normalizada ($\overline{H}$); o símbolo ($'$) é usado para

imagens cifradas e o símbolo (−) indica que a métrica de segurança correspondente não é claramente fornecida pelos autores do referido trabalho. Texto em negrito é utilizado para destacar os dois melhores resultados de cada métrica.

DESCRIÇÃO DETALHADA DA INVENÇÃO

[033] Para introduzir a transformada manobrável de Fourier em corpos finitos consideramos uma intepretação do domínio em que se encontram os vetores que se deseja calcular a transformada baseada em teoria dos grafos. Será apresentado o cálculo da transformada unidimensional e bidimensional.

[034] No caso unidimensional, uma alternativa para calcular a transformada de Fourier em um corpo $\mathbb{F}_p$ é considerar a representação em grafo do eixo no domínio do tempo, com condições de limites periódicos; essa representação é dada por um grafo circular como o C_8 (Figura 1). Seguindo um procedimento similar ao usado para definir a transformada de Fourier sobre grafos, nós consideramos a Laplaciana de C_N módulo i, $\mathbf{L}(C_N) \equiv \mathrm{circ}([2, p-1, \ldots, p-1\,])(\mathrm{mod}\, p)$, em que $\mathrm{circ}(.)$ denota uma matriz circulante cujas linhas correspondem a versões sucessivamente deslocadas do argumento. Devido a propriedade da convolução cíclica, sabemos que as linhas de uma matriz $\boldsymbol{F}$, $N \times N$, formam uma base ortogonal de $\mathbf{L}(C_N)$. Nesse caso, λ_k, o autovalor para o qual o autovetor $\boldsymbol{v}_k$ de $\mathbf{L}(C_N)$ na k-ésima linha de $\boldsymbol{F}$ é relacionado, é a k-ésima componente da transformada de Fourier em corpos finitos de $[2, -1, \ldots, -1]$, isto é

$$\lambda_k = 2 - \omega^k - \omega^{-k} = 2 - 2\cos_\omega(k).$$

A simetria par do corpo finito formado pela função cosseno implica que $\lambda_k = \lambda_{N-k}$. Então, se N é par, λ_0 e $\lambda_{N/2}$ são autovalores de multiplicidade um de $\mathbf{L}(C_N)$; se N é ímpar, o único autovalor de multiplicidade um é λ_0.

Em ambos os casos, existem outros $\lceil N/2-1 \rceil$ autovalores distintos de multiplicidade dois.

[035] Como $\mathbf{L}(C_N)$ possui autovalores repetidos, as linhas de $\boldsymbol{F}$ não constituem sua autobase única. De fato, pode-se obter outra autobase ao aplicar uma rotação no corpo finito de autovetores dispostos autoespaço. Isso nos leva a definição da transformada manobrável de Fourier em corpos finitos; a matriz da TMFCF é denotada por $\boldsymbol{F}_S$ e basicamente consiste em substituir linhas $\boldsymbol{v}_k$ e $\boldsymbol{v}_{N-k}$ de $\boldsymbol{F}$, $k \neq 0$ e $k \neq N/2$ (se N é par), por $\boldsymbol{v}'_k$ e $\boldsymbol{v}'_{N-k}$ de acordo com

$$\begin{bmatrix} \boldsymbol{v}'_k \\ \boldsymbol{v}'_{N\text{-}k} \end{bmatrix} = \begin{bmatrix} \cos_{\alpha_k}(\theta_k) & \operatorname{sen}_{\alpha_k}(\theta_k) \\ -\operatorname{sen}_{\alpha_k}(\theta_k) & \cos_{\alpha_k}(\theta_k) \end{bmatrix} \begin{bmatrix} \boldsymbol{v}_k \\ \boldsymbol{v}_{N\text{-}k} \end{bmatrix}.$$

Adicionalmente, $\boldsymbol{v}'_0 = \boldsymbol{v}_0$ e, se N é par, $\boldsymbol{v}'_{N/2} = \boldsymbol{v}'_{N/2}$.

[036] A TMFCF é uma transformada multiparamétrica cuja definição desambígua requer a especificação de vetores $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_{\lceil N/2-1 \rceil}]$ e $\boldsymbol{\theta} = [\theta_1, \theta_2, \ldots, \theta_{\lceil N/2-1 \rceil}]$. Se $\boldsymbol{\theta}$ é um vetor vazio, a TMFCF coincide com a transformada de Fourier em corpos finitos. Por motivos de simplicidade, deste ponto em diante, assumiremos que $\boldsymbol{\alpha}$ é um vetor constante cujas componentes coincidem com ω, o elemento utilizado para obter vetores v_k, $k = 0,1, \ldots, N-1$ (linhas de $\boldsymbol{F}$).

[037] O cálculo de $\boldsymbol{X}_S \in \mathbb{F}_p^N$, a TMFCF do vetor $\boldsymbol{x} \in \mathbb{F}_p^N$, pode ser realizado computando inicialmente a transformada de Fourier em corpos finitos de tal vetor e em seguida multiplicando o resultado por $\mathbf{R}(\boldsymbol{\theta}) \in \mathbb{F}_p^{N \times N}$, a matriz que rotaciona cada par de autovetores. Então, temos que $\boldsymbol{X}_S = \boldsymbol{F}_S(\boldsymbol{\theta})\boldsymbol{x} = \mathbf{R}(\boldsymbol{\theta})\boldsymbol{F}\boldsymbol{x} = \mathbf{R}(\boldsymbol{\theta})\boldsymbol{X}$. Consequentemente, a TMFCF inversa pode ser calcular por $\boldsymbol{x} = \boldsymbol{F}^{-1}\mathbf{R}(-\boldsymbol{\theta})\boldsymbol{X}_S$.

[038] Analogamente ao caso unidimensional, a transformada de Fourier em corpos finitos bidimensional pode ser derivada de um grafo em rede toroidal $\mathcal{T}_{N_1,N_2} = C_{N_1} \times C_{N_2}$ (Figura 2). Sem perdas por generalização,

vamos considerar $N = N_1 = N_2$. Pelos Teoremas 2 e 3 em (Fracastoro e Magli, 2017), também válidos no cenário atual, sabemos que a base da transformada de Fourier em corpos finitos bidimensional é uma autobase de $\mathbf{L}(\mathcal{T}_{N,N})$, com autovalores $\mu_{r,s} = \lambda_r + \lambda_s = \mu_{s,r},\ r,s = 0,1,\dots,N-1$, tais que

- $\mu_{r,s} = \mu_{s,r} = \mu_{r,N-r} = \mu_{N-r,r} = \mu_{s,N-s} = \mu_{N-r,N-s} = \mu_{N-s,N-r},\ r,s = 1,2,\dots,N/2-1,\ r \neq s$, tem multiplicidade 8;
- $\mu_{r,N-r} = \mu_{N-r,r} = \mu_{N-r,N-r},\ r = 1,2,\dots,N/2-1,\ r \neq s,$ tem multiplicidade 4;
- $\mu_{r,s} = \mu_{s,r} = \mu_{r,N-s} = \mu_{N-s,r}\ (\text{ou } \mu_{r,s} = \mu_{s,r} = \mu_{N-r,s} = \mu_{s,N-r}),\ r = 0, N/2$ e $s = 1,2,\dots,N/2-1$ (ou $r = 1,2,\dots,N/2-1$ e $s = 0, N/2$), tem multiplicidade 4;
- $\mu_{0,N/2} = \mu_{N/2,0}$ tem multiplicidade 2;
- $\mu_{0,0}$ e $\mu_{N/2,N/2}$ tem multiplicidade um.

[039] Para construir a matriz da 2D-TMFCF, consideramos pares de autovalores relacionados ao mesmo autovalor de $\mathbf{L}(\mathcal{T}_{N,N})$ e aplicar uma rotação em corpo finito. Mais especificamente, consideramos vetores $\boldsymbol{u}_{r,s}$ e $\boldsymbol{u}_{s,r},\ r \neq s$, da base da transformada de Fourier em corpos finitos bidimensional. Eles são auto vetores de $\mathbf{L}(\mathcal{T}_{N,N})$ com o autovalor $\mu_{r,s}$, e suas componentes são rearranjadas de forma que elas pertençam a $\mathbb{F}_p^{1\times N^2}$. Os autovetores rotacionados $\boldsymbol{u}'_{r,s}$ e $\boldsymbol{u}'_{s,r}$ são obtidos por

$$\begin{bmatrix}\boldsymbol{u}'_{r,s}\\ \boldsymbol{u}'_{s,r}\end{bmatrix} = \begin{bmatrix}\cos_\omega(\boldsymbol{\theta}_{r,s}) & \operatorname{sen}_\omega(\boldsymbol{\theta}_{r,s})\\ -\operatorname{sen}_\omega(\boldsymbol{\theta}_{r,s}) & \cos_\omega(\boldsymbol{\theta}_{r,s})\end{bmatrix}\begin{bmatrix}\boldsymbol{u}_{r,s}\\ \boldsymbol{u}_{s,r}\end{bmatrix}.$$

[040] Usando a nova autobase, pode-se obter o operador da 2D-TMFCF como uma matriz $\boldsymbol{F}_S^{2D}$ no corpo $\mathbb{F}_p^{N^2\times N^2}$. Então, de forma similar ao caso 1D, a 2D-TMFCF de $\boldsymbol{x} \in \mathbb{F}_p^{N\times N}$ pode ser obtida por $\boldsymbol{X}_S^{2D} = \boldsymbol{F}_S^{2D}(\boldsymbol{\theta}^{2D})\boldsymbol{x} = \mathbf{R}(\boldsymbol{\theta}^{2D})\boldsymbol{F}^{2D}\boldsymbol{x} = \mathbf{R}(\boldsymbol{\theta}^{2D})\boldsymbol{X}$; neste caso, $\boldsymbol{\theta}^{2D}$ é um vetor de comprimento $N(N-1)/2$ de ângulos em um corpo finito e $\boldsymbol{X}$ é a 2D-TMFCF de $\boldsymbol{x}$.

[041] Para utilização da TMFCF em criptografia de imagens propomos um esquema que emprega um vetor $\boldsymbol{\theta}^{2D}$ de ângulos em um corpo finito

gerados usando uma chave secreta. O procedimento para criptografar uma imagem I (texto claro) é ilustrado no diagrama de blocos apresentado na Figura 3 e envolve os seguintes passos:

1. Divida a imagem I em blocos de $N \times N$ pixels;
2. Use uma chave secreta para gerar o vetor $\boldsymbol{\theta}^{2\mathrm{D}}$ de comprimento $N(N-1)/2$;
3. Calcule a 2D-TMFCF de cada bloco de I usando o vetor $\boldsymbol{\theta}^{2\mathrm{D}}$ gerado no passo 2;
4. Obtenha uma imagem intermediária I' com os blocos transformados que foram calculados no passo 3;
5. Embaralhe os pixels de I' aplicando o mapa de Arnold (Chen *et al.*, 2013) três vezes e obtenha uma segunda imagem intermediária I'';
6. Divida a segunda imagem intermediária I'' em blocos de $N \times N$ pixels;
7. Calcule a 2D-TMFCF de cada bloco de I'' usando o mesmo vetor $\boldsymbol{\theta}^{2\mathrm{D}}$ e obtenha a imagem cifrada I_c.

[042] Para realizar a decifragem podemos executar os passos anteriores, do 1 ao 7, na ordem contrária; naturalmente, nos passos 7 e 3 deve ser usada a 2D-TMFCF inversa e no passo 5 deve ser usado o mapa de Arnold inverso.

[043] O vetor de ângulos $\boldsymbol{\theta}^{2D}$ pode ser obtido, por exemplo, usando gerador de números aleatórios baseado em teoria do caos (Beirami *et al.*, 2014; Liu e Tong, 2016; Stojanovski e Kocarev, 2001; Stojanovski *et al.*, 2001) devido a alta sensibilidade às condições iniciais de tais geradores.

[044] Para comprovar a eficiência do esquema de criptografia de imagens proposto foram realizados experimentos computacionais para avaliação de aspectos de segurança e sensibilidade.

[045] Nos experimentos, realizamos a cifragem de 141 imagens em escala de cinza (8 bits) de dimensão 512×512. As imagens foram extraídas dos volumes *Textures*, *Aerials* e *Miscellaneous* da base de imagens da Universidade da Califórnia do Sul, Instituto de Processamento

de Imagens e Sinais (USC-SIPI *Image Database*), e foram convertidas para o formato mencionado. Nós consideramos o corpo finito $\mathbb{F}_{257}$ pois $p = 257$ é o menor primo que cobre o intervalo $[0,255]$. Escolhemos $N = \mathrm{ord}(\omega) = 128$ e o elemento $\omega = 9$ para calcular as funções trigonométricas em corpo finito e definir as transformações requeridas nos passos da cifragem. É importante mencionar que imagens de dimensões diferentes de 512×512 podem ser cifradas combinando *zero-padding* e o uso de blocos com dimensões diferentes 128×128. O vetor $\boldsymbol{\theta}^{2D}$ foi gerado aleatoriamente e possui $128 \times \frac{127}{2} = 8128$ componentes inteiros no intervalo $[0,127]$.

[046] Teste 1: segurança contra ataques estatísticos

[047] As imagens cifradas resultantes possuem um aspecto completamente ruidoso, sem reter vestígios visuais que correspondam as imagens originais; isto pode ser visto na Figura 4. Também é possível notar que independentemente do histograma antes da cifragem, os valores dos pixels de cada imagem cifrada são uniformemente distribuídos. Este comportamento qualitativo possui relação com algumas métricas numéricas. Mais especificamente, nós calculamos os valores absolutos do coeficiente de correlação e a entropia normalizada de todas as imagens originais e cifradas. Os resultados sugerem que ataques estatísticos contra o esquema proposto não seriam efetivos (ver Tabela 1).

[048] Teste 2: segurança contra ataques diferenciais

[049] Nós verificamos que o esquema pode resistir a ataques diferenciais. Isso foi avaliado realizando o seguinte experimento 100 vezes para cada uma das imagens originais: (i) selecione aleatoriamente um pixel de uma imagem original I e inverta seu bit menos significativo para produzir uma imagem minimamente modificada $\tilde{I}$; (ii) cifre as imagens I e $\tilde{I}$ usando a mesma chave secreta e obtenha as imagens cifradas I_c e $\tilde{I}_c$,

respectivamente; (iii) compare I_c e $\tilde{I}_c$ calculando a taxa de mudança de pixels (NPCR, *number of pixels change rate*) e a intensidade de mudança média unificada (UACI, *unified average changing intensity*) (Wu *et al.*, 2011). Os valores mínimos e máximos, obtidos após considerar todas as imagens de teste e apresentados na Tabela 1, são próximos dos valores teóricos esperados ($\mathrm{NPCR} \approx 99{,}61\%$ e $\mathrm{UACI} \approx 33{,}46\%$) (Wu *et al.*, 2011).

[050] Teste 3: sensibilidade

[051] Nós avaliamos a sensibilidade da invenção proposta a pequenas mudanças no vetor $\boldsymbol{\theta}^{2D}$. O teste foi realizado executando o seguinte experimento 100 vezes para cada uma das imagens originais: (i) cifre uma imagem I usando o vetor $\boldsymbol{\theta}^{2D}$ de ângulos no corpo finito e obtenha a imagem cifrada I_c; (ii) selecione aleatoriamente um bit entre os utilizados na representação binária das componentes de $\boldsymbol{\theta}^{2D}$, inverta-o e obtenha um vetor $\widetilde{\boldsymbol{\theta}}^{2D}$ minimamente modificado; (iii) use $\widetilde{\boldsymbol{\theta}}^{2D}$ para decifrar I_c e obtenha $\tilde{I}$; (iv) compare $\tilde{I}$ e I calculando o NPCR. O resultado, também apresentado na Tabela 1, indicam que o esquema é altamente sensível a mudanças em $\boldsymbol{\theta}^{2D}$. Além disso, é importante mencionar que o vetor $\boldsymbol{\theta}^{2D}$ possui 8128×7 bits de comprimento, isto é, o vetor é suficientemente longo para tornar um ataque direto impraticável.

[052] Teste 4: comparação com outros esquemas

[053] Teste 4(a): segurança

[054] Neste aspecto, nossa invenção é comparada com os métodos apresentados em (Mikhail *et al.*, 2017; Annaby *et al.*, 2016; Kang e Tao, 2018; Kang *et al.*, 2018; Yang *et al.*, 2015; Kaur e Kumar, 2018; Lima *et al.*, 2015), conforme Tabela 2. Sendo mais específico, nós consideramos o comprimento das chaves secretas, os menores valores máximos do coeficiente de correlação, as médias entre os valores máximos e mínimos de NPCR_d e UACI_d mais próximos do valor teórico de tais métricas e os

maiores valores mínimos de entropia normalizada. Na Tabela 2 nós indicamos $2^{256} - 2^{56896}$ como o comprimento das chaves do nosso método pois, como discutido anteriormente, o vetor $\boldsymbol{\theta}^{2D}$, usando na parametrização da 2D-TMFCF, pode ser produzido por um gerador de números aleatórios cujas condições iniciais são tomadas como a chave secreta. Resumidamente, isso significa que o esquema proposto fornece flexibilidade em escolher a chave secreta e ao mesmo tempo satisfaz os requerimentos de segurança. Pelos resultados fornecidos, é possível notar que o esquema proposto está sempre entre os melhores. Uma alternativa para aumentar ainda mais a segurança do nosso esquema é utilizar diferentes vetores $\boldsymbol{\theta}^{2D}$ para transformar cada bloco nos passos 3 e 7 do processo de cifragem ou utilizar um vetor $\boldsymbol{\alpha}$ não constante.

[055] Teste 4(b): sensibilidade

[056] Já que todas as operações aritméticas dos passos da transformação do esquema proposto são realizadas módulo p, o método é altamente sensível a modificações nos parâmetros secretos, na imagem original e na imagem cifrada. Desta forma, o esquema fornece altas taxas de mudança de pixel após cifragem ou decifragem, conforme discutido anteriormente. Em outras palavras, podemos dizer que, se a aritmética módulo p é usada, uma pequena mudança no vetor (inverter um bit em uma de suas componentes, por exemplo) não necessariamente leva a pequenas mudanças na 2D-TMFCF; isso ocorre devido a redução modular aplicada durante o cálculo da transformada. Isso trás um certo nível de segurança ao usar poucas etapas de cifragem ao comparar com métodos baseados em operações no domínio dos números reais ou complexos (Annaby *et al.*, 2016; Kang e Tao, 2018; Kang *et al.*, 2018; Kang *et al.*, 2015; Gao *et al.*, 2018; Hsue e Chang, 2015). Neste contexto, esses métodos podem ser mais suscetíveis a alguns tipos de ataques específicos.

[057] Teste 4(c): complexidade computacional

[058] A TMFCF, que constitui o núcleo do esquema de cifragem proposto, é de fácil construção e pode ser calculada de forma eficiente como um produto entre uma matriz esparsa funções trigonométricas em um dado corpo finito e uma TFCF convencional; tal produto envolve $\mathcal{O}(N)$ operações aritméticas e uma TFCF pode ser calculada, por exemplo, com algoritmos rápidos cuja complexidade é de $\mathcal{O}(N \times \log_2 N)$. Então, a complexidade computacional total para calcular a TMFCF é de $\mathcal{O}(N \times \log_2 N)$. Adicionalmente, dependendo do primo que caracteriza o corpo $\mathbb{F}_p$, é possível calcular a TFCF com algoritmos livres de multiplicação. Em contraste, outras transformadas normalmente empregadas em cifragem de imagens normalmente requerem $\mathcal{O}(N^2)$ operações aritméticas reais ou complexas (Kang *et al.*, 2018; Kang *et al.*, 2015; Gao *et al.*, 2018; Hsue e Chang, 2015).

[059] Teste 4(d): representação da imagem

[060] Naturalmente, as imagens cifradas produzidas por nosso esquema possuem componentes no domínio dos inteiros. Mais especificamente, se $p = 257$, os valores dos pixels correspondentes estão no intervalo $[0{,}256]$ e não podem ser representados com uma codificação usual de 8 bits. De qualquer forma, algumas simples alternativas podem ser adotadas para contornar esta restrição. Poder-se-ia representar, por exemplo, cada inteiro no intervalo de $[0{,}254]$ usando o byte correspondente no intervalo $[00000000{,}11111110]$; o byte 11111111 seria utilizado como um tipo de *flag*, que seria seguido de um "nono" bit 0 (referente ao valor 1) para representar o valor decimal 255 (referente ao valor 256). Assumindo que os símbolos (valores dos pixels) em uma imagem cifrada são equiprováveis, o número médio de bits por pixel na representação proposta seria dado por $(255 \times 8 + 2 \times 9)/257 = 8{,}0077821012$. Isso

significa que o número de bits adicionais devido a cifragem é desprezível. Além disso, já que não são necessários arredondamentos, se a chave correta é utilizada, a imagem recuperada pela decifragem é idêntica a imagem original correspondente. Por outro lado, métodos de cifragem de imagens que utilizam transformadas definidas em um corpo infinito precisam lidar estratégias de truncamento e preservação de realidade (Annaby *et al.*, 2016; Kang e Tao, 2018; Kang *et al.*, 2018; Venturini e Duhamel, 2004); isso pode levar a problemas relacionados a precisão e considerável aumento na taxa de bits das imagens cifradas, já que é necessária a representação em ponto flutuante.

REFERÊNCIAS BIBLIOGRÁFICAS

[061] Annaby, M.H.; Rushdi, M.A.; Nehary, E.A. Image encryption via discrete fractional Fourier-type transforms generated by random matrices, Signal Process., Image Commun. 49 (2016) 25–46.

[062] Beirami, A.; Nejati, H.; Callegari, S. Fundamental performance limits of chaotic- map random number generators, in: Proceedings of the 52nd Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, 2014, pp. 1126–1131.

[063] Blahut, R.E. Fast Algorithms for Signal Processing, Cambridge University Press, 2010.

[064] Chen, F.; Wong, K.W.; Liao, X.; Xiang, T. Period distribution of the generalized discrete Arnold cat map for $N = 2e$, IEEE Trans. Inform. Theory 59 (5) (2013) 3249–3255.

[065] Fracastoro, G; Magli, E. Steerable discrete Fourier transform, IEEE Signal Process. Lett. 24 (3) (2017) 319–323.

[066] Gao, Z.; Chen, D.; Zhang, W.; Cai, S. Colour image encryption algorithm using one- time key and FrFT, IET Image Process. 12 (4) (2018) 472–478.

[067] Hsue, W.L.; Chang, W.C. Real discrete fractional Fourier, Hartley, generalized Fourier and generalized Hartley transforms with many parameters, IEEE Trans. Circuits Syst. I. Regul. Pap. 62 (10) (2015) 2594–2605.

[068] Hua, Z.; Zhou, Y. Design of image cipher using block-based scrambling and image filtering, Inform. Sci. 396 (8) (2017) 97–113.

[069] Hua, Z.; Yi, S.; Zhou, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion, Signal Process. 144 (3) (2018) 134–144.

[070] Hua, Z; Jin, F.; Xu, B.; Huang, H. 2D logistic-sine-coupling map for image encryption, Signal Process. 149 (8) (2018) 148–161.

[071] Kang, X.; Ming, A.; Tao, R. Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption, IEEE Trans. Circuits Syst. Video Technol. (2018).

[072] Kang, X.; Tao, R. Color image encryption using pixel scrambling operator and reality-preserving MPFRHT, IEEE Trans. Circuits Syst. Video Technol. (2018).

[073] Kang, X.; Zhang, F.; Tao, R. Multichannel random discrete fractional Fourier transform, IEEE Signal Process. Lett. 22 (9) (2015) 1340–1344.

[074] Kaur, M.; Kumar, V. Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain, IET Image Process. 12 (7) (2018) 1273–1283.

[075] Lima, J.B.; Campello Souza, R.M. Finite field trigonometric transforms, Appl. Algebra Eng. Commun. Comput. 22 (5–6) (2011) 393–411.

[076] Lima, J.B.; Madeiro, F.; Sales, F.J.R. Encryption of medical images based on the cosine number transform, Signal Process., Image Commun. 35 (2015) 1–8.

[077] Liu, Y.; Tong, X. Hyperchaotic system-based pseudorandom number generator, IET Inf. Secur. 10 (6) (2016) 433–441.

[078] Mikhail, M.; Abouelseoud, Y.; ElKobrosy, G. Two-phase image encryption scheme based on FFCT and fractals, Secur. Commun. Netw. (2017) 1–13.

[079] Stojanovski, T.; Kocarev, L.; Chaos-based random number generators – part I: analysis, IEEE Trans. Circuits Syst. I 48 (3) (2001) 281–288.

[080] Stojanovski, T.; Pihl, J.; Kocarev, L. Chaos-based random number generators – part II: practical realization, IEEE Trans. Circuits Syst. I 48 (3) (2001) 382–385.

[081] USC-SIPI Image Database, http://sipi.usc.edu/database/.

[082] Venturini I.; Duhamel, P. Reality preserving fractional transforms, in: Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Montreal, Canada, 2004, pp. 205–208.

[083] Wu, Y.; Noonan, J.P.; Agaian, S. NPCR And UACI randomness tests for image encryption, Cyber J.: J. Sci. Technol. J. Sel. Areas Telecommun. (2011) 31–38.

[084] Yang, Y.-G.; Pan, Q.-X.; Sun, S.-J.; Xu, P. Novel image encryption based on quantum walks, Sci. Rep. 5 (2015) 1–9.

Reivindicações

1. Processo para criptografia de imagens caracterizado por compreender as seguintes etapas:

   a. divida uma imagem I em blocos de $N \times N$ pixels;

   b. use uma chave secreta para gerar um vetor $\boldsymbol{\theta}^{2D}$ de comprimento $N(N-1)/2$;

   c. calcule a 2D-TMFCF de cada bloco de I usando o vetor $\boldsymbol{\theta}^{2D}$ gerado no passo (b);

   d. obtenha uma imagem intermediária I' com os blocos transformados que foram calculados no passo (c);

   e. embaralhe os pixels de I' e obtenha uma segunda imagem intermediária I'';

   f. divida a segunda imagem intermediária I'' em blocos de $N \times N$ pixels;

   g. calcule a 2D-TMFCF de cada bloco de I'' usando o mesmo vetor $\boldsymbol{\theta}^{2D}$ e obtenha a imagem cifrada I_c.

2. Processo de decifragem, de acordo com a reivindicação 1, caracterizado por compreender as seguintes etapas:

   a. divida a imagem cifrada I_c em blocos de $N \times N$ pixels;

   b. use a mesma chave secreta usada no processo de cifragem para gerar o vetor $\boldsymbol{\theta}^{2D}$ de comprimento $N(N-1)/2$;

   c. calcule a 2D-TMFCF inversa de cada bloco de I_c usando o vetor $\boldsymbol{\theta}^{2D}$ e obtenha a imagem intermediária I';

   d. desembaralhe os pixels de I' e obtenha uma segunda imagem intermediária I'';

e. divida a segunda imagem intermediária I'' em blocos de $N \times N$ pixels;

f. calcule a 2D-TMFCF inversa de cada bloco de I'' usando o mesmo vetor $\boldsymbol{\theta}^{2D}$ e obtenha a imagem original I.

FIGURA 1

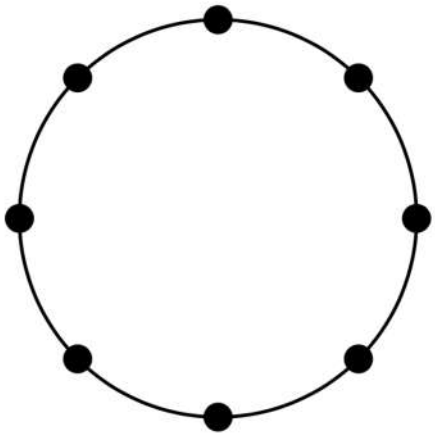


FIGURA 2

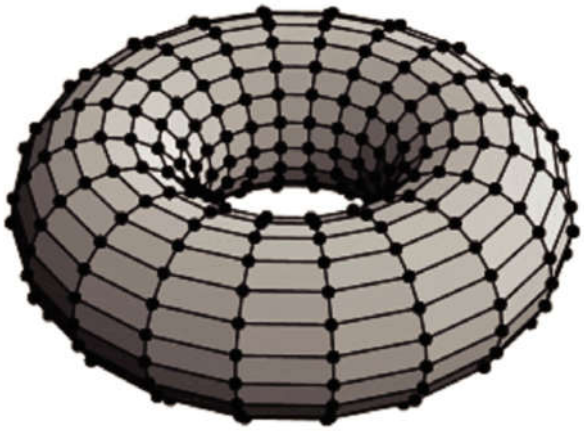


FIGURA 3

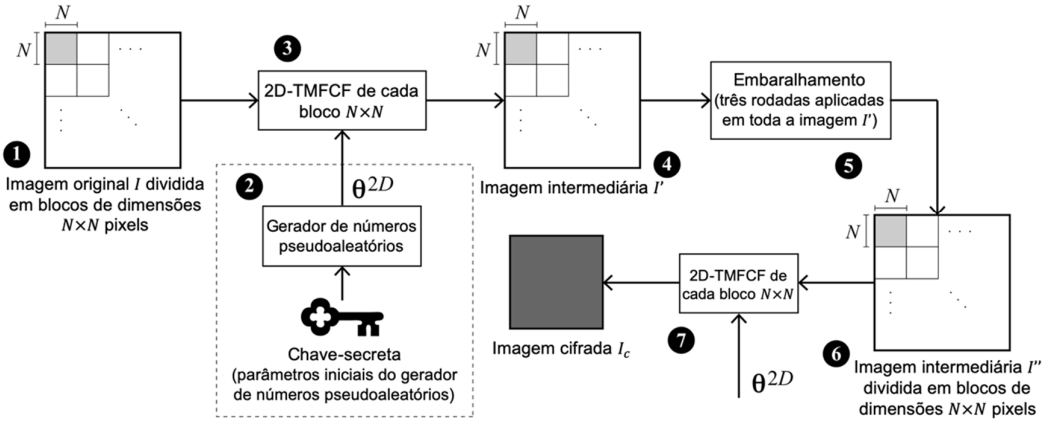


FIGURA 4

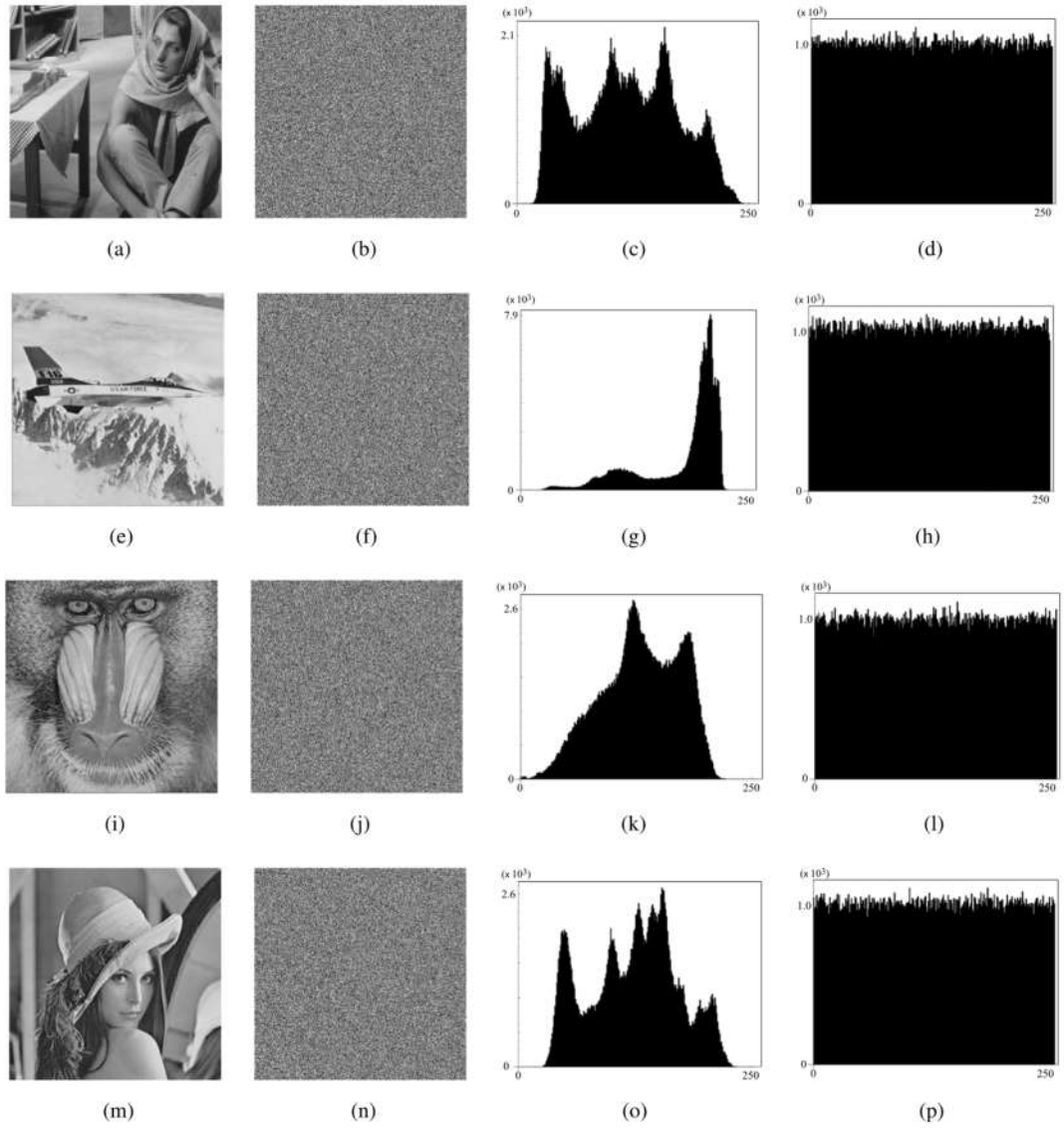


TABELA 1

	$\lvert \boldsymbol{r} \rvert$	$\lvert \boldsymbol{r'} \rvert$	$\overline{\boldsymbol{H}}$	$\overline{\boldsymbol{H'}}$	$\mathrm{NPCR}_{\boldsymbol{d}}$	$\mathrm{UACI}_{\boldsymbol{d}}$	$\mathrm{NPCR}_{\boldsymbol{s}}$
Min	0,02624	0,00001	0,06246	0,99989	99,56	33,27	99,57
Máx	1,00000	0,00837	0,95488	0,99993	99,65	33,66	99,65

TABELA 2

Método	Comp. chave	$\lvert \boldsymbol{r'} \rvert$	$\mathrm{NPCR}_{\boldsymbol{d}}$	$\mathrm{UACI}_{\boldsymbol{d}}$	$\lvert \overline{\boldsymbol{H'}} \rvert$
Invenção	$\mathbf{2^{256} - 2^{56896}}$	$\mathbf{0,00001 - 0,00837}$	$\mathbf{99,56 - 99,65}$	$\mathbf{33,27 - 33,66}$	$\mathbf{0,99989 - 0,99993}$
(Yang *et al.*, 2015)	2^{325}	$0{,}00136 - 0{,}00859$	$99{,}64 - 99{,}68$	$33{,}40 - 33{,}66$	$0{,}99982 - 0{,}99998$
(Kaur e Kumar, 2018)	$\mathbf{2^{26952}}$	$\mathbf{0,00010 - 0,00730}$	$99{,}67 - 99{,}70$	$32{,}58 - 33{,}66$	$0{,}99963 - 0{,}99976$
(Kang e Tao, 2018)	–	$0{,}00010 - 0{,}00910$	$99{,}86 - 100{,}00$	$26{,}16 - 33{,}34$	–
(Kang *et al.*, 2018)	$\approx 2^{325}$	$0{,}00016 - 0{,}00842$	$99{,}99 - 100{,}00$	$33{,}30 - 33{,}34$	–
(Annaby *et al.*, 2016)	–	$0{,}00982 - 0{,}39088$	$100{,}00$	$33{,}24 - 33{,}45$	$0{,}99965 - 0{,}99967$
(Lima *et al.*, 2015)	2^{160}	$0{,}00010 - 0{,}01320$	$99{,}58 - 99{,}99$	$33{,}19 - 33{,}56$	$0{,}99820 - 0{,}99990$
(Mikhail *et al.*, 2017)	2^{71}	$0{,}00010 - 0{,}00910$	$\mathbf{99,54 - 99,71}$	$\mathbf{33,44 - 33,52}$	$\mathbf{0,99997 - 0,99999}$

Resumo

PROCESSO PARA CRIPTOGRAFIA DE IMAGENS ATRAVÉS DA TRANSFORMADA MANOBRÁVEL DE FOURIER EM CORPOS FINITOS

A presente invenção introduz a transformada manobrável de Fourier em corpos finitos (TMFCF) propiciando um processo de criptografia de imagens que atende a aspectos de segurança contra ataques, sensibilidade da chave secreta e complexidade computacional. Esta transformada corresponde a generalização da conhecida transformada em corpos finitos, obtida ao aplicar uma rotação de pares de vetores, em um dado corpo finito, da base original da transformada de Fourier em corpos finitos. Nós provemos exemplos ilustrativos acerca da construção da TMFCF e propomos um esquema de criptografia baseado nesta nova transformada; o princípio do método é utilizar os ângulos das referidas rotações como parâmetros secretos. Demostramos que o esquema proposto é resistente contra os principais ataques criptográficos e possui uma menor complexidade computacional comparado a outros métodos publicados na literatura.