CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
UNIDADE ARAXÁ

RAFAEL RODRIGUES SILVA

MÉTODO DE CRIPTOGRAFIA CAÓTICA DE VÍDEOS PARA TRANSMISSÕES AO VIVO

ARAXÁ/MG

2023

RAFAEL RODRIGUES SILVA

MÉTODO DE CRIPTOGRAFIA CAÓTICA DE VÍDEOS PARA TRANSMISSÕES AO VIVO

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Automação Industrial, do Centro Federal de Educação Tecnológica de Minas Gerais - CEFET/MG, como requisito parcial para obtenção do grau de Bacharel em Engenharia de Automação Industrial.

Orientador: Prof. Dr. Cirilo Gonçalves Júnior
Coorientador: Prof. Dr. Leandro Resende Mattioli

ARAXÁ/MG

2023

MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
DEPARTAMENTO DE ELETROMECÂNICA - AX

ATA Nº 90 / 2023 - DELMAX (11.57.05)

Nº do Protocolo: 23062.060617/2023-50

Araxá-MG, 11 de dezembro de 2023.

Ata de Defesa do Trabalho de Conclusão de Curso de Engenharia de Automação Industrial do Aluno Rafael Rodrigues Silva

Às quatorze horas do dia oito de dezembro de dois mil e vinte e três, reuniu-se, no Centro Federal de Educação Tecnológica de Minas Gerais - CEFET-MG/ Campus Araxá, a Comissão Examinadora de Trabalho de Conclusão de Curso para julgar, em exame final, o trabalho intitulado **MÉTODO DE CRIPTOGRAFIA CAÓTICA DE VÍDEOS PARA TRANSMISSÕES AO VIVO**, como requisito parcial para a obtenção do grau de Bacharel em Engenharia de Automação Industrial. Abrindo a sessão, o Presidente da Comissão, Prof. Dr. Cirilo Gonçalves Jr., após dar a conhecer aos presentes o teor das Normas Regulamentares do Trabalho Final, concedeu a palavra ao candidato, **Rafael Rodrigues Silva**, para a exposição de seu trabalho. Após a apresentação, seguiu-se a arguição pelos examinadores, com a respectiva defesa do candidato. Ultimada a arguição, a Comissão se reuniu, sem a presença do candidato e do público, para julgamento e expedição do resultado final. Após a reunião da Comissão Examinadora, o candidato foi considerado: **APROVADO**, obtendo nota final de: **97**/100 (noventa e sete). O resultado final foi comunicado publicamente ao candidato pelo Presidente da Comissão. O aluno, abaixo assinado, declara que o trabalho ora identificado é da sua autoria material e intelectual, excetuando-se eventuais elementos, tais como passagens de texto, citações, figuras e datas, desde que devidamente identificada a fonte original. Declara ainda, neste âmbito, não violar direitos de terceiros. Nada mais havendo a tratar, o Presidente encerrou os trabalhos. O Prof. Leandro Resende Mattioli, responsável pela disciplina "Trabalho de Conclusão de Curso II", lavrou a presente ATA, que, após lida e aprovada, será assinada por todos os membros participantes da Comissão Examinadora e pelo candidato.

Araxá, 08 de dezembro de 2023.

Assinado eletronicamente por:
• Presidente e Orientador: Prof. Dr. Cirilo Gonçalves Jr.
• Coorientador: Prof. Dr. Leandro Resende Mattioli
• Membro Titular: Prof. Dr. Mateus Antunes Oliveira Leite
• Membro Titular: Profª. Drª. Aline Fernanda Bianco Mattioli
• Professor da Disciplina TCC 2: Prof. Dr. Leandro Resende Mattioli
• Aluno: Rafael Rodrigues Silva

(Assinado digitalmente em 11/12/2023 09:14)
ALINE FERNANDA BIANCO MATTIOLI
PROFESSOR ENS BASICO TECN TECNOLOGICO
DFGAX (11.57.03)
Matrícula: 2720850

(Assinado digitalmente em 11/12/2023 08:28)
CIRILO GONCALVES JUNIOR
PROFESSOR ENS BASICO TECN TECNOLOGICO
DFGAX (11.57.03)
Matrícula: 1135882

(Assinado digitalmente em 11/12/2023 20:33)
LEANDRO RESENDE MATTIOLI
PROFESSOR ENS BASICO TECN TECNOLOGICO
DELMAX (11.57.05)
Matrícula: 2973183

(Assinado digitalmente em 11/12/2023 14:59)
MATEUS ANTUNES OLIVEIRA LEITE
PROFESSOR ENS BASICO TECN TECNOLOGICO
CAAAX (11.57.01)
Matrícula: 3138470

(Assinado digitalmente em 11/12/2023 11:01)
Rafael Rodrigues Silva
DISCENTE
Matrícula: 20193006391

À Deus pai por ser a minha fonte de vida e sabedoria.
Aos meus pais pelo carinho e educação. À minha irmã
pelo zelo diário.

Agradecimentos

Expresso profundos agradecimentos à Duda, pelo apoio e motivação.

Aos amigos da classe que compartilharam os sonhos e desafios comigo - Alderico, Gabriel, Lucas e Otávio. Aos amigos de toda uma vida, Leonardo, Lucas Guimarães, Rilma e Victor, pela compreensão.

Agradeço aos professores do CEFET que me capacitaram, em especial, expresso minha gratidão a Cirilo, Henrique, Leandro e Luis Paulo.

"Uma descoberta transcende a mera curiosidade ao tornar-se útil através de sua aplicação prática, mas só atinge o seu verdadeiro valor ao beneficiar a sociedade."

Resumo

As transmissões de vídeos ao vivo são uma ferramenta fundamental da sociedade contemporânea. Contudo, diante da sua aplicabilidade tanto na comunicação interpessoal quanto no monitoramento industrial, em que a segurança dos dados é vital, há uma necessidade de garantir a confidencialidade e a confiabilidade dessas informações, o que implica no desenvolvimento de métodos sistemáticos para o envio de vídeos de forma segura e sigilosa. Neste trabalho é apresentado um promissor método de criptografia que usa mapas caóticos para alterar as posições e as intensidades dos pixels nos quadros de um vídeo. Nesse sentido, algumas combinações dos mapas caóticos de Baker, Arnold, logístico e Hénon são avaliadas levando em conta os principais testes de segurança e velocidade da atualidade. Os resultados mostram que o melhor algoritmo atingiu uma notável velocidade de encriptação, gastando apenas 10,76ms para criptografar e descriptografar quadros de dimensão 480×640 no padrão de cores RGB, levando-o a encriptar 92 quadros por segundo. O método proposto tem o potencial de ser aplicado em transmissões de vídeos ao vivo, usando as funcionalidades do codificador H.264 a fim de otimizar a sua velocidade, melhorando, assim, a experiência dos usuários.

Palavras-Chave: Criptografia Caótica. Criptografia de Vídeos. Transmissões Ao Vivo.

Abstract

Live video broadcast is a fundamental tool in modern society. However, considering its applicability both in personal communication and in industry, where data security is vital, there is a clear need to ensure the confidentiality and reliability of this information, implying in the development of solutions for sending videos securely and privately. This paper presents a promising encryption method that uses chaotic maps to alter pixels' positions and intensities in frames of a video stream. In this sense, some combinations of the Baker, Arnold, logistic and Hénon chaotic maps are evaluated, taking into account the current security and speed tests. The results show that the best algorithm achieved a remarkable encryption speed, taking only 10.76ms to encrypt and decrypt frames of size 480×640 *in the RGB color standard, enabling it to encrypt 92 frames per second. The proposed solution has potential applications in live video transmissions, using features from the H.264 decoder to optimize its speed, thus improving user experience.*

Keywords: *Chaotic Cryptography. Live Streaming. Video Cryptography.*

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

A pandemia de Covid-19, evidenciada em 2020, provocou uma transformação na maneira como as pessoas se comunicam. Com a necessidade do distanciamento social, o trabalho remoto se disseminou em todo o mundo, tornando os vídeos uma ferramenta essencial para a comunicação. De fato, estima-se que o trabalho híbrido aumentou 38% em 2022 (MICROSOFT, 2022), o que mostra essa modalidade de trabalho continuou sendo adotada mesmo no contexto pós-pandemia. No contexto industrial, os vídeos para monitoramento têm se mostrado cada vez mais importantes. Na China, algumas subestações de energia têm usado redes elétricas monitoradas por câmeras para evitar o contato entre colaboradores (YI; TIAN; CHEN, 2021). No Brasil, existe uma proposta para aumentar o uso dos ambientes virtuais de inspeção de subestações com uso de imagens de campo (MATTIOLI, 2021). Os vídeos também são utilizados na geração e transmissão de imagens geográficas produzidas por satélite (AL-KHASAWNEH; ABU-ULBEH; KHASAWNEH, 2020) e na vigilância de tráfego rodoviário (SRINIVASAN et al., 2004).

De fato, as transmissões de vídeos têm tido destaque tanto na comunicação interpessoal quanto no monitoramento industrial, em que a segurança dos dados é vital, pois a exposição de informações pode acarretar prejuízos financeiros ou riscos pessoais e estruturais para a empresa. Dessa forma, o valor agregado à confidencialidade e confiabilidade justifica a necessidade de proteger tais dados, o que resulta na necessidade do desenvolvimento de métodos sistemáticos de envio de vídeos de forma segura e sigilosa. A Criptografia é uma das principais soluções para a segurança cibernética, pois trata-se do estudo dos métodos de envio de uma mensagem de modo que nenhum terceiro indesejado seja capaz de compreender o seu conteúdo (COUTINHO, 2005).

Os métodos de criptografia de vídeo baseados em sistemas caóticos têm recebido considerável atenção nos últimos anos, pois este tipo de criptografia contribui significativamente no aumento da segurança dos dados, devido às propriedades das sequências caóticas. Esses sistemas são dinâmicos e o seu comportamento futuro é determinado por suas condições iniciais. Embora seu modelo matemático permita a

previsão do seu comportamento, pequenas alterações nas suas condições iniciais levam a desvios significativos nos resultados, tornando-os imprevisíveis ao logo do tempo (KOCAREV; LIAN, 2011). A segurança da criptografia está diretamente relacionada ao fato de que o sistema é determinístico, e as condições iniciais são usadas para a construção da chave de criptografia, dessa forma, qualquer alteração neste parâmetro leva a grandes alterações no resultado final. Tal fato pode ser explicado de forma simplista pela famosa metáfora do "efeito borboleta: o bater das asas de um inseto pode causar um tufão do outro lado do mundo", isto é, pequenas alterações nas condições iniciais causam grandes alterações no resultado.

No contexto dos métodos de criptografia caótica de vídeo são identificados quatro tipos principais (KOCAREV; LIAN, 2011):

- Criptografia de dados brutos – apresenta uma alta segurança, mas o custo computacional depende da complexidade de implementação dos mapas caóticos;
- Criptografia de regiões de interesse – eficiente em termos de custo computacional, porém com baixa ou média segurança;
- Criptografia durante a compressão – a segurança e eficácia deste tipo de criptografia dependem da complexidade dos mapas caóticos implementados;
- Criptografia pós-compressão – alta eficiência devido ao menor custo computacional, sendo que a segurança está relacionada à escolha dos mapas caóticos.

Al-Khasawneh et al. em 2020, analisaram várias técnicas relacionadas à criptografia de imagens de satélite e concluíram que o uso de sistemas caóticos teve grande importância para a segurança dos algoritmos (AL-KHASAWNEH; ABU-ULBEH; KHASAWNEH, 2020). Em 2021, Kumar e Singh propuseram um algoritmo que gerava suas chaves a partir da criptografia RSA e obtiveram a segurança desejada. Segundo estes autores, trabalhos futuros poderiam melhorar a performance do algoritmo em termos de diminuir o custo computacional (KUMAR; SINGH, 2021). Um esquema de criptografia caótica altamente seguro foi proposto por Zhang et al., em 2021, no entanto, os autores indicaram que outros estudos deveriam ser realizados levando em conta o custo computacional deste algoritmo em aplicações que requerem maior velocidade (ZHANG et al., 2021). Em geral, os artigos sobre criptografia de vídeo tornam evidente a dificuldade em encontrar equilíbrio entre velocidade de encriptação e a segurança dos dados.

A criptografia de vídeos em tempo real é uma área que busca o equilíbrio entre custo computacional e segurança, de forma a proteger as informações transmitidas de maneira eficiente. Em transmissões ao vivo, a encriptação muitas vezes é feita pós-compressão para obter maior velocidade. No entanto, há a necessidade de aprofundar os estudos acerca da segurança nesse contexto, visto que a escolha dos mapas caóticos também exerce influência

direta na eficiência computacional do algoritmo. Isso ocorre devido aos padrões distintos de construção e implementação presentes nesses mapas caóticos, resultando em variações no tempo de criptografia (KOCAREV; LIAN, 2011).

Para reduzir o custo computacional, uma abordagem eficaz envolve a exploração das características construtivas dos algoritmos de criptografia. Isso pode ser alcançado por meio da otimização dos algoritmos de criptografia em relação às operações repetidas em diferentes quadros de uma transmissão de vídeo ao vivo. Identificar padrões repetitivos e redundâncias dados possibilita aprimorar a eficiência do processo de encriptação, garantindo que as operações sejam executadas com menor custo computacional, proporcionando uma alta eficiência (KOCAREV; LIAN, 2011).

Embora os mapas caóticos sejam frequentemente usados para aumentar a segurança dos algoritmos de criptografia de vídeo, os métodos atuais deste tipo de criptografia pouco abordam o equilíbrio entre a segurança e o custo computacional. Essa lacuna compromete a eficiência da transmissão de dados, um fator crucial para transmissões ao vivo. Assim, surge a necessidade do desenvolvimento de métodos eficientes para garantir a segurança dos dados sem prejudicar a eficiência computacional. Nesse contexto, uma solução promissora é alcançada por meio da seleção do momento e método de compressão, escolha criteriosa dos mapas caóticos e otimização dos algoritmos. Essa abordagem possibilita a criação de um algoritmo que não só garante a segurança dos dados, mas também se destaca pela eficiência na transmissão.

Este trabalho tem como objetivo principal elaborar uma abordagem para a criptografia caótica de vídeos em transmissões ao vivo, buscando harmonizar a velocidade de transmissão e a segurança dos dados. O método proposto é baseado na utilização adequada de mapas caóticos validados por meio de testes de segurança e velocidade. Para atingir o resultado pretendido, são primordiais os seguintes objetivos específicos:

- Avaliar os principais mapas caóticos adequados para as transmissões ao vivo presentes na literatura;
- Desenvolver um método de criptografia caótica de vídeos;
- Avaliar os principais testes de velocidade e segurança para métodos de criptografia de vídeo presentes na literatura;
- Implementar algoritmos relativos aos testes de velocidade e segurança;
- Validar a segurança e velocidade do algoritmo de criptografia caótica de vídeos.

Para alcançar esses objetivos, o presente trabalho procura apresentar os principais conceitos sobre o tema e descrever a elaboração do método em capítulos descritos a seguir.

No capítulo 2, são apresentados os fundamentos essenciais para o desenvolvimento do método de criptografia caótica de vídeos para transmissões ao vivo. Desde os conceitos

fundamentais de imagem e vídeo até uma revisão dos principais resultados sobre criptografia. Também são apresentados os quatro mapas caóticos avaliados neste trabalho, bem como os testes usados na validação do algoritmo proposto.

O capítulo 3 apresenta a metodologia adotada neste trabalho, destacando o processo de seleção do momento e do método de compressão, dos mapas caóticos e dos testes de segurança e velocidade. Além disso, também expõe os detalhes construtivos do algoritmo, proporcionando uma compreensão abrangente de sua estrutura.

No capítulo 4, são disponibilizados os resultados e as análises obtidas ao longo do desenvolvimento do trabalho. Inicialmente, são apresentadas as evidências que fundamentaram as escolhas relativas à compressão, seguido dos resultados dos testes de segurança e velocidade relacionados aos mapas caóticos, a fim de fundamentar as escolhas dos mapas que melhor se adequem ao problema de criptografia de vídeo para transmissão ao vivo, deixando o algoritmo o mais eficiente possível. Por fim, é apresentado um método para a criptografia caótica de vídeos destinada às transmissões ao vivo, bem como aborda questões referentes ao compartilhamento de chaves. Ademais, o capítulo 5 destaca as contribuições e melhorias identificadas neste trabalho, proporcionando uma visão abrangente do impacto do método proposto.

Capítulo 2

Revisão de Literatura

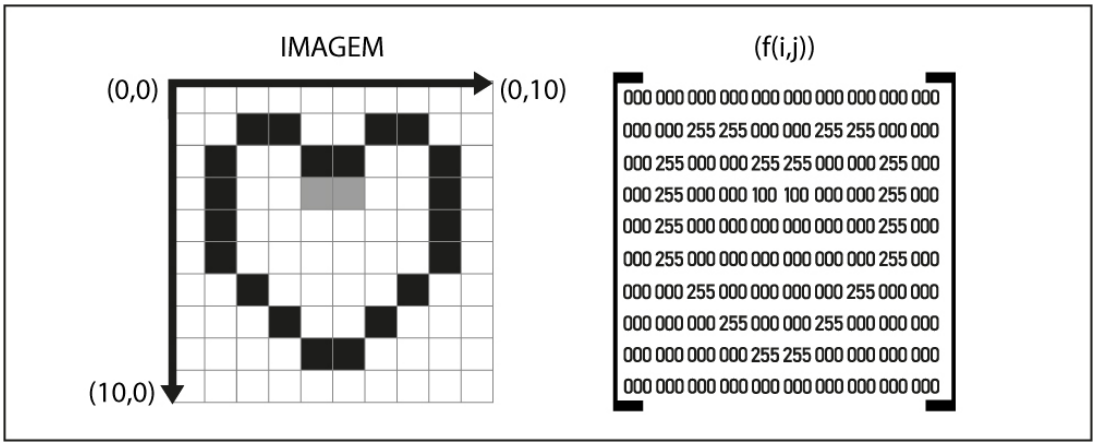
Este capítulo tem como objetivo apresentar os fundamentos necessários para o desenvolvimento do método de criptografia. Para tanto, são discutidas as principais características de imagem, vídeo, transmissões ao vivo e compressão de vídeos, bem como alguns tipos de criptografia. Também é apresentada uma introdução aos mapas caóticos. Ademais, compara os modelos atuais de criptografia caótica de vídeo, desenvolvidos nos últimos anos, além de apresentar alguns testes de segurança e velocidade relevantes para a validação do algoritmo.

2.1 Imagem e Vídeo

Neste trabalho, a seguinte notação é usada para descrever uma imagem: uma **imagem digital** (ou simplesmente imagem) é uma matriz $(f(i,j))$, com $1 \leq i \leq n$ e $1 \leq j \leq m$, em que $f(i,j)$ é um valor de intensidade na escala de cinza, no padrão RGB (Vermelho, Verde, Azul) ou no padrão CMYK (Ciano, Magenta, Amarelo, Preto). Assim, uma imagem pode ser representada no plano, isto é, uma malha retangular $n \times m$ (dividido horizontalmente em n sub-retângulos e verticalmente em m sub-retângulos, todos com mesmas dimensões), o qual o sub-retângulo da posição (i,j) é preenchido pela intensidade $f(i,j)$, de acordo com a respectiva escala de cor da imagem. A notação $(i,j,f(i,j)) \in \mathbb{N}^3$ é usada para denotar o sub-retângulo na posição (i,j) com intensidade $f(i,j)$, isto é, os elementos $(i,j,f(i,j))$ são os **pixels** da imagem. Na Figura 2.1 é apresentado a representação no plano e a forma matricial de uma imagem. (GONZALES; WOODS, 2009).

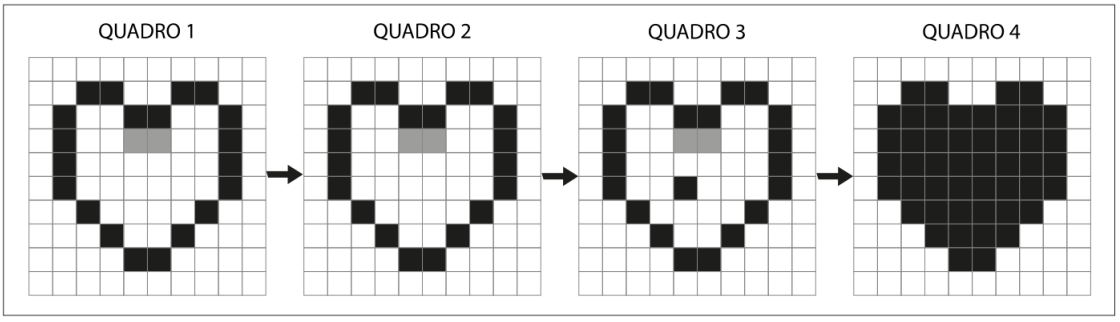
A **resolução** de uma imagem é definida pelo número de pixels em uma determinada área, dada em pixel por polegada (PPI), sendo que, quanto maior for a resolução, mais nítida e detalhada será a imagem (GONZALES; WOODS, 2009).

Figura 2.1: Representação de imagem



Um **vídeo** é uma sucessão de imagens que, quando exibidas sequencialmente com uma alta taxa de transição, geram a ilusão de movimento ao olho humano. Cada imagem dessa sequência é chamada de **quadro** e a **taxa de transição dos quadros** é dada em quadros por segundo (QPS). Dessa forma, a resolução e a taxa de transição dos quadros contribuem para a qualidade do vídeo (KOCAREV; LIAN, 2011). Na Figura 2.2 apresenta-se a representação da sequência de quadros de um vídeo.

Figura 2.2: Representação de quadros



Para garantir que o movimento pareça contínuo, a taxa de QPS precisa ser suficientemente alta, garantindo assim que o cérebro humano possa processar a transição entre os quadros de forma suave (GONZALES; WOODS, 2009). Nas transmissões ao vivo os quadros são enviados e, ao serem recebidos, são reproduzidos pelo destinatário. Na próxima seção serão apresentadas as principais características das transmissões ao vivo.

2.2 Transmissão de Vídeo ao Vivo

Nos últimos anos, o avanço das redes sociais tem impulsionado o uso das transmissões de vídeo ao vivo (DAO et al., 2022), permitindo que os espectadores tenham acesso aos conteúdos praticamente instantaneamente.

Para que os vídeos sejam transmitidos de forma fluida deve-se levar em consideração a **latência**, isto é, o atraso entre a captura do vídeo do emissor, e a reprodução do espectador. Assim sendo, uma alta latência pode levar a atrasos perceptíveis na transmissão, impactando negativamente na percepção do usuário (DAO et al., 2022).

Além disso, também deve-se levar em consideração a estabilidade do vídeo. Essa estabilidade está ligada à **taxa de bits do vídeo** (*bitrate*), medida pela quantidade de bits transferidos por segundo (bps), a tendência é que uma alta taxa de bits alcance uma maior qualidade da transmissão, exigindo em contrapartida, que a largura de banda seja mais alta, causando possíveis atrasos ou interrupções na transmissão para espectadores com conexões de internet mais lentas (DAO et al., 2022).

Dessa forma, um método de criptografia de vídeos ao vivo deve considerar a latência da transmissão e a estabilidade do vídeo transmitido. A tendência é que a criptografia aumente a latência e a taxa de bits, devido ao processamento e execução do algoritmo, faz-se necessário encontrar um equilíbrio entre a velocidade de transmissão e a segurança exigida em cada aplicação. Uma das formas de diminuir o tempo gasto para envio dos quadros de um vídeo é o uso da compressão, que diminui a quantidade de bits necessários para representar cada quadro. Na próxima seção serão apresentadas as principais características da compressão.

2.3 Compressão de Vídeo

Segundo Gonzales e Woods (2009, p. 366), a **compressão** de vídeos é "a arte e a ciência de reduzir o volume de dados necessários para representar um vídeo". Todos que navegam pela internet, assistem filmes e usam redes sociais são beneficiados pelos algoritmos de compressão. Um exemplo prático proposto por Gonzales e Woods (2009, p. 366) diz que um filme em SD - padrão das webcams e câmeras de monitoramento que hoje tem sido substituído por dimensões HD (720×1280), FHD (1080×1920) e UHD (2160×3840) - utiliza a dimensão 480×640 e 24 bits, para a reprodução de com taxa de 30 QPS de um filme de duas horas. Seriam necessários

$$(30)\,\frac{\text{quadros}}{\text{s}} \times (480 \times 640)\,\frac{\text{pixels}}{\text{quadros}} \times (3)\,\frac{\text{bytes}}{\text{pixels}} \times \left(60^2\right)\frac{\text{s}}{\text{h}} \times (2)\,\text{h} \cong 199\text{GB}$$

para armazenar o vídeo. Mas, em geral, os filmes em SD de duas horas de duração devem ter o tamanho máximo de um DVD de camada dupla de 8,5 GB, o que demonstra uma redução percentual de 95,72% (GONZALES; WOODS, 2009). Isso evidencia a importância do uso da compressão de vídeos. Para reduzir o volume de dados a compressão mantêm apenas as informações necessárias para a compreensão humana, eliminando os outros dados.

A compressão de vídeos evoluiu significativamente com o passar dos anos, devido aos padrões de codificação cada vez mais eficientes. Entre os mais conhecidos estão o MPEG-4 sucessor do MPEG-2 amplamente aplicado na televisão, o H.264, padrão comum na transmissão de vídeos da internet, e o H.265 foi projetado para ser o sucessor do H.264, com uma eficiência perceptível em relação à compressão, suportando vídeos com qualidades maiores (GONZALES; WOODS, 2009). A técnica de compressão interquadros se tornou de particular interesse, visto que o objetivo inicial deste trabalho era o uso da criptografia apenas em quadros-chave e quadros-delta, como forma de alcançar uma maior eficiência em relação ao custo computacional.

A técnica de **compressão interquadros** usa redundância nos dados dos quadros consecutivos, para reduzir a quantidade de dados codificados, codificando apenas os quadros-chave e os quadros-delta. Os **quadros-chave** são os principais quadros de um vídeo, que representam as informações necessárias para compreensão humana. Entre o envio de diferentes quadros-chave, são enviados os **quadros-delta**. Esses quadros contêm apenas a informação referente a diferença do quadro atual em relação ao quadro-chave anterior, isto é, para facilitar o entendimento tomaremos um quadro-delta do quadro $(f(i,j))$ em relação ao quadro-chave anterior $(g(i,j))$, com $1 \leq i \leq n$ e $1 \leq j \leq m$, como o quadro $(h(i,j))$, em que

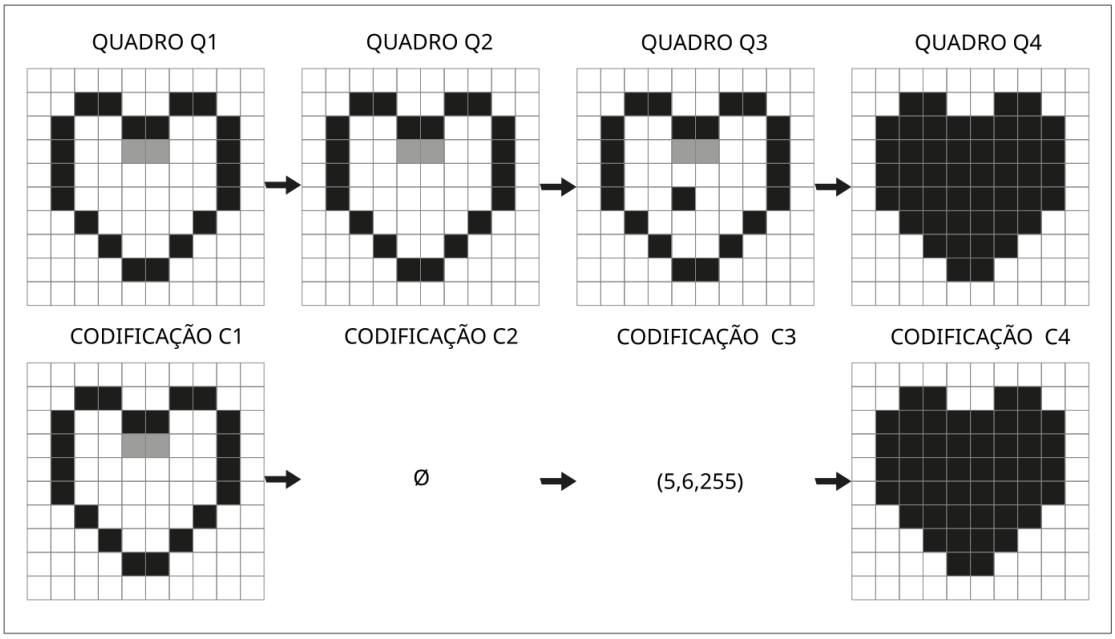
$$h(i,j) = \begin{cases} f(i,j) & \text{se } f(i,j) \neq g(i,j) \\ 0 & \text{caso contrário} \end{cases},$$

apenas as intensidades diferentes de zero são enviadas, dessa forma, a compressão interquadros permite reduzir significativamente o tamanho do arquivo de vídeo, pois apenas as diferenças entre os quadros são codificadas, sendo que a junção de quadros-chave e quadros-delta fornecem as informações necessárias para reconstruir o vídeo de forma adequada (RICHARDSON, 2003).

De forma simplificada, no início do processo o primeiro quadro é codificado integralmente, e é tomado como quadro-chave. Nos quadros subsequentes, a diferença entre o quadro atual e o quadro-chave é calculada. Essa diferença é codificada como um quadro-delta, a menos que ocorra uma alteração significativa, determinada por critérios preestabelecidos, que justifique codificar o quadro completo para torná-lo o novo quadro-chave. Uma maneira de verificar a necessidade de codificar o novo quadro como quadro-chave é avaliar o número de bits necessários para codificar o quadro-delta. Se a quantidade de bits necessária para codificar um quadro-delta for menor do que a quantidade de bits necessária para codificar o quadro completo, apenas diferença entre os quadros é codificada como quadro-delta. Caso contrário, o quadro completo é codificado como quadro-chave. Essa abordagem garante que o custo computacional de codificar um

quadro como quadro-delta seja menor do que codificar o quadro completo. Esse processo continua até o final da codificação do vídeo. Na Figura 2.3, é apresentado uma sequência de quatro quadros originais (Q1, Q2, Q3 e Q4) e os dados codificados (C1, C2, C3 e C4). O quadro Q1 é o primeiro quadro-chave e é codificado como C1. Na transição do quadro Q1 para Q2, eles são comparados e observa-se que não houve alteração, sendo assim, conforme C2 apenas a informação de que não houve mudança é codificada. Em seguida, comparando o quadro Q2 com Q3 observa-se que ocorreu uma pequena alteração, sendo assim só é necessário codificar C3, que é o quadro-delta correspondente. De Q3 para Q4 houve uma alteração significativa, assim, o quadro Q4 é tomado como o novo quadro-chave e conforme C4 o quadro é codificado integralmente.

Figura 2.3: Representação de quadros-chave e quadros-delta



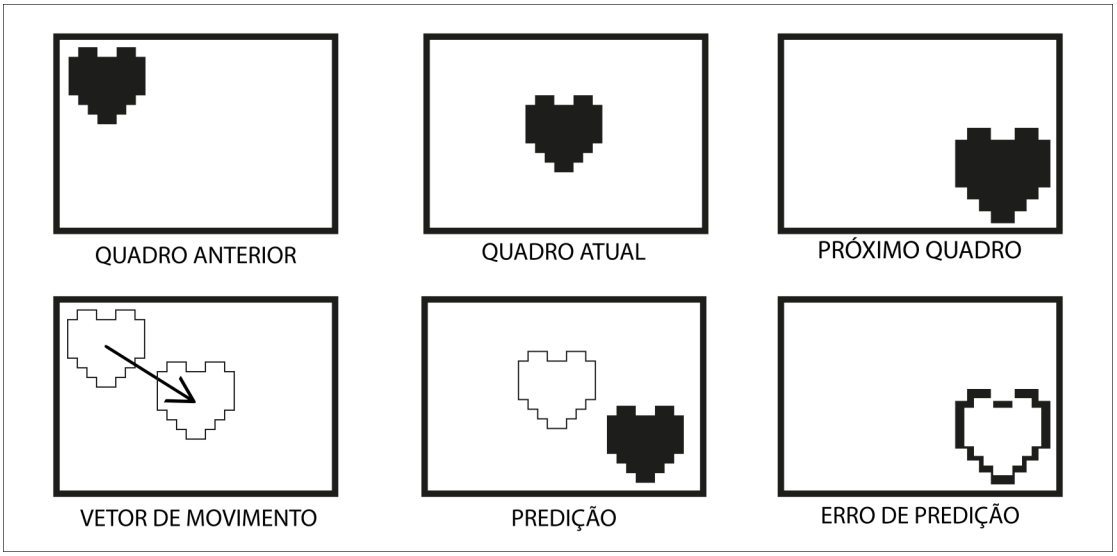
Os métodos atuais de compressão utilizam de técnicas ainda mais avançadas para reduzir o tamanho dos arquivos. Eles aproveitam das diferenças temporais (quadros-delta), codificando apenas as diferenças entre os quadros sucessivos, somando com alguns recursos valiosos como a predição de movimento, compensação de movimento e taxa de bits variável (STOLFI, 2018).

A **predição de movimento** é uma técnica avançada que aproveita a ideia de que, em uma sucessão de quadros, os deslocamentos de objetos podem ser previstos com base nos quadros anteriores. A ideia central é semelhante a compressão interquadros, buscando explorar a redundância temporal nos quadros do vídeo, armazenando apenas as diferenças entre os quadros sucessivos, em vez de armazenar cada quadro inteiramente. Este processo é realizado a partir de um quadro que é dividido em blocos. Para um destes blocos é realizada uma busca por correspondências nos quadros anteriores, procurando as posições anteriores

de um mesmo objeto em um determinado bloco. Após encontrar o objeto correspondente nos quadros anteriores, um **vetor de movimento** é calculado levando em consideração as posições anteriores em relação a posição atual do objeto. Por meio deste vetor é feita uma predição de como o objeto deve se mover no próximo quadro. Assim, para codificar o próximo quadro é necessário codificar apenas a diferença entre o movimento real e a predição de movimento do objeto, essa diferença é chamada de **erro de predição**. Em uma previsão perfeita, o erro é zero, entretanto, isso não ocorre na prática. Existe ainda a **compensação de movimento**, definida pela observação de que o objeto ao se deslocar para uma nova posição, tem a intensidade de seus pixels alterada em relação a posição anterior (STOLFI, 2018).

Na imagem Figura 2.4 é observado que o quadro atual contém um objeto posicionado no centro. No quadro anterior, esse objeto encontrava-se no canto superior esquerdo. A partir dessa mudança de posição, é gerado um vetor de movimento, o qual é utilizado para fazer a predição e a compensação de movimento, sendo apenas essas informações codificadas. No próximo quadro, o objeto é ampliado e se move para o canto inferior direito. A predição feita é próxima do movimento real, portanto, só é necessário codificar o erro de predição, isto é, a informação de que o objeto foi ampliado.

Figura 2.4: Representação da predição de movimento



Dado que os recursos empregados nos mecanismos de compressão possuem tamanhos variáveis e considerando que o propósito deste trabalho é a transmissão desses dados, torna-se crucial a implementação de uma taxa de bits variável para a transmissão dos quadros. Essa abordagem permite que a taxa de bits usada para codificar cada quadro varie ao longo do tempo, ajustando-se dinamicamente ao tamanho dos elementos presentes. A flexibilidade na taxa de bits é fundamental para otimizar o número de bits da transmissão, assegurando que apenas a quantidade necessária seja enviada para cada

elemento de codificação do quadro. Em contraste, uma taxa de bits fixa resultaria na transmissão de uma quantidade excessiva e desnecessária de dados contendo a mesma informação. A taxa de bits variável normalmente é controlada usando um perfil de codificação que especifica limites máximos e mínimos de taxa de bits, permitindo que os codificadores mantenham a qualidade dentro de limites aceitáveis (DAO et al., 2022).

Ainda no contexto da compressão de quadros, existem duas abordagens: a compressão com perdas e a compressão sem perdas. Enquanto a compressão com perdas demonstra alta eficácia na redução do tamanho dos arquivos, ela inevitavelmente implica na perda de informações. Esta abordagem revela-se particularmente útil em diversos contextos, como reprodução de vídeos e filmes, em que perdas imperceptíveis são aceitáveis (GONZALES; WOODS, 2009). No entanto, na criptografia caótica de vídeos a perda de dados acarreta a impossibilidade de reconstrução do quadro original, pois todos os dados são necessários e interdependentes. Nesse cenário, torna-se indispensável a adoção de uma abordagem de compressão sem perdas, mesmo que esta seja mais lenta.

2.4 Métodos de Compressão de Vídeo

A compressão de vídeos abrange uma variedade de métodos que evoluíram ao longo do tempo, adaptando-se às necessidades específicas de suas aplicações. Três organizações desempenharam papéis significativos nesse processo: a *International Electrotechnical Commission* (IEC), a *International Organization for Standardization* (ISO) e a *International Telecommunication Union* (ITU) (GONZALES; WOODS, 2009).

A IEC desenvolveu o padrão *digital video* (DV), concebido em 1995, este formato é caracterizado por padrões leves de compressão e amplamente empregado em fitas cassetes. Este padrão de vídeo foi projetado especialmente para equipamentos e aplicações de produção semiprofissional de vídeo. Com suporte para dimensões de até 576×720 pixels, taxas de até 25 QPS e taxa de compressão 5:1, o DV utiliza compressão com perdas para reduzir o tamanho dos arquivos de vídeo digital. Contudo este padrão DV se destaca pelas mínimas, e muitas vezes imperceptíveis, perdas de qualidade. Essa característica tornou-o uma escolha popular em contextos em que é essencial manter a qualidade visual do vídeo (GONZALES; WOODS, 2009).

A ITU desenvolveu os famosos padrões *High 26X* (H.26X) concebidos principalmente para videoconferência e transmissões de vídeo, sendo especialmente adequados para situações com taxas de bits relativamente baixas. Essa série de padrões teve início em 1988 com o H.261, que suportava quadros de até 288×352 pixels, taxa de 30 QPS, taxa de compressão até 100:1, com previsão de quadro a quadro, fazendo uso de técnicas de compressão com perdas (RICHARDSON, 2003).

O H.262 é um padrão que foi desenvolvido para várias aplicações, incluindo

transmissão de televisão digital, DVDs e vídeo de alta qualidade. Este padrão foi concebido visando atender as necessidades relativas à produção de DVDs, que trabalham a uma taxa de transferência de 15 Mb/s, dimensões de até 720×1280 pixels, taxas de até 60 QPS e taxa de compressão até 200:1. O H.263 é uma versão melhorada do H.261, com foco em videoconferências com dimensões de até 512×1408 pixels, taxas de até 60 QPS e taxa de compressão 200:1 (RICHARDSON, 2003).

O H.264 é uma extensão dos padrões anteriores com foco em transmissões ao vivo. Suportando predição de quadros com codificação adaptativa, além de várias opções para compressão com perdas e sem perdas. É um padrão altamente eficiente que suporta uma ampla variedade de dimensões de até 4320×7680 pixels, taxas de até 240 QPS e taxa de compressão variável (FFMPEG, 2023).

A ISO desenvolveu em parceria com a IEC os famosos padrões *Moving Picture Experts Group* (MPEG-X). Ele estabelece formas para codificação de mídias, incluindo a compressão de áudios, vídeos, gráficos e dados genômicos; e padrões de transmissão e formatos de arquivo. O primeiro padrão MPEG-1 de 1990 é capaz de compactar vídeos em dimensões de até 480×640 pixels, taxas de até 30 QPS e taxa de compressão 200:1 (GONZALES; WOODS, 2009).

O MPEG-2 desenvolvido na mesma época que o MPEG-1 é mais avançado e flexível. Ele é amplamente utilizado em DVDs e transmissões de televisão digital. Suporta até 720×1280 pixels, taxas de até 60 QPS e taxa de compressão 200:1, segundo Gonzales e Woods (2009, p. 357), este foi o padrão de codificação mais bem sucedido até aquele momento devido as suas aplicações (GONZALES; WOODS, 2009).

O MPEG-4 é uma extensão do MPEG-2 que suporta tamanhos variáveis de blocos e diferenciação da predição de movimento em quadros. É geralmente um padrão de compressão com perdas, no entanto ele oferece alguma flexibilidade e recursos que podem permitir um maior controle sobre a qualidade de vídeo e a taxa de bits, as dimensões são de até 4320×7680 pixels, taxas de até 60 QPS e taxa de compressão variável (FFMPEG, 2023).

Os padrões H.264 e o MPEG-4 destacam-se, mesmo com a criação de novos padrões de codificação, como o H.265 e MPEG-5. O H.264 foi desenvolvido para ser o sucessor do padrão MPEG-4. Segundo Nemcic, Vranjes e Rimac-Drlje, o H.264 supera o MPEG-4 em qualidade de compressão, isso ocorre mesmo em vídeos que apresentam poucas semelhanças entre os quadros, o que dificulta a compressão. Essa característica é importante, visto que em vídeos criptografados existem poucas semelhanças entre os quadros. A taxa de compressão do H.264 é de 1,5 a 2 vezes maior que a do MPEG-4 (NEMCIC; VRANJES; RIMAC-DRLJE, 2007).

O H.264 permite diversas opções de configuração, alterando algumas características para melhor atenderem as necessidades de codificação. Nas configurações é possível

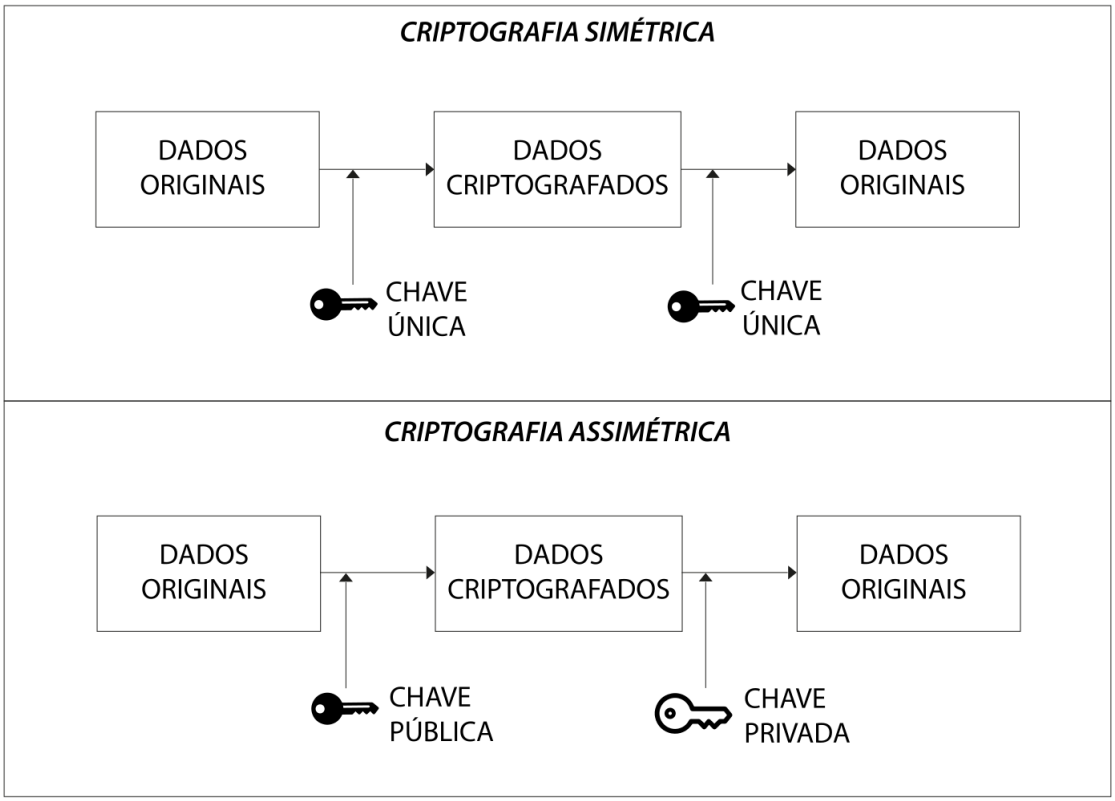
escolher o perfil de codificação, definindo a fidelidade de cores do codificador. O **perfil 4:4:4 no H.264**, por exemplo, refere-se a um perfil que suporta a codificação de vídeo com uma alta fidelidade de cor. A notação "4:4:4" refere-se à taxa de amostragem de cada cor. No perfil 4:4:4, todas as amostras de cor são mantidas para cada pixel, o que resulta em uma alta qualidade de cor. Em comparação, outros perfis, como 4:2:0, 4:2:2 etc., realizam subamostragem de cor para reduzir o volume de dados, sacrificando a qualidade de cor em favor da eficiência de compressão. Outra importante configuração presente no H.264 é o **fator de taxa constante** (CRF). Este fator determina a fidelidade do arquivo codificado ao arquivo original, isto é, o quanto será permitido perdas nas características do vídeo durante a redução tamanho do arquivo. No H.264, esse valor varia de 0 a 51, em que 0 significa uma compressão sem perdas, mas com mínima compressão, e 51 é a máxima compressão, mas com muitas perdas (FFMPEG, 2023). Com a escolha de valores baixos de CRF são gerados pacotes de dados maiores, tornando necessário uma maior velocidade de transmissão em comparação com a velocidade necessária para pacotes gerados a partir de valores altos de CRF, isso ocorre para que a velocidade de transmissão não afete a fluidez das transmissões ao vivo.

2.5 Criptografia

A palavra **criptografia** tem origem grega e significa “escrita secreta ou oculta”. De acordo com Coutinho (2005, p. 1) a criptografia é “o estudo dos métodos de codificação de uma mensagem de forma que apenas o destinatário legítimo possa interpretá-la”. Essa técnica é essencial em nossas vidas, seja para enviar mensagens seguras pelo celular, trocar informações confidenciais, enviar e-mails seguros, proteger senhas bancárias e outras informações importantes. A encriptação pode ser dividida em dois tipos principais: simétrica e assimétrica.

- **Criptografia simétrica:** a mesma chave é usada tanto para criptografar quanto para descriptografar os dados (BONFIM, 2017).
- **Criptografia assimétrica:** contém uma chave pública usada para criptografar e uma chave privada usada para descriptografar. Isso significa que qualquer pessoa pode enviar os dados usando a chave pública, mas apenas o destinatário desejado pode descriptografar a mensagem, usando a chave privada (BONFIM, 2017).

Figura 2.5: Fluxogramas de criptografia



Vários métodos de criptografia são usados para proteger informações, entre eles o RSA (COUTINHO, 2005) e o ELGamal (KOCAREV; LIAN, 2011). Estes são métodos de chave pública altamente seguros, contudo, seus algoritmos são consideravelmente lentos em relação aos algoritmos de cifragem simétrica. Por esse motivo, a criptografia de chave pública é mais adequada para encriptação de pequenos pacotes de dados, como mensagens e/ou para o compartilhamento de senhas, usadas posteriormente por algoritmos de chave simétrica (ABD EL-SAMIE et al., 2013).

Devido ao grande volume de dados presentes nos vídeos, não é recomendável encriptá-los usando técnicas convencionais de criptografia. De fato, a redundância presente nos vídeos faz com que os códigos convencionais não tenham sucesso em obscurecer todas as informações, além facilitar a quebra das cifras (ABD EL-SAMIE et al., 2013). Recentemente, uma atenção crescente tem sido dedicada ao uso da teoria caótica para implementar o processo de criptografia de imagens e vídeos. A principal vantagem dessa técnica reside na observação de que um sinal caótico parece ruído para usuários não autorizados, além da aumentar a dificuldade de encontrar padrões de reconstrução para o vídeo original (KOCAREV; LIAN, 2011). Na próxima seção serão apresentados alguns mapas que usufruem das propriedades caóticas.

2.6 Mapas Caóticos

Os mapas caóticos são utilizados na criptografia de vídeos e imagens para obter a confusão e a difusão.

- A **confusão** é gerada a partir do embaralhamento da posição dos pixels.
- A **difusão** é obtida alterando o valor da intensidade dos pixels.

Os principais mapas usados na criptografia de vídeos são o mapa de Arnold, o mapa de Baker, o mapa logístico e o mapa de Hénon (KOCAREV; LIAN, 2011)(ABD EL-SAMIE et al., 2013).

2.6.1 Mapa de Arnold

Considere a imagem quadrada $(f(i,j))$, com $1 \leq i,j$ e $i,j \leq N$. O **mapa de Arnold** é dado pela seguinte transformação

$$(i, j, f(i,j)) \rightarrow ((i+j) \bmod (N), (i+2j) \bmod (N), f(i,j)),$$

o qual $a \bmod (N)$ é o resto da divisão de a por N. Assim, o mapa move a intensidade $f(i,j)$ para a posição $((i+j) \bmod (N), (i+2j) \bmod (N))$ (VALDEVINO, 2006). Na Figura 2.6 é apresentado uma imagem de dimensão 101×101, e as imagens resultantes da aplicação do mapa de Arnold.

Observa-se que após 25 iterações, a figura resultante é igual à figura original. Isso ocorre pois o mapa de Arnold é uma transformação cíclica. De forma geral, dada uma imagem $(f(i,j))$, existe um número inteiro $0 < k \leq N^2$, tal que a figura resultante da k-ésima iteração, do mapa de Arnold, é igual a figura original. Nota-se que, dada uma imagem $(f(i,j))$, cada pixel $(i, j, f(i,j))$ possui um ciclo sob o mapa de Arnold, isto é, um número inteiro $t > 0$, tal que após t-ésima iteração este pixel retorna à posição inicial. Desta forma, se k é mínimo múltiplo comum dos ciclos de todos os pixels da imagem, então, a fim de otimizar os cálculos, o **período** de $(f(i,j))$ pode ser tomado como sendo k (VALDEVINO, 2006). Os algoritmos de criptografia de imagens adotam tabelas contendo o período de imagens, de determinada dimensão, sob este mapa, como a Tabela 2.1.

O mapa de Arnold também é conhecido como mapa do gato de Arnold, pois Arnold utilizou as imagens de seu gato para exemplificar as iterações do sistema (VALDEVINO, 2006).

Figura 2.6: Aplicação mapa de Arnold

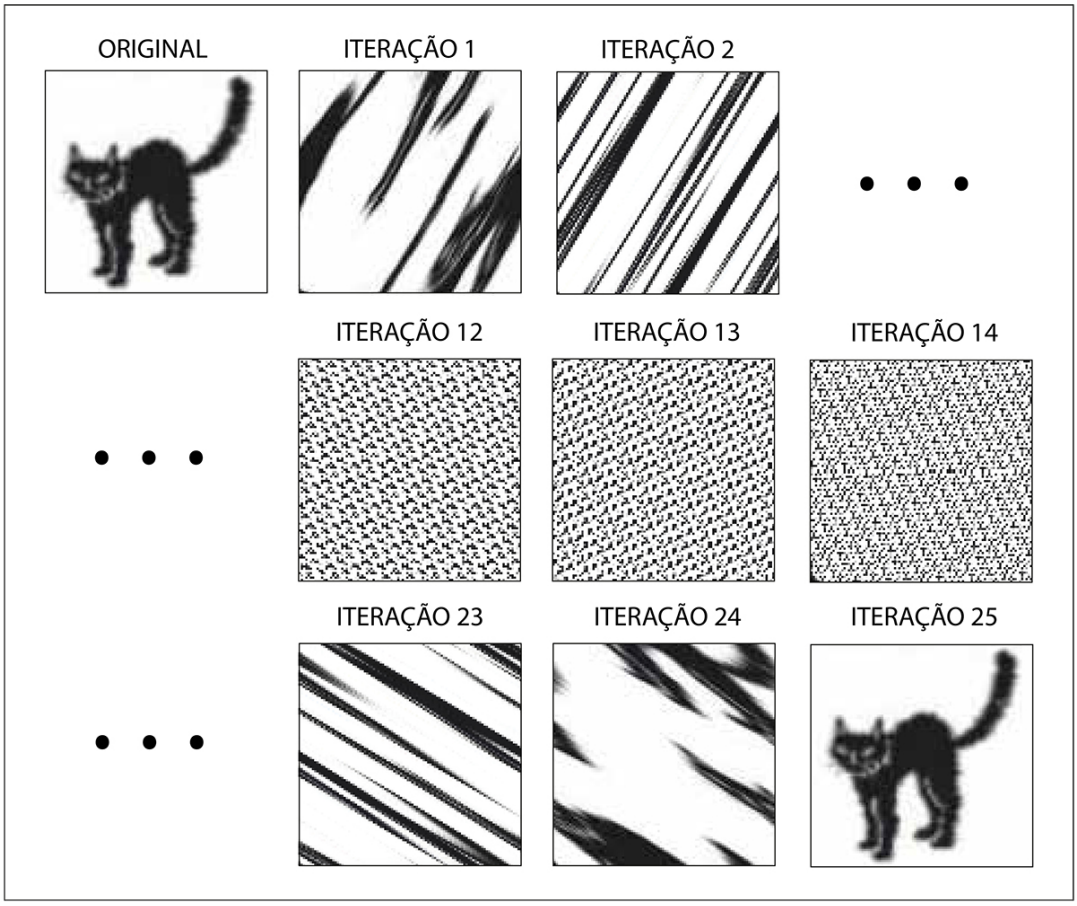


Tabela 2.1: Exemplos de períodos mapa de Arnold

Dimensão [pixel]	**Período**
32×32	24
124×124	15
512×512	378
764×764	265
1024×1024	768

Fonte: Huang et al. (2021, p. 2)

2.6.2 Mapa de Baker

Considere a imagem quadrada $(f\,(i,j))$ com dimensão $N \times N$, é determinado uma senha $(n_1; \ldots; n_k)$ formada por divisores positivos de N, tais que tais que $N = n_1 + \cdots + n_k$. O **mapa de Baker** $B_{(n_1 \ldots n_k)}$ age da seguinte maneira sobre a imagem:

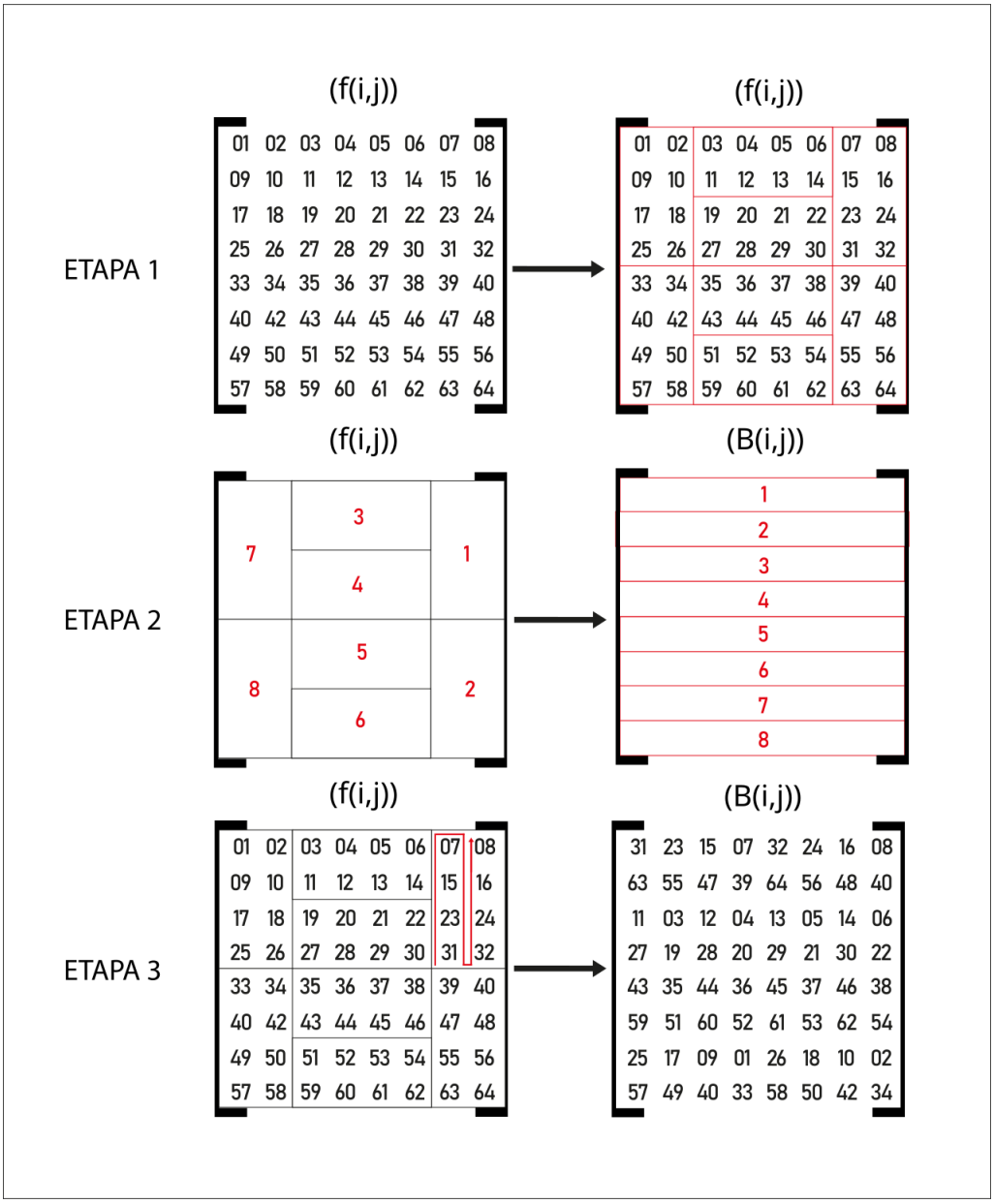
1. $(f\,(i,j))$ é dividida, a partir da esquerda superior, em N sub-retângulos de largura n_i e altura $\frac{N}{n_i}$.

2. Os sub-retângulos são numerados de 1 a N, ordenadamente de cima para baixo e da direita para esquerda.

3. Os elementos do j-ésimo sub-retêngulo são reorganizados na linha j da imagem criptografada ($B(i, j)$) de baixo para cima e da esquerda para a direita.

Na Figura 2.7 é possível observar o passo a passo para a reordenação posições dos pixels da imagem usando o mapa de Baker em uma imagem de dimensão 8×8 pixels e senha $(2; 4; 2)$.

Figura 2.7: Aplicação mapa de Baker



Dessa forma, o mapa de Baker pode ser aplicado na imagem quadrada ($f(i, j)$), com $1 \leq i,j \leq N$, por meio da seguinte transformação

$$(i, j, f(i, j)) \rightarrow (i', j', f(i, j)),$$

o qual i' e j' são a primeira e segunda entrada de $B(n_1 \ldots n_k)(i, j)$. Assim, o mapa move a intensidade $f(i, j)$ para a posição $B(n_1 \ldots n_k)(i, j)$, para propagar o caos é necessário iterar o mapa diversas vezes na imagem (ABD EL-SAMIE et al., 2013).

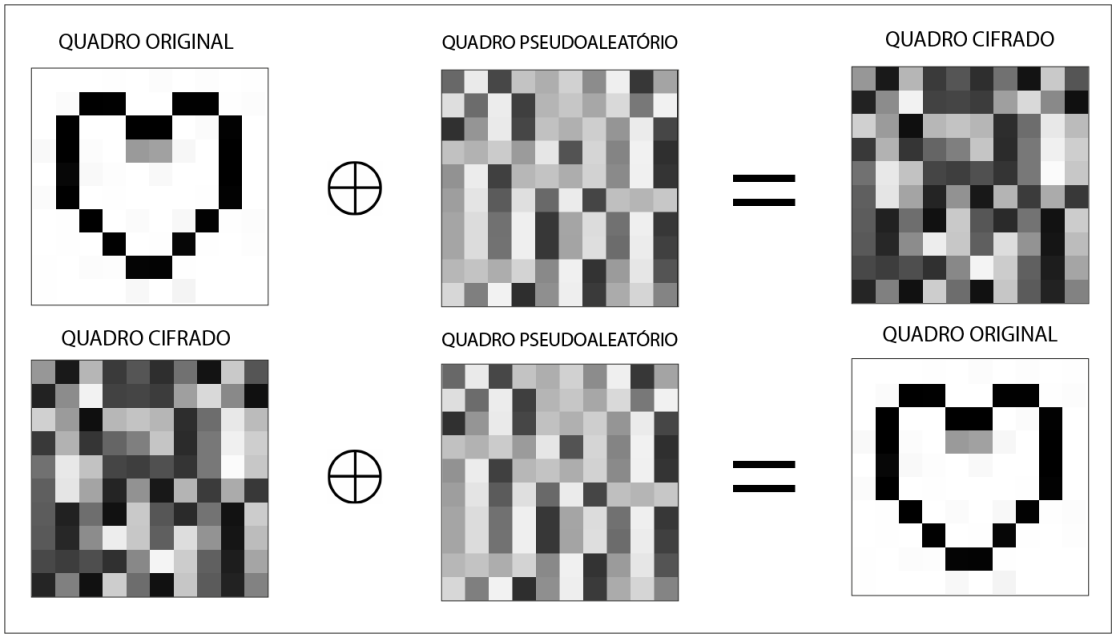
2.6.3 Mapa Logístico

Diferentemente dos mapas anteriores o **mapa logístico** é usado para alterar a intensidade do pixel de uma determinada posição. Este mapa é definido por

$$x_{n+1} = r x_n (1 - x_n), \tag{2.1}$$

em que r deve ser tomado de maneira a garantir o comportamento caótico do mapa, em geral o caos é adquirido com a escolha de $3,5 \leq r \leq 4$. Dessa forma, este mapa altera as intensidades dos pixels de uma imagem $(f(i, j))$, $1 \leq i \leq n$, $1 \leq j \leq m$, através da sua operação XOR (OU exclusivo) pixel a pixel com os valores de $(l_{i,j})$, em que a matriz $(l_{i,j})$ é formada por valores pseudoaleatórios gerados usando mapa logístico (2.1) (KOCAREV; LIAN, 2011). Na Figura 2.8 o quadro original é operado pixel a pixel, através da operação XOR, com a matriz $(l_{i,j})$ obtendo, assim, o quadro cifrado. Como a inversa da XOR é a própria XOR, o processo de descriptografia é realizado repetindo a operação sobre o quadro cifrado.

Figura 2.8: Aplicação mapa logístico



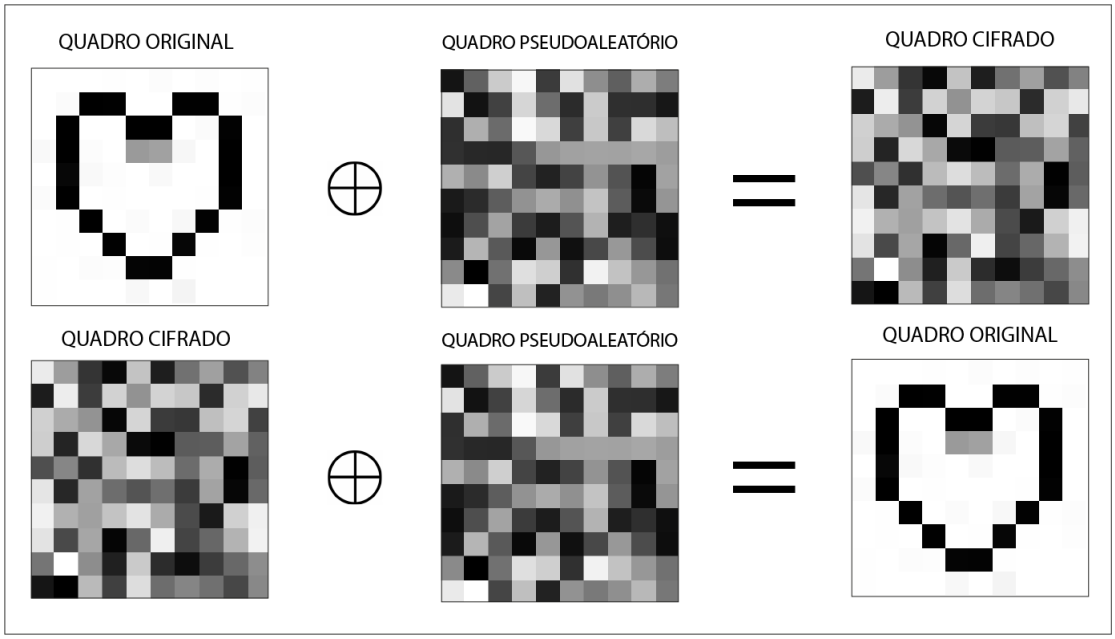
2.6.4 Mapa de Hénon

O **mapa de Hénon** é o mapa bidimensional, definido por

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n, \end{cases} \tag{2.2}$$

o qual a e b são os parâmetros de dimensionamento, e devem ser tomados de maneira a garantir o comportamento caótico do mapa, o trabalho original de Hénon usa $a = 1,4$ e $b = 0,3$. De forma análoga ao mapa logístico, o mapa de Hénon (2.2) é usado para alterar as intensidades dos pixels de uma imagem ($f(i, j)$) (KOCAREV; LIAN, 2011). Também, de forma análoga ao mapa logístico na Figura 2.9, o quadro original é então encriptado.

Figura 2.9: Aplicação mapa de Hénon



2.7 Algoritmos de Criptografia de Vídeo

Em 2011, Kocarev e Lian apresentaram o algoritmo de criptografia de vídeos de Qian, Chen e Yan (KOCAREV; LIAN, 2011). Este método criptografa o vídeo após a sua compressão e isso resulta em um ganho de performance na velocidade de encriptação. Embora, o trabalho tenha sido baseado no uso de três mapas caóticos o algoritmo oferece apenas uma segurança mediana segundo os autores (QIAN; CHEN; YUAN, 2008).

O algoritmo apresentado por Kumar et al., em 2019, propõe três níveis de criptografia: primeiramente é feita uma seleção aleatória dos quadros, depois esses

quadros são embaralhados através de um mapa caótico, e finalmente ocorre a difusão, isto é, os valores de intensidade dos pixels são alterados. Segundo os autores este algoritmo mostrou-se eficaz nos testes de NPCR e UACI (ver na seção 2.8) (RANJITH KUMAR et al., 2019).

Em 2020, Al-Khasawneh, Abu-Ulbeh e Khasawneh analisaram várias técnicas relacionadas a criptografia de imagens de satélite, e concluíram que o uso de sistemas caóticos teve grande importância para a segurança dos algoritmos (AL-KHASAWNEH; ABU-ULBEH; KHASAWNEH, 2020). Malladar e Kunte propuseram um método de criptografia seletiva usando o H.264 como codificador. Tal algoritmo usa classes de equivalência juntamente ao mapa logístico a fim de aumentar a sua segurança. Esse método mostrou-se eficiente em relação à custo computacional (MALLADAR; KUNTE, 2020).

Um sistema de criptografia de vídeos para comunicação ultrassônica foi apresentado por Huang et al.. Neste método, os pixels têm sua posição e intensidade alterada através dos mapas de Arnold e logístico, respectivamente. A combinação destes mapas faz com que o algoritmo tenha bons resultados de segurança no teste de histograma (ver na seção 2.8). Entretanto, o trabalho não apresenta uma estratégia visando a redução do custo computacional e aumento na velocidade de encriptação, o que pode tornar o algoritmo inadequado para transmissões ao vivo (HUANG et al., 2021). Zhang et al. propuseram um método de criptografia baseado na discretização do sistema hipercaótico de Lorentz. Os autores apontaram a necessidade de mais estudo buscando a redução custo computacional e aumento de eficiência da codificação (ZHANG et al., 2021). Ainda em 2021, Salama e Aly usaram o mapa de Arnold para embaralhar os quadros de um vídeo usando o codificador MPEG-2 (SALAMA; ALY, 2021).

Em 2022, El-Mowafy et al. propuseram dois algoritmos de criptografia de vídeos codificados por H.264. O primeiro propõe um método robusto que usa mapas caóticos, o segundo propõe um algoritmo que mescla técnicas de esteganografia (técnicas para ocultar a existência de uma imagem dentro de outra) e um método de criptografia baseada em caos. Os autores apontaram que o mapa logístico ofereceu maior eficiência para o algoritmo (EL-MOWAFY et al., 2022).

2.8 Testes de Segurança e Velocidade

Um bom algoritmo de criptografia para transmissões ao vivo deve ser seguro sem comprometer na velocidade do envio, por isso é necessário realizar testes para avaliar segurança e velocidade de transmissão.

2.8.1 Inspeção Visual

A **inspeção visual** é considerada uma das métricas mais importantes para examinar um quadro criptografado de maneira qualitativa. A perda das características essenciais da imagem pode anular o efeito da vigilância do adversário (terceiro indesejado que deseja interceptar os dados) na interceptação dos dados. Portanto, quanto mais ocultas elas estiverem, melhor será o algoritmo de criptografia. Mas isso não é o suficiente para garantir a segurança do método (ABD EL-SAMIE et al., 2013).

2.8.2 Difusão

A difusão é um parâmetro importante, pois avalia a randomização do algoritmo de criptografia. Isso significa que a difusão é alta quando o quadro original tem uma relação muito complexa com o quadro criptografado. A **difusão por efeito avalanche** é uma métrica usada para testar a eficiência da difusão. A partir de um quadro original P usando uma chave c é gerado o quadro criptografado C, com a mínima alteração possível na chave c é obtido a chave c' usada para criptografar P e gerar C'. O efeito avalanche é a porcentagem de bits diferentes entre C e C', se a diferença for de pelo menos 50%, então o método possui um comportamento caótico elevado, pois uma pequena alteração na chave gera um resultado significativamente diferente (ABD EL-SAMIE et al., 2013).

2.8.3 Desvio de Histograma

O **desvio de histograma**, é uma medida que avalia a qualidade da criptografia em termos das diferenças entre as imagens original e criptografada. O objetivo é quantificar a diferença entre os histogramas das duas imagens e, assim, avaliar a qualidade da criptografia. Para isso, o histograma $HP_{(k)}$ da imagem original $(P(i,j))$ de dimensão $n \times m$ é estimado a partir do algoritmo:

> **Histograma de uma imagem.**
> **entrada:** inteiros $k = 0$, $i = 0$ e $j = 0$.
> **saída:** histograma $HP_{(k)}$.
> **etapa 1:** se $k = P(i,j)$, então $H_k = H_k + 1$ caso contrário não faça nada.
> **etapa 2:** se $i = n - 1$ vá para etapa 3, caso contrário $i = i + 1$ e volte na etapa 1.
> **etapa 3:** se $j = m - 1$ vá para etapa 4, caso contrário $j = j + 1$ e volte na etapa 1.
> **etapa 4:** se $k = 255$ pare, caso contrário $k = k + 1$ e volte na etapa 1.

De forma análoga é calculado o histograma para a imagem criptografada $(C(i,j))$, o histograma $HC_{(k)}$. Então é estimado a diferença absoluta D_{PC} através do algoritmo:

Diferença absoluta de histograma.
entrada: um inteiro $k = 0$.
saída: diferença absoluta D_{PC}.
etapa 1: $D_{PC(k)} = HP_{(k)} - HC_{(k)}$
etapa 4: se $k = 255$ pare, caso contrário $k = k + 1$ e volte na etapa 1.

Assim, o desvio de histograma é dado por:

$$D_H = \frac{\frac{D_{PC(0)}+D_{PC(255)}}{2} + \sum_{l=1}^{254} D_{PC(l)}}{nm}.$$

Concluindo que quanto maior o valor de D_H, melhor será a qualidade da criptografia neste quadro em termos de maximização de desvio (ABD EL-SAMIE et al., 2013).

2.8.4 Coeficiente de Correlação Linear

Seja $(C(i,j))$ a imagem resultante da encriptação de uma imagem $(P(i,j))$. O **coeficiente de correlação linear** é uma métrica usada para medir as relações lineares entre os pixels das duas imagens. Dessa forma, essa métrica é usada para quantificar a semelhança entre os pixels correspondentes nas duas imagens e, assim, avaliar a qualidade da criptografia (MORETTIN; BUSSAB, 2010). O coeficiente de correlação de $(C(i,j))$ e $(P(i,j))$ é dado por

$$r_{PC} = \frac{n\sum_{i=1}^{n}\sum_{j=1}^{m} P(i,j)\,C(i,j) - \sum_{i=1}^{n}\sum_{j=1}^{m} P(i,j)\sum_{i=1}^{n}\sum_{j=1}^{m} C(i,j)}{\sqrt{n\sum_{i=1}^{n}\sum_{j=1}^{m} P(i,j)^2 - \left(\sum_{i=1}^{n}\sum_{j=1}^{m} P(i,j)\right)^2}\sqrt{n\sum_{i=1}^{n}\sum_{j=1}^{m} C(i,j)^2 - \left(\sum_{i=1}^{n}\sum_{j=1}^{m} C(i,j)\right)^2}}.$$

Os valores de r_{PC} variam de -1 a 1, sendo que 1 significa que existe uma relação direta entre os pixels dos dois quadros e -1 significa que a relação é inversa. Concluímos que, quanto mais próximo de zero for r_{PC}, mais segura será a criptografia, de fato, se $r_{PC} = 0$, então não existe uma relação linear entre os pixels dos dois quadros (MORETTIN; BUSSAB, 2010).

2.8.5 NPCR e UACI

O **NPCR** e o **UACI** são úteis para avaliar a influência de um pixel em todo quadro criptografado. Para o cálculo, é criptografado dois quadros de dimensão $n \times m$ com

diferença de intensidade em apenas um pixel, denotadas por C_1e C_2. É rotulado os valores de intensidade dos pixels na grade (i, j) em C_1e C_2 por $C_1\,(i, j)$ e $C_2\,(i, j)$, respectivamente. Assim é definido uma matriz binária $n \times m$, $(D\,(i, j))$ da seguinte maneira

$$D\,(i, j) = \begin{cases} 0, & \text{se } C_1\,(i, j) = C_2\,(i, j) \\ 1, & \text{se } C_1\,(i, j) \neq C_2\,(i, j)\,. \end{cases}$$

O NPCR é definido por

$$\text{NPCR} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} D\,(i, j)}{nm} \times 100.$$

Deste modo, ele mede a porcentagem de pixels diferentes nos dois quadros, quanto maior o seu valor, melhor será a criptografia (ABD EL-SAMIE et al., 2013).

O UACI é definido por

$$\text{UACI} = \frac{1}{nm}\left(\sum_{i=1}^{n}\sum_{j=1}^{m} \frac{C_1\,(i, j) - C_2\,(i, j)}{255}\right) \times 100.$$

Sendo assim, ele mede a média das diferenças das intensidades entre os dois quadros criptografados, quanto maior o seu valor, melhor será a criptografia (ABD EL-SAMIE et al., 2013).

2.8.6 Velocidade

Por fim, existem os testes de velocidade, fundamentais para as transmissões ao vivo, pois se o custo computacional ou o tempo presumido de um método de criptografia de vídeos for muito baixo esse método é adequado para transmissões ao vivo. De maneira qualitativa, o algoritmo é validado se o receptor conseguir assistir o vídeo sem perda de informações e sem atrasos relevantes na transmissão. De forma quantitativa, o tempo para geração da chave é avaliado juntamente com o **tempo de encriptação**, isto é, o tempo total para criptografar e descriptografar os dados, medido em segundos (KOCAREV; LIAN, 2011).

Capítulo 3

Materiais e Métodos

3.1 Materiais

Os códigos empregados neste trabalho foram concebidos nas linguagens de programação C e C++, embora sua implementação seja passível de reprodução em diversas linguagens. Todos os códigos foram implementados e testados em um ambiente Fedora Linux®, aproveitando as vantagens de estabilidade e flexibilidade oferecidas por este sistema operacional. Os experimentos foram conduzidos em um computador com configurações apresentadas na Tabela 3.1. Os dados são fornecidos para garantir a reprodutibilidade dos experimentos, permitindo que outros pesquisadores reproduzam e validem os resultados apresentados neste estudo. Contudo, não é necessário usar as mesmas configurações para desenvolver o método de criptografia caótica de vídeos em transmissões ao vivo. A flexibilidade é mantida nesse aspecto, possibilitando a adaptação do método em diferentes contextos e configurações.

Tabela 3.1: Configurações de hardware

Componente	**Especificação**
Processador	Intel® Core™ i7-11800H
Placa de vídeo	GeForce® RTX™ 3060 Laptop
Memória RAM	16Gb 3200Mhz

3.2 Métodos

Nesta seção, descreve-se o desenvolvimento do projeto. Primeiramente, realizou-se a seleção do momento e do método de compressão, seguido pelo desenvolvimento dos algoritmos dos métodos de criptografia e dos testes de segurança e velocidade. Por fim, propõe-se um método para a criptografia destinada às transmissões ao vivo.

3.2.1 Escolha do Método e Momento da Compressão

A primeira fase deste trabalho consistiu na seleção do método e momento para a compressão de vídeos. A escolha do método de compressão foi pautada no equilíbrio entre a qualidade do vídeo e o tamanho dos dados, visando assegurar uma transmissão fluida e sem interrupções. Para tal conduziu-se um estudo dos padrões de codificação, complementado por análises comparativas, a fim de determinar qual desses métodos melhor atende às exigências específicas da transmissão ao vivo e se integra de forma otimizada a este projeto. Entre os codificadores examinados incluem-se H.261, H.262, H.263, H.264, MPEG-1, MPEG-2 e MPEG-4, cujos detalhes e análises podem ser consultados nas seções 2.4 e 4.1. A determinação do momento da compressão também se revela uma decisão que impacta diretamente no desempenho e segurança do método. Foi explorado as opções de compressão pós e pré-criptografia, avaliando seus respectivos efeitos no contexto deste projeto, a análise está disponível na seção 4.1.

3.2.2 Desenvolvimento de Métodos de Criptografia

Em seguida, foram desenvolvidos os algoritmos dos mapas caóticos. Estes mapas são responsáveis por gerar sequências de valores imprevisíveis e não periódicos, o que está diretamente ligado à segurança do método de criptografia. Estes mapas podem alterar a posição dos pixels, assim após algumas iterações a imagem resultante é irreconhecível, tornando difícil recuperar a figura original. Por outro lado, existem mapas caóticos que são projetados para modificar a intensidade dos pixels, esses mapas aplicam transformações não lineares nas intensidades, resultando em alterações imprevisíveis. Para a correta escolha dos mapas do método de criptografia fez-se necessário o desenvolvimento dos algoritmos dos mapas e de suas combinações, estas se baseiam na junção de mapas de confusão e difusão. Na Tabela 3.2 são apresentados os métodos desenvolvidos.

No desenvolvimento, foi usada uma *webcam*, com dimensão de 480×640 pixels com escala de cores no padrão RGB, sendo que a sua dimensão e a sua escala de cores foram adotadas como parâmetros dos quadros originais no desenvolvimento do trabalho. Os mapas que alteram a posição dos pixels possuem a particularidade de exigir uma imagem de formato quadrado para a criptografia. Portanto, foi necessário redimensionar a imagem original em todos os métodos que incorporavam um mapa de confusão. A Tabela 3.3 detalha as dimensões dos métodos utilizados. A escolha específica das dimensões relacionadas ao mapa de Arnold é discutida na seção 4.2.1, proporcionando uma compreensão mais aprofundada desse aspecto do desenvolvimento.

Tabela 3.2: Métodos

Método	**Mapa(s) Caótico(s)**
1	Baker
2	Arnold
3	Logístico
4	Hénon
5	Baker + Logístico
6	Baker + Hénon
7	Arnold + Logístico
8	Arnold + Hénon

Tabela 3.3: Dimensões dos métodos

Métodos	**Dimensão [pixels]**
3 e 4	480×640
1, 5 e 6	640×640
2, 7 e 8	642×642

O processo inicial do algoritmo envolve a geração da chave de criptografia, sendo que tal **chave** está relacionada com uma **senha** característica de cada mapa caótico. Essas senhas são definidas das seguintes maneiras:

- **Mapa de Baker** – a senha é dada por $(t : n_1; n_2; \ldots; n_k)$, no qual t é o número de iterações do mapa e $n_1; n_2; \ldots; n_k$ são divisores de N, com $N = n_1 + n_2 + \cdots + n_k$, sendo N a largura da imagem.

- **Mapa de Arnold** – a senha corresponde ao par $(t; p)$, no qual t é o número de iterações e p é período do mapa para imagens de determinadas dimensão. Desta forma são necessárias t iterações para gerar a chave de criptografia e $p - t$ iterações para gerar a chave de descriptografia.

- **Mapa logístico** – a senha é o par $(r; x_0)$, no qual r é o parâmetro e x_0 é a condição inicial do mapa, sendo tomado como um número racional positivo.

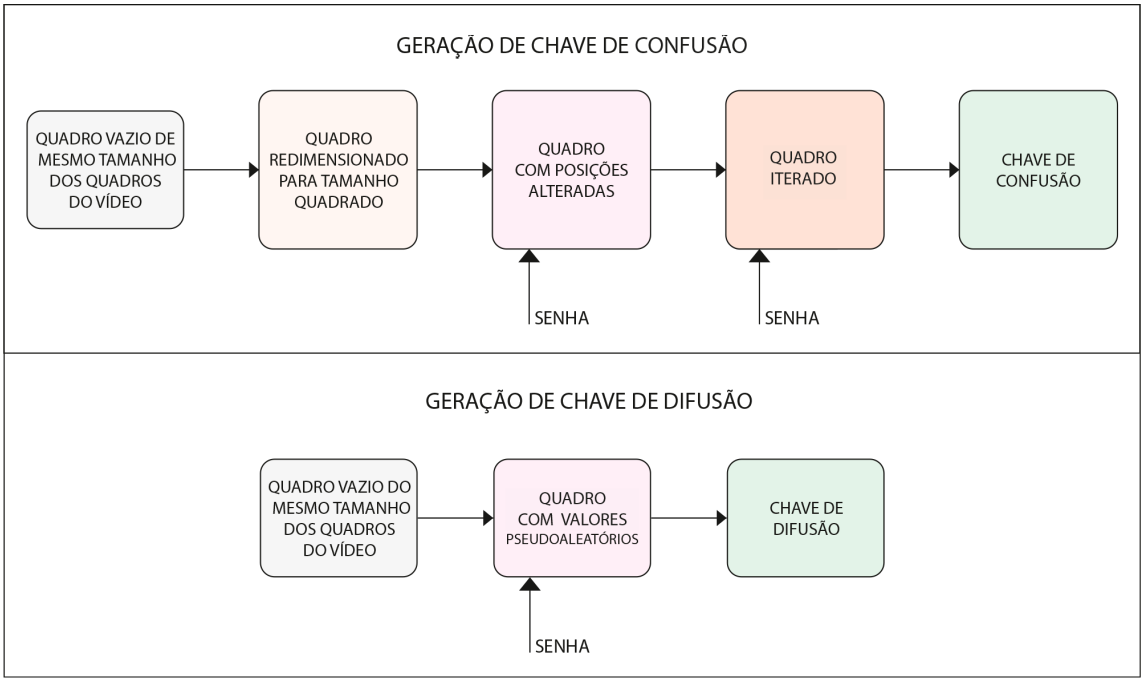
- **Mapa de Hénon** – a senha consiste no vetor $(a; b; x_0; y_0)$, no qual a e b são os parâmetros e x_0 e y_0 as condições iniciais do mapa, sendo tomados como números racionais positivos.

Neste trabalho as chaves de criptografia são adotadas como os próprios mapas caóticos. Assim, as chaves são responsáveis pelos seguintes processos no algoritmo de criptografia:

- **Chave de confusão** – indica as posições para as quais cada pixel deve se mover, gerando o embaralhamento dos pixels de um quadro.
- **Chave de difusão** – é uma matriz de valores pseudoaleatórios, gerados pelo do mapa caótico. Os valores desta matriz são operados, coordenada a coordenada através da operação XOR, com os valores de intensidades de um quadro, alterando, assim, as intensidades dos pixels deste quadro.

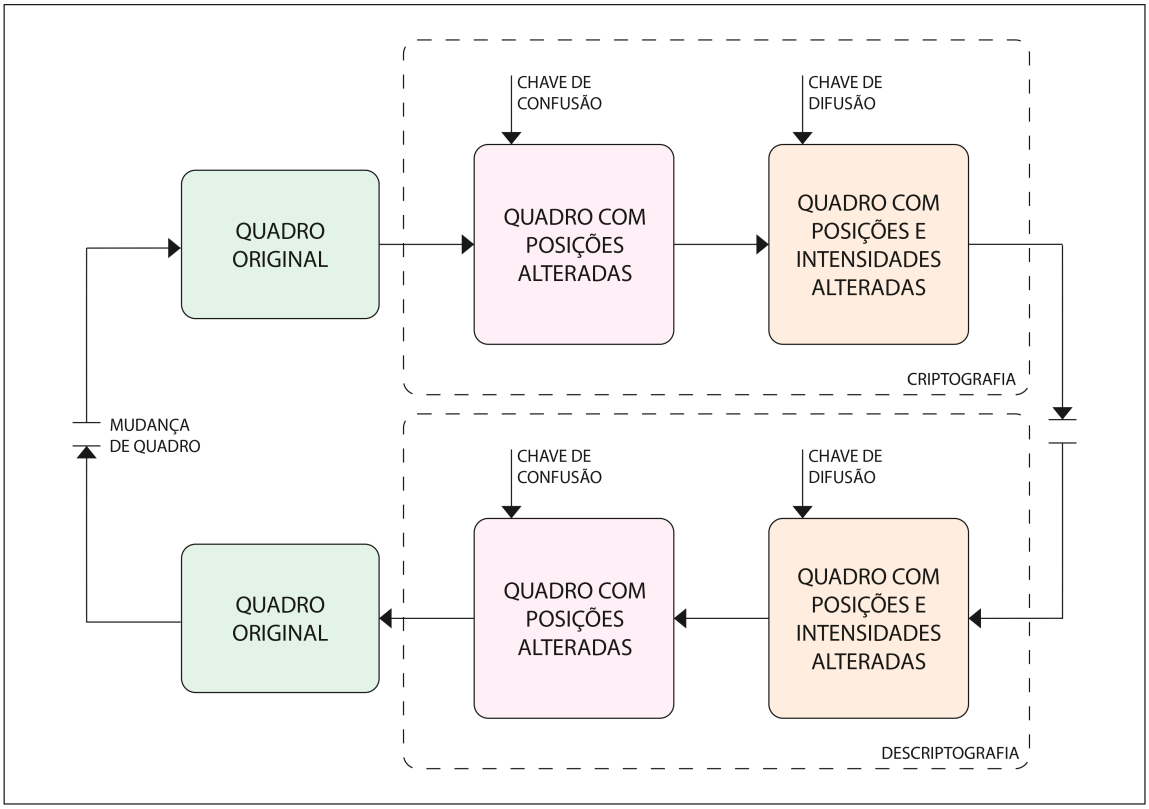
Na Figura 3.1, apresenta-se o passo a passo para a geração de chaves, tanto nos mapas de confusão quanto nos mapas de difusão. Observa-se que os mapas de confusão necessitam de iterações para um efetivo embaralhamento (cf. seção 2.6).

Figura 3.1: Fluxogramas de geração das chaves



A partir das chaves geradas é possível a encriptação quadro a quadro do vídeo. É adotado como **encriptação** o processo de criptografar e descriptografar. Na Figura 3.2 é apresentado o fluxograma de encriptação, no qual o quadro original é criptografado através do embaralhamento causado pela chave de confusão e da alteração da intensidade dos pixels pela chave de difusão. O caminho inverso reconstrói o quadro original. Assim, o processo continua com a encriptação de um novo quadro.

Figura 3.2: Fluxograma de encriptação



3.2.3 Validação da Segurança e Velocidade

A partir da construção dos algoritmos de encriptação torna-se necessário validá-los, a fim de escolher a combinação adequada de mapas caóticos. Um bom algoritmo de criptografia para transmissões ao vivo deve ser seguro e com uma boa velocidade de encriptação. Para isso, foi realizada a validação dos mapas caóticos através dos testes de segurança: inspeção visual, desvio de histograma, difusão por efeito avalanche, coeficiente de correlação, NPCR e UACI (cf. seção 2.8). Todos os testes foram executados usando um vídeo de monitoramento rodoviário (Figura 3.3), a fim de padronizar os testes para comparar a eficiência dos mapas.

A velocidade é um fator importante para as transmissões ao vivo. A fim de validá-la o tempo de geração das chaves é medido e a média do tempo de encriptação é calculada, dos 500 primeiros quadros do vídeo (Figura 3.3). Por fim, é possível prever quantos quadros podem ser criptografados por segundo.

Figura 3.3: Quadro de vídeo de monitoramento rodoviário

Fonte: Techblog.gr (2010)

3.2.4 Proposta de Método

A consolidação efetiva da proposta do método de criptografia caótica de vídeos para transmissão ao vivo reside na escolha dos mapas caóticos, com base nos resultados de segurança e velocidade da (cf. seção 4.8) e do momento e método de compressão (cf. seção 4.1). Assim, desenvolvendo um método seguro e eficiente em termos computacionais, obtendo um método de criptografia robusto, adaptável e eficiente para transmissões ao vivo. Por fim, são analisadas as vantagens e desvantagens do criptossistema, além de apresentar as suas devidas aplicações.

Capítulo 4

Resultados e Análises

Este capítulo apresenta os principais resultados obtidos ao longo do trabalho, proporcionando uma visão ampla das contribuições alcançadas. Cada seção aborda aspectos específicos do projeto. Inicialmente, foi feita uma análise do método de compressão, bem como o momento em que o algoritmo de criptografia comprime os quadros. Em seguida, os parâmetros dos mapas caóticos foram ajustados com o objetivo de otimizar suas características de segurança e velocidade. Munido de parâmetros e configurações adequadas, os algoritmos foram submetidos a uma "bateria de testes" visando compará-los quanto a segurança e velocidade de criptografia. Ademais, foram exploradas algumas possibilidades de melhoria nos resultados dos testes de segurança. Por fim, foi proposto o método de criptografia caótica de vídeos.

4.1 Método e Momento da Compressão

Inicialmente, foi proposto a construção de um algoritmo de criptografia focado na cifragem seletiva de quadros-chave e quadros-delta, visando otimizar a velocidade do processo. No entanto, ao examinar os métodos de compressão, tornou-se evidente a eficácia superior dos métodos mais recentes. Nestes métodos, as técnicas de compressão interquadros foram substituídas pela predição e compensação de movimento. De fato, a cifragem seletiva de quadros-chave e quadros-delta exigiria uma implementação complexa e a utilização de algoritmos de compressão desatualizados, que resultaram em taxas de compressão mais baixas. Diante desse panorama, as análises sobre a velocidade de execução dos métodos de criptografia revelaram que o desempenho não estava unicamente vinculado à compressão, mas também à estrutura do método de criptografia. Assim, este trabalho focou na construção do algoritmo criptografia de forma otimizada e na adoção de métodos atuais de compressão, resultando em uma abordagem mais segura e eficaz. A escolha do momento de compressão levou em conta o fato que os mapas de confusão, necessitam das informações a respeito de todos os pixels de cada quadro. Dessa

forma, a compressão deve ocorrer após a criptografia. Assim, os mapas caóticos atuam sobre os dados no formato de imagens, mantendo a eficácia do processo de cifragem. Garantindo a reversibilidade do processo, isto é, assegurando que seja possível recuperar a imagem original na descriptografia.

O método de compressão escolhido para este trabalho foi o H.264 com perfil 4.4.4 e CRF igual a 0. Essa decisão é respaldada pela eficiência comprovada do H.264, desenvolvido para transmissões ao vivo. A capacidade do H.264 de suportar predição de quadros, opções versáteis de compressão, dimensões de até 4320×7680 pixels, e taxas de até 240 QPS, o torna uma escolha versátil e eficaz para diversas aplicações. O CRF de 0, adotado neste contexto, visou preservar a máxima fidelidade em relação ao arquivo original, indicando uma taxa de compressão mínima, contudo fiel ao conteúdo original. A escolha do perfil 4:4:4 no H.264, que não subamostra informações de cor, é fundamental para atender aos requisitos da compressão sem perdas, assegurando a integridade dos dados criptografados. Essa abordagem proporciona uma combinação equilibrada entre qualidade de compressão, preservação da informação e eficiência na transmissão, visando atender os objetivos propostos nesse trabalho.

4.2 Ajustes de Parâmetros

Nesta seção, foi realizada uma análise criteriosa dos parâmetros essenciais dos mapas caóticos, buscando aprimorar suas características fundamentais. Os parâmetros analisados desempenham um papel crucial para o comportamento caótico desses mapas, sendo que este comportamento é essencial para o melhor desempenho dos mapas no contexto de criptografia.

4.2.1 Período do Mapa de Arnold

O período do mapa de Arnold tem relação direta com a dimensão dos quadros do vídeo, sendo que neste trabalho o vídeo foi dimensionado em 480×640 pixels. Como este mapa é definido apenas para imagens quadradas, e a menor imagem quadrada possível proveniente da ampliação dos quadros do vídeo têm dimensão 640×640 pixels. Esperava-se que essa seria a dimensão do vídeo que melhor se adequaria a este trabalho. Entretanto, o mapa de Arnold apresenta algumas particularidades para imagens com essa dimensão. A Tabela 4.1 mostra o período de cinco dimensões de imagens, que variam de 640×640 pixels até 682×682 pixels. Esta tabela foi gerada por meio de testes brutos, que identifica quantas iterações são necessárias para que todos os pixels retornem às suas posições iniciais, sendo que o período da imagem é tomado como o mínimo múltiplo comum do período de todos os pixels.

Tabela 4.1: Períodos mapa de Arnold

Dimensão [pixel]	**Período**
640×640	480
642×642	36
644×644	24
646×646	18
682×682	15

Este parâmetro exerce uma influência direta no tempo dedicado à fase de criptografia. A definição do período é crucial, uma vez que determina o número de iterações necessárias para que a imagem retorne ao seu estado original. Quanto maior o período, mais iterações são necessárias, resultando em um aumento no tempo despendido na geração da chave de criptografia. Além disso, ao considerar o tempo de criptografia de cada quadro, a dimensão do quadro desempenha um papel significativo. Quanto maior a dimensão, mais tempo é requerido para calcular as novas posições durante o processo de criptografia. Sendo assim, a Tabela 4.2 apresenta as amostras do tempo de geração de chave e o tempo médio de encriptação dos 500 primeiros quadros do vídeo de monitoramento rodoviário (Figura 3.3) para cada dimensão de quadro.

Tabela 4.2: Velocidade de criptografia do mapa de Arnold

Dimensão [pixel]	**Período**	**Geração de chave [s]**	**Encriptação [ms]**
640×640	480	33,16940	5,05
642×642	36	1,86321	6,34
644×644	24	1,56799	6,43
646×646	18	1,12825	6,52
682×682	15	1,01440	7,29

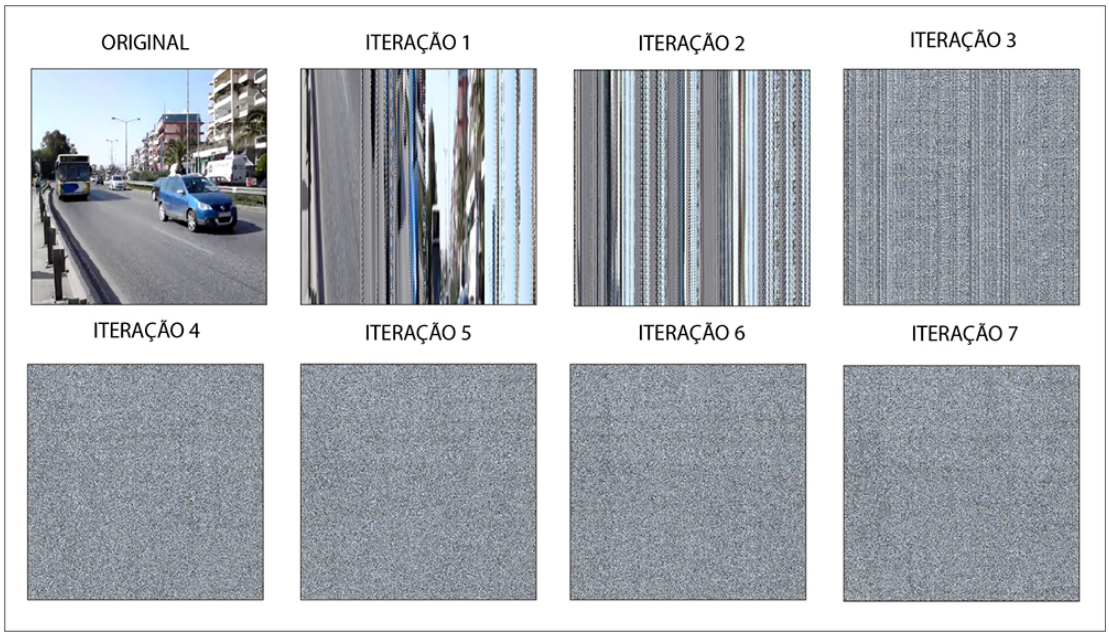
A dimensão 640×640 apresentou o menor tempo de encriptação. No entanto, para gerar a chave relativa a essa dimensão é necessário iterar o mapa 480 vezes, o que resulta em um tempo de geração de chave muito alto em relação às outras dimensões. Em relação ao tempo de encriptação, é fato que quanto menor a dimensão, menor é o tempo de encriptação. Diante disso, a configuração mais apropriada se revelou na dimensão de 642×642 pixels. Esta dimensão ofereceu a vantagem de apresentar o segundo menor tempo de encriptação, contudo, o seu tempo de geração de chave é consideravelmente menor em comparação com a dimensão de menor tempo de encriptação. Assim, a escolha de 642×642 fez com que a senha do Mapa de Arnold seja o par $(t; 36)$, isto implica que são necessárias t iterações para gerar a chave de criptografia e $36 - t$ iterações para gerar a chave de descriptografia. Para

aumentar a eficiência gerando uma única chave para criptografar e descriptografar, tomou-se $t = 18$, dessa forma, a senha do mapa de Arnold foi o par $(18; 36)$. Essa escolha resultou em uma eficiente combinação de desempenho e eficácia no contexto do trabalho.

4.2.2 Iterações do Mapa de Baker

O mapa de Baker, quando executado apenas uma vez, realiza um embaralhamento inicial da posição dos pixels de forma caótica. No entanto, para resultados mais aprimorados é necessário que o quadro original seja submetido a várias iterações. Isso é evidenciado na Figura 4.1 na qual o mapa de Baker foi iterado sete vezes no quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3) redimensionado para a dimensão 640×640 pixels.

Figura 4.1: Iterações do mapa de Baker



A inspeção visual revelou que, ao aumentar o número de iterações, o mapa de Baker realiza um embaralhamento mais complexo e eficaz, contribuindo para a dispersão uniforme dos pixels na imagem e, consequentemente, fortalecendo a robustez do processo de criptografia. Essa abordagem iterativa desempenha um papel crucial na melhoria do embaralhamento de pixels, otimizando a segurança e a complexidade do algoritmo de criptografia. O parâmetro escolhido foi 5, visto que essa quantidade de iterações já apresenta uma notável dispersão dos pixels, indicando um estágio de embaralhamento adequado para fins de segurança e eficiência, este parâmetro foi tomado como uma das senhas do mapa de Baker. O ideal é que seja o menor número de iterações possível com a dispersão necessária, pois o aumento do número de iterações resulta em um maior tempo de geração de chave, conforme as amostras apresentadas na Tabela 4.3. Desta forma, a senha tomada foi $(5 : 2; 4; 160; 40; 40; 8; 80; 2; 4; 160; 40; 8; 2; 4; 40; 2; 2; 40; 2)$.

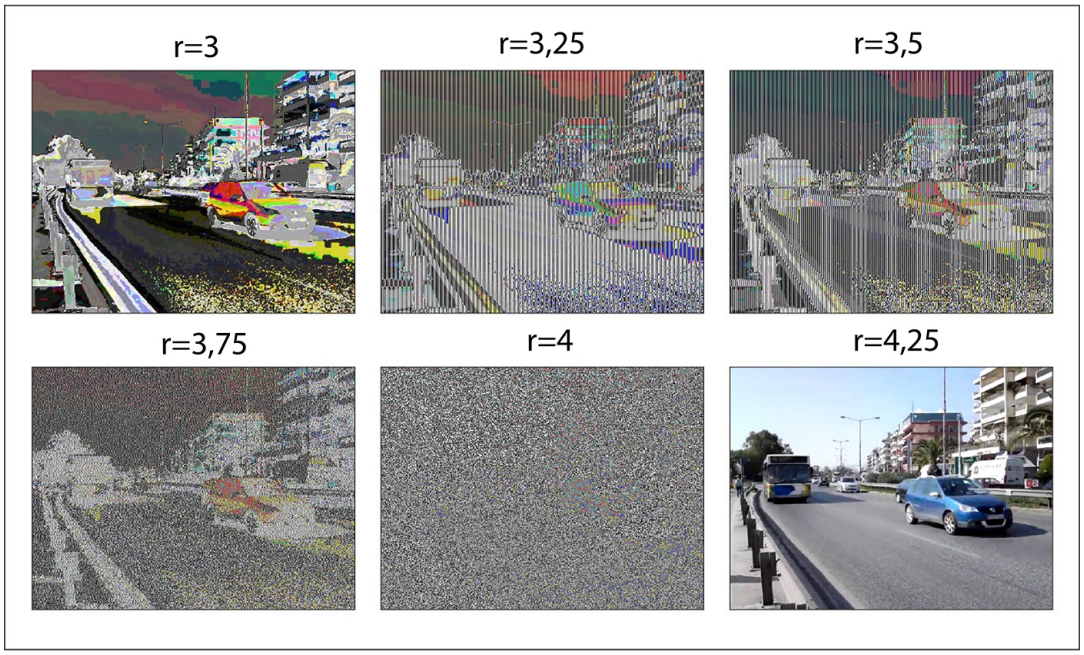
Tabela 4.3: Velocidade de geração de chave do mapa de Baker

Iterações	Geração de chave [s]
1	0,43900
2	0,46461
3	0,56424
4	0,57346
5	0,64410
6	0,71568
7	0,79662

4.2.3 Parâmetros do Mapa Logístico

O mapa logístico é usado para causar difusão nas imagens, e para alcançar esse efeito, é essencial selecionar o parâmetro r de maneira a garantir o comportamento caótico do mapa. Em geral, o caos é obtido com a escolha de valores dentro do intervalo $3,5 \leq r \leq 4$ (KOCAREV; LIAN, 2011). O ajuste preciso desse parâmetro pôde ser facilmente observado por meio de inspeção visual da imagem criptografada do quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3), variando os valores de r no intervalo de 3 a 4, 25, conforme ilustrado na Figura 4.2. Assim a senha adotada foi o par $(4; 0, 123456789)$.

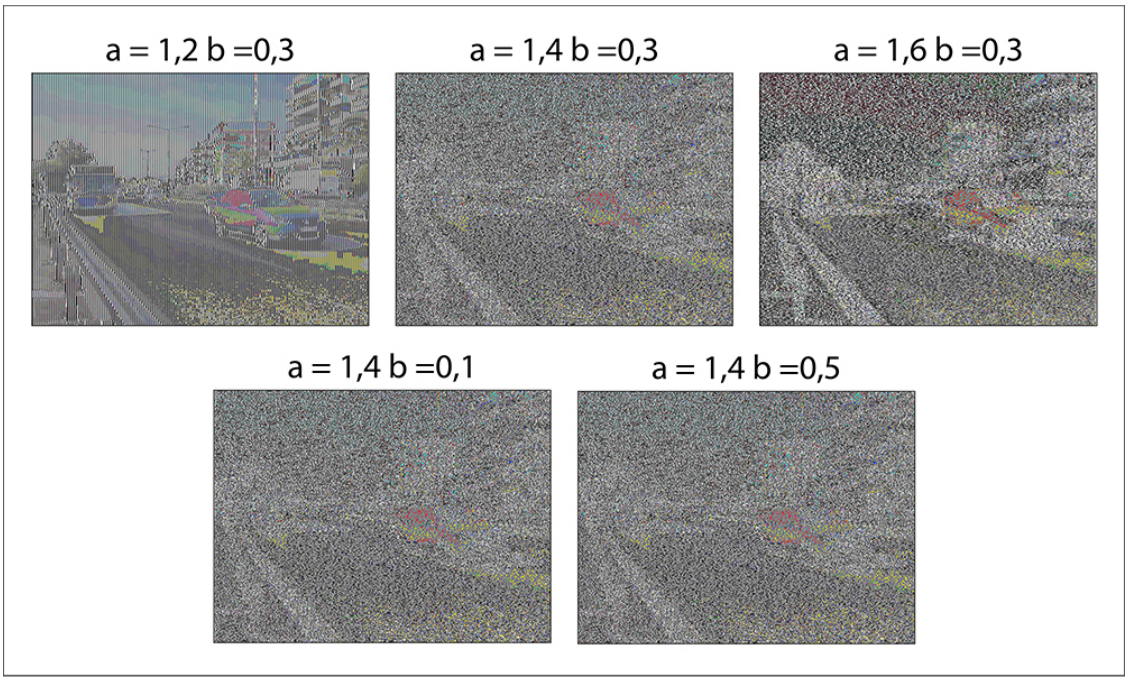
Figura 4.2: Influência de parâmetro r no mapa logístico



4.2.4 Parâmetros do Mapa de Hénon

O mapa de Hénon age de forma semelhante ao mapa logístico. Por ser um mapa bidimensional ele tem dois parâmetros a e b que são ajustados com o objetivo de garantir o comportamento caótico do mapa. O trabalho original de Hénon usa $a = 1,4$ e $b = 0,3$, na Figura 4.3 observa-se na inspeção visual da imagem criptografada do quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3) uma forte influência do parâmetro a para o comportamento caótico, sendo que b influencia pouco. De acordo com a análise da Figura 4.3 a e b foram mantidos com seus parâmetros conceituais, em que $a = 1,4$ e $b = 0,3$. Assim a senha adotada foi o vetor $(1,4; 0,3; 0,1; 0,1)$.

Figura 4.3: Influência dos parâmetros a e b no mapa de Hénon



4.3 Inspeção Visual

A perda das características essenciais da imagem torna-se evidente através da inspeção visual. Na Figura 4.4, é possível comparar a imagem (quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3)) com as suas imagens criptografadas por diferentes combinações de mapas caóticos. A análise revelou que, devido às propriedades caóticas inerentes aos mapas utilizados, os quadros criptografados perdem suas características distintivas originais. Ao observar a imagem criptografada pelo mapa de Arnold foi possível ver um padrão de construção com linhas diagonais na imagem criptografada. No entanto, em mapas que alteram somente a intensidade dos pixels, isto é, o mapa logístico e o mapa de Hénon, foi possível observar regiões que representam objetos do quadro original. Na Figura 4.5 nota-se a presença do objeto carro azul em

ambas as imagens criptografadas pelos mapas de intensidade. Essa observação ressaltou a importância do uso de mapas de confusão, contribuindo para a eficácia dos algoritmos de criptografia.

Figura 4.4: Inspeção visual dos métodos

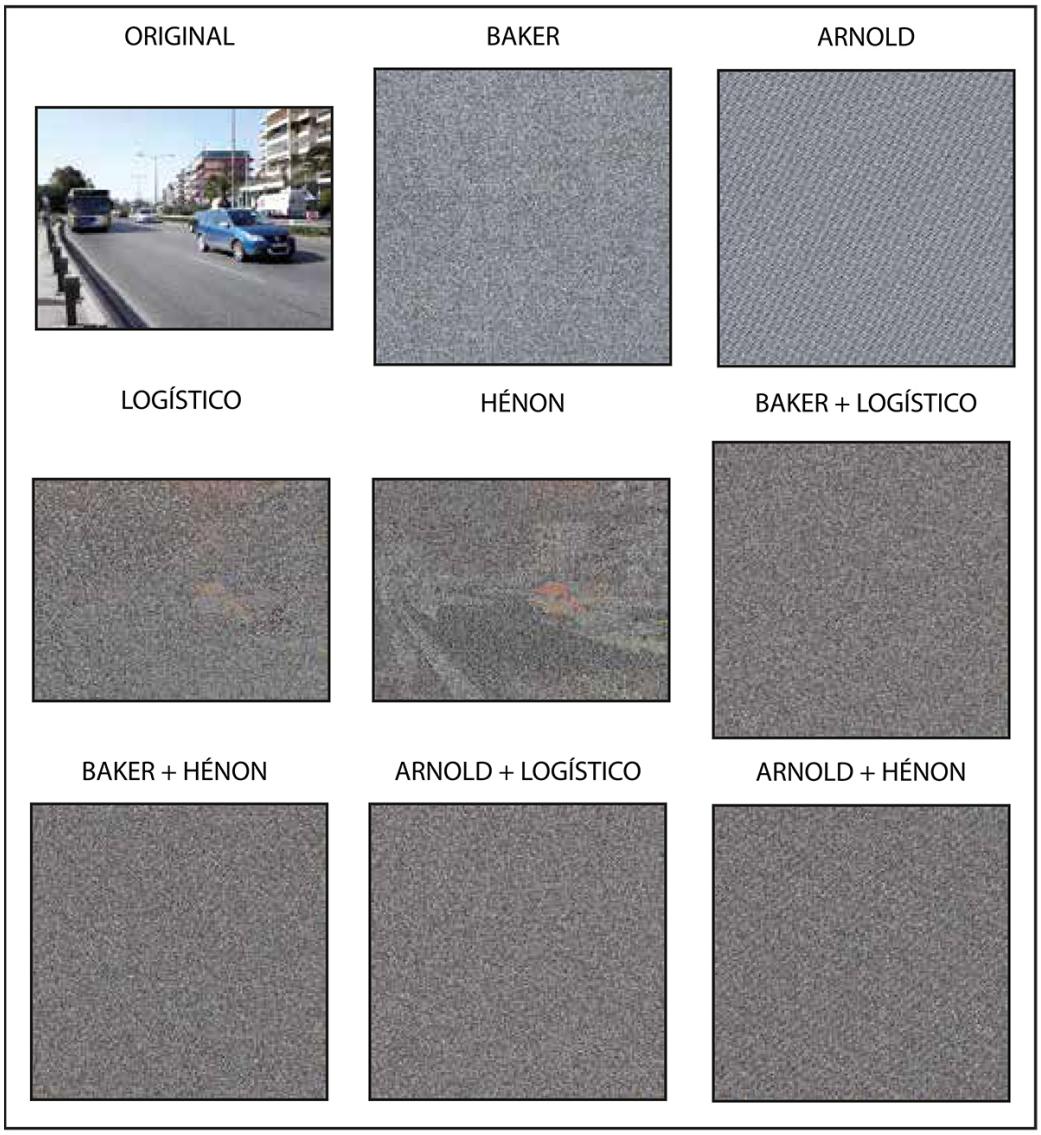
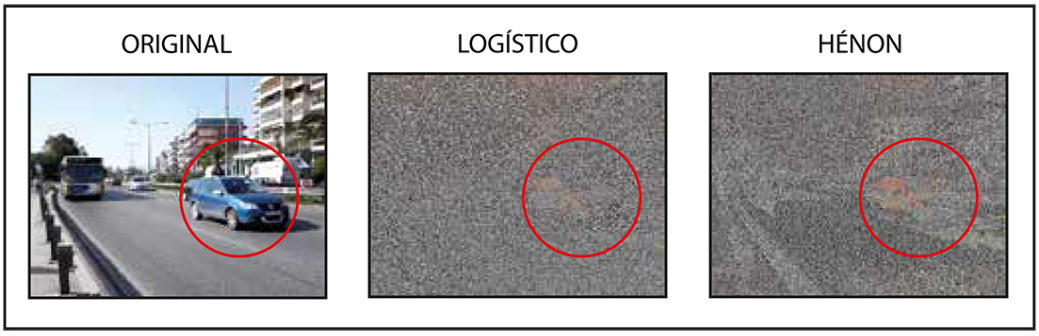


Figura 4.5: Inspeção visual dos mapas de difusão



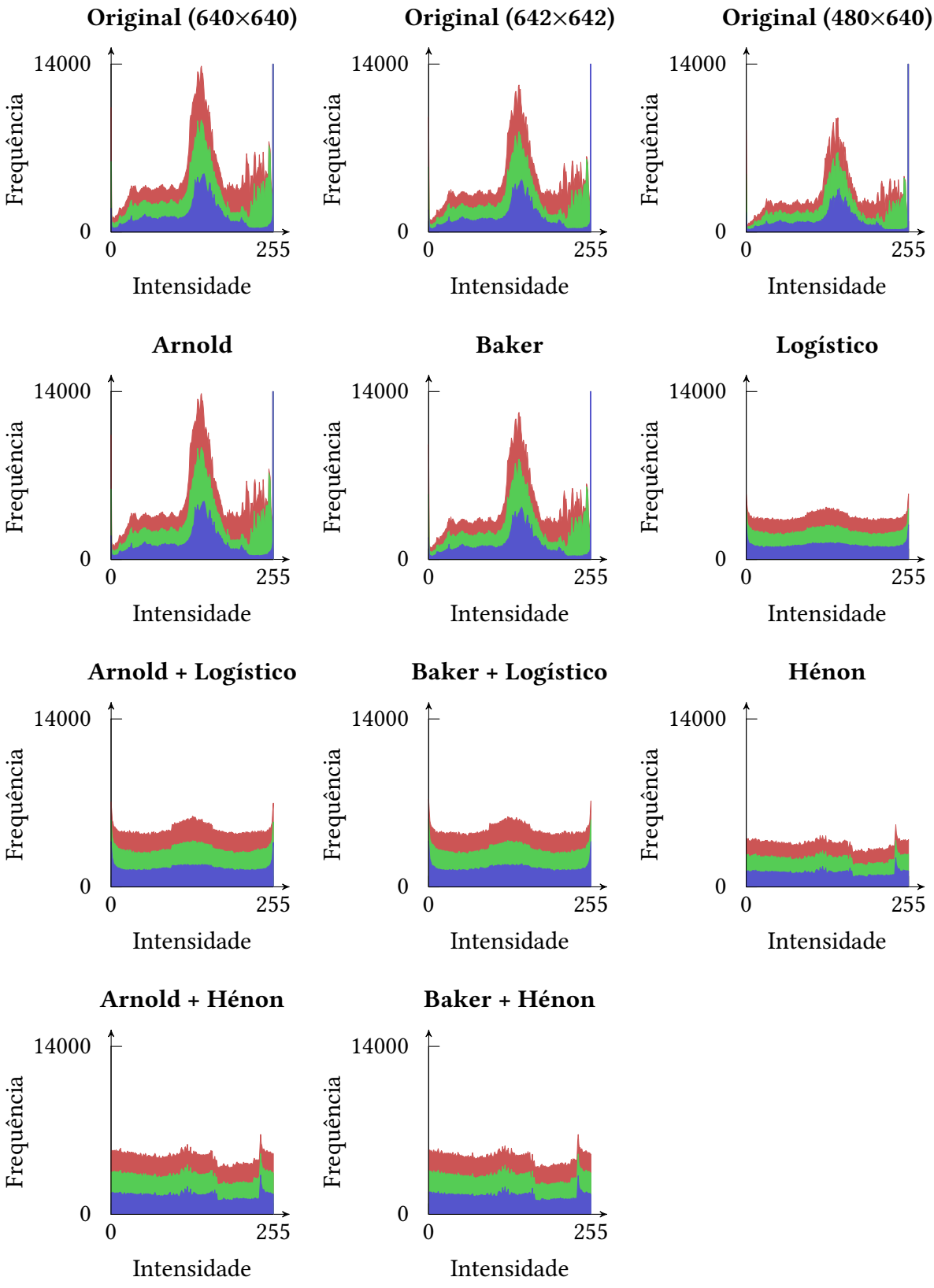
4.4 Desvio de Histograma

O desvio de histograma é uma métrica importante, pois avalia a difusão da criptografia, ou seja, a discrepância na distribuição de intensidades entre o quadro original e o quadro criptografado, sendo que quanto maior o desvio de histograma mais seguro é o método de criptografia. A Figura 4.6 apresenta os histogramas do quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3) e os histogramas do mesmo quadro criptografado por cada um dos métodos apresentados neste trabalho. Notou-se que os mapas de Baker e Arnold não apresentaram desvios, de fato, os mapas de confusão não alteram as intensidades dos pixels, fazendo com que não haja diferenças entre as distribuições de intensidades do quadro original e o quadro criptografado. A análise da Tabela 4.4 revelou que o mapa de Hénon se destaca em relação ao mapa logístico, apresentando maiores desvios, com diferenças percentuais de 7,42% quando estão sozinhos, 8,03% quando associados ao mapa de Baker e 7,68% quando combinados com o mapa de Arnold. Essa análise evidencia a importância do uso dos mapas de difusão, visto que estes mapas possuem a propriedade de alterar a intensidade dos pixels da imagem, e isso aumenta potencialmente a segurança do algoritmo.

Tabela 4.4: Resultados de desvio de histograma

Mapa(s) do método	**Desvio [%]**
Baker	0,00
Arnold	0,00
Logístico	24,12
Hénon	25,91
Baker + Logístico	23,65
Baker + Hénon	25,55
Arnold + Logístico	23,69
Arnold + Hénon	25,51

Figura 4.6: Histogramas dos métodos



4.5 Difusão

A difusão por efeito avalanche é usada para avaliar a eficiência da randomização do algoritmo de criptografia. Sendo que quanto maior a difusão mais robusto é o método em questão. Neste estudo, a difusão foi utilizada para destacar a influência do comportamento caótico dos mapas, no qual uma mínima alteração na senha deve levar a resultados completamente distintos dos resultados originais. Entretanto, nos mapas de confusão essa mudança foi limitada, visto que o mapa de Arnold não permite variação na senha, isto é, no período do mapa (cf. seção 2.6.1), e no mapa de Baker a senha deve satisfazer certas propriedades (cf. seção 2.6.2). O teste de difusão por efeito avalanche tem ampla aplicação nos mapas de difusão, no entanto, as alterações na senha devem ser feitas de forma a garantir o comportamento caótico do mapa, bem como a reversibilidade do processo de criptografia.

Na Tabela 4.5, é possível examinar os resultados da difusão decorrente da menor alteração possível na senha para criptografar o quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3). Os mapas de difusão se destacaram nesse aspecto, visto que promovem alterações na intensidade dos pixels (ABD EL-SAMIE et al., 2013). No teste, foi observado que a difusão produzida pelo mapa de Hénon foi de 99,63%, sendo a maior entre a difusão dos quatro mapas caóticos. Entretanto, o mapa de Hénon apresentou pouca vantagem em relação ao mapa logístico, visto que a diferença percentual entre as difusões produzidas por estes mapas foi de apenas 0,29%.

Tabela 4.5: Resultados da difusão

Mapa	**Difusão [%]**
Baker	28,37
Arnold	não se aplica
Logístico	99,34
Hénon	99,63

4.6 Coeficiente de Correlação Linear

O coeficiente de correlação linear foi usado para medir as relações entre os pixels de um quadro criptografado com o seu respectivo quadro original (quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3)). Na Tabela 4.6, observa-se que todas as combinações dos mapas caóticos apresentam pequenos valores de coeficiente de correlação, resultando em uma relação complexa do quadro criptografado e o quadro original.

Tabela 4.6: Resultados do coeficiente de correlação

Método	**Correlação**
Baker	0,04637
Arnold	-0,00061
Logístico	0,00370
Hénon	-0,65482
Baker + Logístico	0,00005
Baker + Hénon	-0,00201
Arnold + Logístico	0,00066
Arnold + Hénon	0,00205

4.7 Velocidade

A velocidade de encriptação é um fator crucial para as transmissões ao vivo. Como a geração de chave ocorre apenas uma vez, este processo tem menor influência na velocidade da criptografia. A Tabela 4.7 apresenta a amostra do tempo gasto para a geração da chave, o tempo médio de encriptação dos 500 primeiros quadros do vídeo de monitoramento rodoviário (Figura 3.3) e a taxa de quadros encriptados por segundo para cada um dos algoritmos desenvolvidos no trabalho. Foi notório que os mapas de difusão apresentaram os melhores tempos de geração de chave, quando comparados com os mapas de confusão, sendo estes últimos os principais responsáveis pelo tempo gasto para geração de chave das combinações dos mapas caóticos. Ademais, levando em conta a necessidade da utilização de um mapa de confusão e difusão para otimizar a segurança do método (cf. seção 4.8), foi visto que, dentre aqueles que usam os dois tipos de mapas, o algoritmo usando o Mapa de Hénon e mapa de Baker, foi o que apresenta o menor tempo de geração de chave.

Como a chave é gerada apenas uma vez, o que realmente impacta na experiência do usuário é o tempo total de encriptação, pois este pode resultar em atrasos de transmissão. A Tabela 4.7 mostra, novamente, que a melhor eficiência produzida por combinações de mapas foi gerada pelos mapas de Baker e Hénon. A taxa de quadros encriptados por segundo é relevante para dimensionar a eficácia do algoritmo em intervalos de transmissão. Essa taxa leva em consideração outros fatores alheios ao algoritmo de criptografia, tais como a velocidade, influenciada pelo meio de transmissão e pelo processo de compressão. Contudo, a tabela não leva esses fatores em consideração, visto que ela foi usada apenas para comparação dos métodos no que diz respeito ao processo de encriptação.

Tabela 4.7: Resultados de velocidade

Método	Chave [s]	Criptografia [ms]	Descriptografia [ms]	Encriptação [ms]	Taxa [QPS]
Baker	0,64410	2,96	2,78	5,74	174
Arnold	1,86321	3,35	2,98	6,34	157
Logístico	0,00312	1,13	1,13	2,26	442
Hénon	0,00286	1,12	1,12	2,24	446
Baker + Logístico	1,37345	4,03	4,35	8,38	119
Baker + Hénon	1,22995	4,00	4,33	8,32	120
Arnold + Logístico	2,58148	4,40	4,74	9,14	109
Arnold + Hénon	2,50551	4,24	4,63	8,87	112

4.8 Análise dos Métodos

Com base na inspeção visual, tornou-se evidente a necessidade de empregar mapas que alteram a posição dos pixels de forma caótica. Na análise do desvio de histograma, destacou-se a importância do uso de mapas de difusão para alterar a intensidade dos pixels. No contexto dos mapas de confusão, o mapa de Baker demonstrou superioridade em relação ao mapa de Arnold, em termos de velocidade. Ademais, o algoritmo proveniente deste último mapa não pôde ter a sua randomização avaliada por meio do teste de difusão por efeito avalanche. Nos mapas de difusão o mapa de Hénon superou o mapa logístico em todos os testes realizados. Estes destaques foram respaldados pelos resultados dos testes de segurança e velocidade na combinação do mapa de Baker e do mapa de Hénon, quando comparada às outras combinações testadas.

4.9 NPCR e UACI

Uma característica dos algoritmos de criptografia de vídeo é a capacidade de propagar a alteração de um pixel no quadro original para os pixels do quadro criptografado. A relação de pixels alterados é medida pelo NPCR, já a média desses desvios é dada por UACI. Essa característica está relacionada à montagem do algoritmo e independe das combinações dos mapas caóticos. Até este ponto, o método não tinha a capacidade de propagar essas alterações. Este fato foi evidenciado pelos resultados

negativos de NPCR e UACI sem o uso do terceiro nível de segurança, os resultados são apresentados na Tabela 4.8. Os testes foram realizados sobre o algoritmo de criptografia proveniente da combinação dos mapas de Hénon e Baker, usando o quinquagésimo quadro do vídeo de monitoramento rodoviário (Figura 3.3), sendo que para tais testes, o pixel na posição $(0, 0)$ teve sua intensidade alterada para 0. Para solucionar o problema dos resultados negativos de NPCR e UACI foi proposto um terceiro nível de segurança que aproveita do uso da escala de cores no padrão RGB.

Considere a imagem $(f_k\,(i, j))$, de dimensão $n \times m$, onde k é o canal de cores no padrão RGB, isto é, $k = R, G, B$. $(f_k\,(i, j))$ é criptografada pela chave de difusão $(d\,(i, j))$, a partir do algoritmo:

> **Terceiro nível de segurança.**
> **entrada:** uma imagem $(f_k\,(i, j))$, uma chave $(d\,(i, j))$ e inteiros $i = 0$, $j = 0$, $R_{n-1} = 0$ e $G_{n-1} = 0$.
> **saída:** uma imagem criptografada $(c_k\,(i, j))$.
> **etapa 1:** faça $(c_R\,(n - i, m - j)) = (f_R\,(n - i, m - j)) \oplus (d\,(n - i, m - j)) \oplus R_{n-1}$, em que $\oplus$ é a operação XOR.
> **etapa 2:** faça $(c_G\,(i, j)) = (f_G\,(i, j)) \oplus (d\,(i, j)) \oplus G_{n-1}$.
> **etapa 3:** faça $(c_B\,(i, j)) = (f_B\,(i, j)) \oplus (d\,(i, j))$.
> **etapa 4:** atualize $R_{n-1} = (c_R\,(n - i, m - j))$ e atualize $G_{n-1} = (c_G\,(i, j))$.
> **etapa 5:** se $j = m - 1$ vá para etapa 6 com $j = 0$, caso contrário $j = j + 1$ e volte na etapa 1.
> **etapa 6:** se $i = n - 1$ pare, caso contrário $i = i + 1$ e volte na etapa 1.

Na Tabela 4.8, os resultados de NPCR e UACI com o uso do terceiro nível de segurança demonstram a propriedade adquirida. Esse nível de segurança é opcional e depende das necessidades de segurança do algoritmo, visto que isso causa um aumento no tempo de encriptação. A combinação utilizada com esse terceiro nível foi capaz de encriptar 92 quadros por segundo.

Tabela 4.8: Resultados de NPCR e UACI

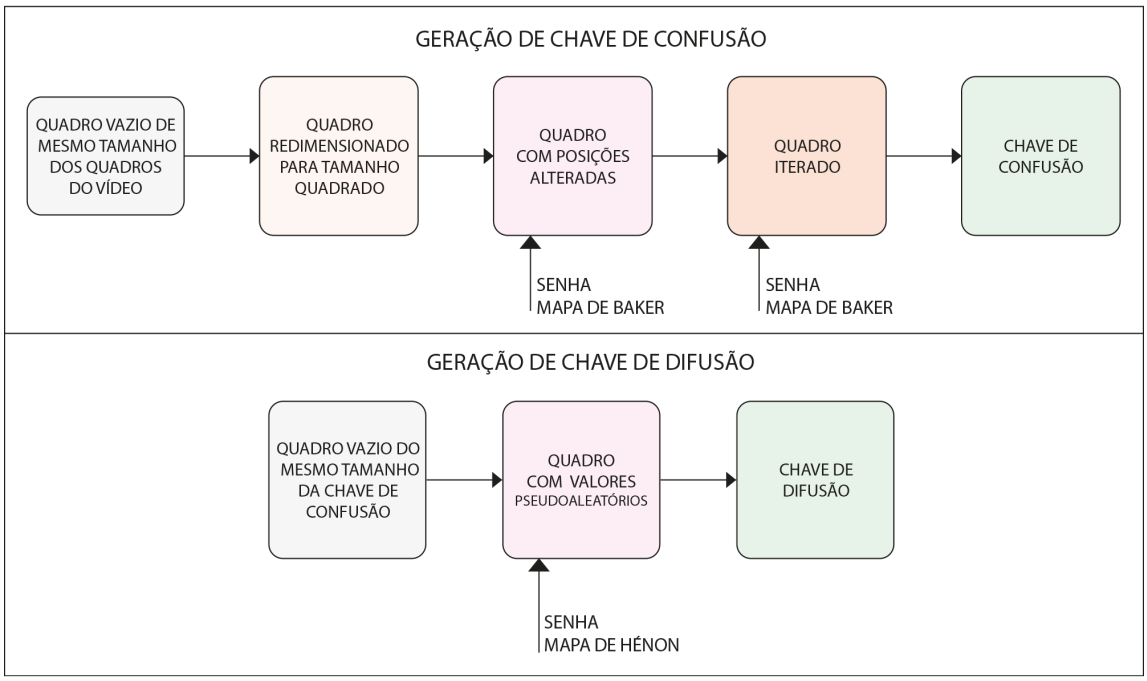
Terceiro nível de segurança	**NPCR [%]**	**UACI [%]**	**Encriptação [ms]**	**Taxa [QPS]**
Não	0,00024	0,00008	8,32	120
Sim	100,00000	16,73715	10,76	92

4.10 Método Proposto

Com base nas análises dos mapas caóticos e suas combinações, a configuração ideal para o algoritmo de criptografia de vídeos para transmissão ao vivo envolve a utilização combinada dos mapas de Baker e Hénon (cf. seção 4.8), juntamente com um terceiro nível de segurança (cf. seção 4.9) sendo que a escala de cores dos quadros do vídeo deve ser no padrão RGB. Além disso, é recomendado a compressão pós-criptografia por meio do codificador H.264 com perfil 4.4.4 e CRF 0 (cf. seção 4.1).

O processo inicial do algoritmo consiste na geração das chaves, onde os parâmetros dos mapas caóticos são adotados como senhas (cf. seção 3.2.2), juntamente com os valores iniciais do terceiro nível de segurança (cf. seção 4.9). Seguido do compartilhamento das senhas entre remetente e destinatário, para isso, é recomendado o uso da criptografia RSA, uma criptografia assimétrica, ideal para esta operação. A partir das senhas é possível a geração das chaves de criptografia, pelo remetente, e descriptografia, pelo destinatário. A geração da chave de confusão, por meio da senha $(t : n_1; n_2; \ldots; n_k)$ do mapa de Baker, resulta na construção de uma imagem da mesma dimensão do quadro original. Se necessário, ajustes devem ser realizados, na dimensão do quadro, para garantir que a imagem seja quadrada. A senha $(a; b; x_0; y_0)$ associada ao mapa de Hénon é usada para gerar a chave de difusão, de mesma dimensão da imagem requerida pelo mapa de Baker, formada por valores pseudoaleatórios. A Figura 4.7 detalha esse processo.

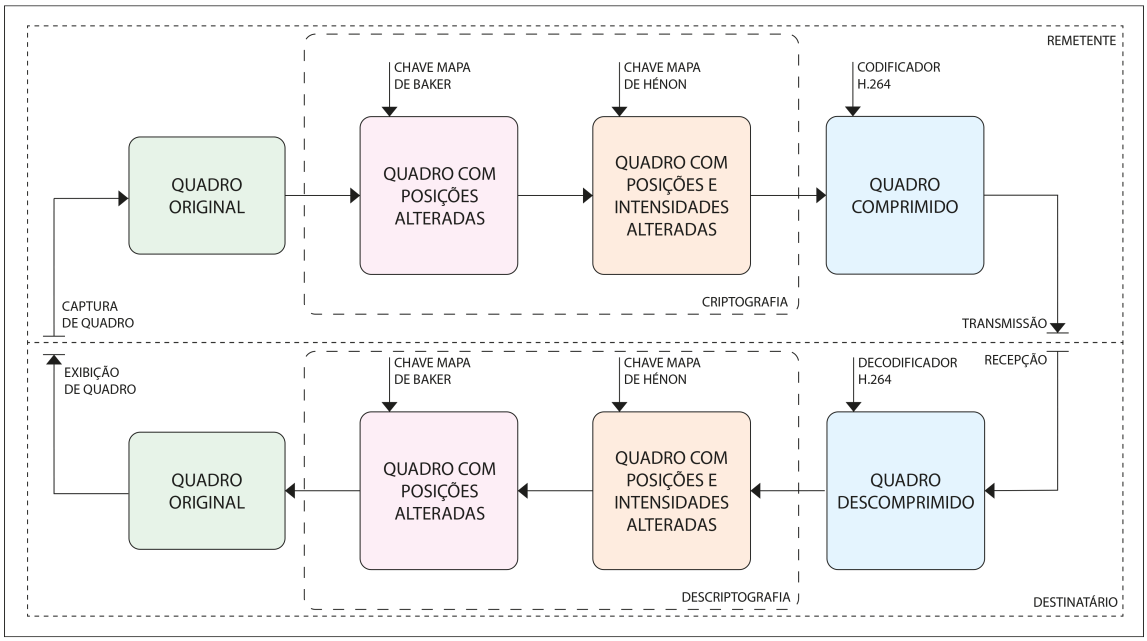
Figura 4.7: Fluxogramas de geração das chaves do método



Para a transmissão ao vivo, o remetente deve capturar o vídeo e em cada um dos quadros ele deve alterar as posições, usando a chave confusão, e as intensidades dos pixels,

usando a chave de difusão acrescido terceiro nível de segurança por meio do processo descrito na seção 4.9. A medida que são criptografados por este método, os quadros são comprimidos através do H.264 e transmitidos ao destinatário. Este, por sua vez, após descomprimir o arquivo recebido, obtém o quadro descriptografado pelo processo inverso ao de criptografia. Conseguindo, deste modo, exibir o vídeo de forma "simultânea" a sua captura, apenas com os atrasos inerentes ao processo. Desta forma, todo o processo é realizado quadro a quadro, por meio do ciclo representado no fluxograma da Figura 4.8.

Figura 4.8: Fluxograma de encriptação do método



4.11 Vantagens e Desvantagens

A fim de categorizar corretamente o trabalho torna-se necessário explorar as vantagens e desvantagens do método, avaliando cuidadosamente os aspectos positivos e negativos do assunto. No contexto do algoritmo de criptografia proposto para transmissões ao vivo, destaca-se as principais vantagens e desvantagens desse método.

Vantagens:

- Segurança avançada – o uso de três níveis de segurança proporciona um algoritmo robusto e seguro, tornando difícil a busca por padrões de reconstrução;
- Confusão – o uso do mapa de Baker proporciona a um terceiro indesejado a dificuldade de reconstrução da imagem original;
- Difusão – o uso do mapa de Hénon para alterar a intensidade dos pixels proporciona

ao algoritmo uma relação muito complexa entre o quadro criptografado e o quadro original;

- Propagação – o terceiro nível de segurança faz com que a alteração de um pixel gere mudanças em todos os pixels;
- Semelhança ao ruído – se a transmissão for interceptada, por um terceiro, ela terá aparência de um ruído;
- Compartilhamento seguro – o uso da criptografia RSA permite um compartilhamento seguro das senhas;
- Eficiência de encriptação – a geração antecipada das chaves e a otimização dos algoritmos permite uma encriptação rápida e segura;
- Eficiência de transmissão – a incorporação da compressão pelo codificador H.264 otimiza a eficiência da transmissão, permitindo uma transmissão mais rápida dos quadros criptografados.

Desvantagens:

- Senhas únicas – a criptografia caótica como um todo é um tipo de criptografia simétrica, isto é, uma vez que interceptada a transmissão não será mais segura;
- Complexidade – a implementação do método proposto envolve uma série de etapas complexas, desde a geração de chaves até a reconstrução do quadro original;
- Processamento adicional – a necessidade de realizar operações XOR e ajustes nos quadros durante a transmissão pode exigir recursos computacionais adicionais;
- Criptografia pré-compressão – o momento da compressão foi escolhido para possibilitar a utilização dos mapas de confusão, o que diminui a eficiência do algoritmo (ABD EL-SAMIE et al., 2013);
- Baixa taxa de compressão – o uso do perfil 4.4.4 e CRF 0, do H.264, gera uma menor taxa de compressão, o que pode gerar atrasos de transmissão devido aos tamanhos dos arquivos a serem enviados.

Capítulo 5

Considerações Finais

Em síntese, este trabalho propõe uma abordagem inovadora para a proteção de transmissões de vídeos ao vivo por meio de um método de criptografia caótica, objetivando o equilíbrio entre segurança e velocidade. Para tal, foi realizada a análise detalhada dos mapas caóticos de Baker, Arnold, logístico e Hénon, revelando a necessidade de combinar estrategicamente mapas que alteram a posição e intensidade dos pixels para garantir maior segurança. A implementação de um terceiro nível de segurança torna o método potencialmente mais seguro e confiável, garantindo que pequenas alterações em um único pixel se propaguem por toda a imagem.

O algoritmo de criptografia desenvolvido usando a combinação dos mapas de Baker e Hénon se destacou nos testes de segurança, ao alcançar 25,55% de desvio de histograma, -0,00201 de coeficiente de correlação linear e 99,63% de difusão por efeito avalanche. Além disso, este algoritmo atingiu uma notável velocidade de encriptação, gastando apenas 10,76ms na cifragem de um quadro, levando-o a encriptar 92 quadros por segundo. A escolha dos mapas caóticos, aliada ao uso estratégico da compressão com o codificador H.264, contribui para uma transmissão eficiente. A validação do método por meio de simulações computacionais e implementação em um ambiente real demonstra a viabilidade e eficácia desse algoritmo.

Entretanto, algumas considerações podem ser feitas em trabalhos futuros, como os testes dos métodos de compressão e otimização de algoritmos. A análise da correlação entre diferentes quadros também se mostra uma oportunidade para desenvolvimento e avaliação. Dessa forma, este trabalho contribui não apenas para o campo da criptografia de transmissões de vídeos ao vivo, mas também oferece perspectivas para pesquisas futuras, explorando diferentes características dos mapas caóticos para enfrentar desafios específicos encontrados em ambientes de transmissões em tempo real. Este trabalho sinaliza um avanço significativo na busca por métodos seguros e eficientes na proteção de dados sensíveis em transmissões de vídeo contemporâneas.

O método de criptografia caótica de vídeos proposto neste trabalho apresenta

potenciais aplicações em diversas áreas que demandam transmissões seguras e eficientes. Contudo, algumas aplicações, como transmissões de videoconferências em redes sociais, transmissões abertas, etc., em geral, não necessitam de tal segurança e complexidade. Algumas das principais aplicações incluem:

- Monitoramento industrial – na utilização de câmeras para monitoramento em ambientes industriais, o método proposto pode ser aplicado para criptografar vídeos provenientes de câmeras de vigilância, garantindo a confidencialidade das informações relacionadas à segurança e operações industriais;
- Transmissões governamentais – em transmissões ao vivo de eventos governamentais, como reuniões, conferências e discursos, a segurança das informações é fundamental, o método pode proteger essas transmissões contra potenciais ameaças de segurança;
- Videomonitoramento de infraestruturas críticas – setores críticos, como energia e transporte, frequentemente utilizam videomonitoramento para garantir a segurança de infraestruturas importantes. A aplicação do método proposto oferece uma camada adicional de proteção, visto que esses dados podem ser utilizados para eventuais danos à sociedade;
- Aplicações militares – em contextos militares, onde a segurança é de extrema importância, a criptografia caótica de vídeos pode ser implementada em transmissões ao vivo para a proteção das informações sensíveis;
- Transmissões geoespaciais – em transmissões de vídeos geoespaciais, como aquelas relacionadas a imagens de satélite e monitoramento ambiental, a segurança dos dados é crucial, visto que essas são informações estratégicas para os países.

Referências

ABD EL-SAMIE, Fathi E. et al. **Image encryption: A communication perspective**. CRC Press, 2013. Publisher Copyright: © 2014 by Taylor & Francis Group, LLC. ISBN 9781466576988. DOI: https://doi.org/10.1201/b16309.

BONFIM, Daniele Helena. **Criptografia RSA**. 2017. Diss. (Mestrado) – Universidade de São Paulo - São Carlos.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Edição: IMPA. 2. ed., 2005. P. 226.

DAO, Nhu-Ngoc et al. A Contemporary Survey on Live Video Streaming from a Computation-Driven Perspective. **ACM Computing Surveys**, v. 54, fev. 2022. DOI: 10.1145/3519552.

FFMPEG. **H.264 Video Encoding Guide**. 10 jun. 2023. Disponível em: <www.trac.ffmpeg.org/wiki/Encode/H.264>. Acesso em: 9 set. 2023.

GONZALES, Rafael C.; WOODS, Richard E. **Processamento Digital de Imagens**. Edição: Pearson. 3. ed., 2009. P. 644.

HUANG, Xin et al. A Chaotic-based Encryption/Decryption System for Secure Video Transmission. In: 2021 IEEE International Conference on Electro Information Technology (EIT). Mai. 2021. P. 369–373. DOI: 10.1109/EIT51626.2021.9491868.

AL-KHASAWNEH, Mahmoud Ahmad; ABU-ULBEH, Waheeb.; KHASAWNEH, Ahmad M. Satellite images encryption Review. In: 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI). Dez. 2020. P. 121–125. DOI: 10.1109/ICHCI51889.2020.00034.

KOCAREV, Ljupco; LIAN, Shiguo. **Chaos-Based Cryptography**: Theory, Algorithms and Applications. Edição: Springer. 1. ed., 2011. P. 395.

KUMAR, Chandan; SINGH, Shailendra. Asymmetric Encryption of Surveillance Videos for Adaptive Threshold based Moving Object Detection. In: 2021 IEEE 8th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). Nov. 2021. P. 1–6. DOI: 10.1109/UPCON52273.2021.9667591.

MALLADAR, Rohit S; KUNTE, R. Sanjeev. Selective Video Encryption using Chaos for H.264 Videos Applicable to Video on Demand(VoD). In: 2020 5th International Conference on Communication and Electronics Systems (ICCES). Jun. 2020. P. 215–220. DOI: 10.1109/ICCES48766.2020.9137861.

MATTIOLI, Leandro Resende. **2D–3D Spatial Registration for Remote Inspection ofPower Substations**. 2021. Tese (Doutorado) – Universidade Federal de Uberlândia.

MICROSOFT. **Great Expectations: Making Hybrid Work Work**. 16 mar. 2022. Disponível em: <https://www.microsoft.com/en-us/worklab/work-trend-index/great-expectations-making-hybrid-work-work>. Acesso em: 13 abr. 2023.

MORETTIN, Pedro A.; BUSSAB, Wilton O. **Estatística Básica**. Edição: Saraiva. 6. ed., 2010. P. 540.

EL-MOWAFY, M. A. et al. Chaos Based Encryption Technique for Compressed H264/AVC Videos. **IEEE Access**, v. 10, p. 124002–124016, 2022. ISSN 2169-3536. DOI: 10.1109/ACCESS.2022.3223355.

NEMCIC, O.; VRANJES, M.; RIMAC-DRLJE, S. Comparison of H.264/AVC and MPEG-4 part 2 coded video. In: ELMAR. 2007. P. 41–44. DOI: 10.1109/ELMAR.2007.4418796.

QIAN, Qinchun; CHEN, Zengqiang; YUAN, Zhuzhi. Video Compression and Encryption Based-On Multiple Chaotic System. In: 2008 3rd International Conference on Innovative Computing Information and Control. 2008. P. 561–561. DOI: 10.1109/ICICIC.2008.597.

RANJITH KUMAR, R. et al. A New One Round Video Encryption Scheme Based on 1D Chaotic Maps. In: 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). Mar. 2019. P. 439–444. DOI: 10.1109/ICACCS.2019.8728443.

RICHARDSON, Ian E. **The H.264 and MPEG-4 - Video Compression**. Edição: Wiley. 1. ed., 2003. P. 281.

SALAMA, Wessam M.; ALY, Moustafa H. Chaotic Maps Based Video Encryption: A New Approach. In: 2021 31st International Conference on Computer Theory and Applications (ICCTA). Dez. 2021. P. 18–25. DOI: 10.1109/ICCTA54562.2021.9916605.

SRINIVASAN, Suman et al. Airborne traffic surveillance systems. ACM, out. 2004. DOI: 10.1145/1026799.1026821.

STOLFI, Guido. **Compressão de Imagens em Movimento: Padrão MPEG, H.264, DIRAC**: PTC3547 - CODIFICAÇÃO E TRANSMISSÃO MULTIMÍDIA. Mai. 2018. Disponível em: <https://www.lcs.poli.usp.br/~gstolfi/PPT/APTV0718.pdf>. Acesso em: 13 set. 2023.

TECHBLOG.GR. **Sony Ericsson Satio 640x480 video sample**. 2010. Disponível em: <www.youtube.com/watch?v=OnFwWgA4uzM>. Acesso em: 9 set. 2023.

VALDEVINO, André. **Criptografia Caótica**. 2006. – Universidade Católica de Brasília.

YI, Xiuqing; TIAN, Miao; CHEN, Cheng. Power System Video Encryption Scheme Based on Chaotic System. In: 2021 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). Jul. 2021. P. 771–776. DOI: 10.1109/ICPSAsia52756.2021.9621413.

ZHANG, Qiao-jia et al. An efficient selective encryption scheme for HEVC based on hyperchaotic Lorenz system. In: 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). Mar. 2021. P. 683–690. DOI: 10.1109/IAEAC50856.2021.9390925.

Índice Remissivo

MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS
SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E CONTRATOS

FOLHA DE ASSINATURAS

Emitido em 15/12/2023

CÓPIA DO TRABALHO Nº 224/2023 - DELMAX (11.57.05)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 15/12/2023 15:19)
CIRILO GONCALVES JUNIOR
PROFESSOR ENS BASICO TECN TECNOLOGICO
DFGAX (11.57.03)
Matrícula: ###358#2

(Assinado digitalmente em 15/12/2023 15:14)
Rafael Rodrigues Silva
DISCENTE
Matrícula: 2019######1

Visualize o documento original em https://sig.cefetmg.br/documentos/ informando seu número: **224**, ano: **2023**, tipo: **CÓPIA DO TRABALHO**, data de emissão: **15/12/2023** e o código de verificação: **634c00234b**