UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA DO CABO DE SANTO AGOSTINHO
BACHARELADO EM ENGENHARIA ELETRÔNICA

THALYTA DE SOUSA SILVA MENDONÇA

Um estudo sobre ocultação de dados para imagens digitais

Cabo de Santo Agostinho - PE
2023

THALYTA DE SOUSA SILVA MENDONÇA

Um estudo sobre ocultação de dados para imagens digitais

Monografia apresentada ao Curso de Graduação em Engenharia Eletrônica da Unidade Acadêmica do Cabo de Santo Agostinho da Universidade Federal Rural de Pernambuco para obtenção do grau de bacharel em Engenharia Eletrônica.

Orientador: Prof. Dr. Felipe Alberto Barbosa Simão Ferreira

Cabo de Santo Agostinho - PE

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

M539e Mendonça, Thalyta de Sousa Silva
Um estudo sobre ocultação de dados para imagens digitais / Thalyta de Sousa Silva Mendonça. - 2023.
50 f. : il.

Orientador: Felipe Alberto Barbosa Simao Ferreira.
Inclui referências e anexo(s).

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal Rural de Pernambuco, Bacharelado em Engenharia Eletrônica, Cabo de Santo Agostinho, 2023.

1. criptografia. 2. esteganografia. 3. segurança. 4. marca d’água digital. I. Ferreira, Felipe Alberto Barbosa Simao, orient. II. Título

CDD 621.3

THALYTA DE SOUSA SILVA MENDONÇA

Um estudo sobre ocultação de dados para imagens digitais

Monografia apresentada ao Curso de Graduação em Engenharia Eletrônica da Unidade Acadêmica do Cabo de Santo Agostinho da Universidade Federal Rural de Pernambuco para obtenção do grau de bacharel em Engenharia Eletrônica.

Aprovada em: 26 de Abril de 2023

Banca Examinadora

Prof. Dr. Felipe Alberto Barbosa Simão Ferreira
Universidade Federal Rural de Pernambuco

Prof. Dr. Marcel Ayres de Araújo
Universidade Federal Rural de Pernambuco

Profa. Dra.Amanda Souza de Paula
Universidade Federal Rural de Pernambuco

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me sustentado e me ajudado a chegar até aqui.
À minha família, meus pais Arly Rodrigues e Josineide de Sousa, por todo suporte emocional e financeiro durante o período universitário e aos meus irmãos Thomaz Filipe e Priscila Sousa, por compartilharem a jornada de engenharia e serem apoio em momentos difíceis, especialmente os de prova.
Ao meu esposo Sérgio Mendonça por todo amor e compreensão durante este processo, obrigada por estar segurando minha mão e me incentivando em toda esta caminhada.
Ao professor Dr. Felipe Barbosa por ter me orientado ao longo desse TCC.
À minha equipe de trabalho pelo apoio durante este projeto e toda jornada acadêmica. Aos meus amigos que me ajudaram e compreenderam minha ausência nesse período.

"*Não fui eu que ordenei a você? Seja forte e corajoso! Não se apavore nem desanime, pois o Senhor, o seu Deus, estará com você por onde você andar.*"

(*Josué 1:9*)

RESUMO

A segurança digital é um campo de estudo em expansão em diversas áreas da ciência, que inclui a esteganografia - a arte de escrever de forma oculta - como uma das novas áreas de pesquisa. Neste trabalho de conclusão de curso, é apresentada a implementação de uma técnica esteganográfica LSB (*Least Significant Bit*) para inserir mensagens de texto em arquivos de imagem. O estudo é fundamentado em pesquisas bibliográficas sobre as técnicas de ocultação de dados em imagens digitais e a importância da utilização de marca d'água como medida de proteção contra a pirataria e a falsificação de imagens. O trabalho apresenta os conceitos teóricos envolvidos na técnica LSB, bem como os métodos e ferramentas utilizadas para a inserção da marca d'água digital. Os resultados obtidos a partir de testes realizados comprovam a eficácia da técnica LSB na inserção de marca d'água digital em imagens digitais de forma segura e eficiente.

Palavras-chave: criptografia; esteganografia; segurança; marca d'água digital.

ABSTRACT

Digital security is a growing field of study in various areas of science, which includes steganography - the art of writing in a hidden manner - as one of the new research areas. This undergraduate thesis presents the implementation of a *Least Significant Bit* (LSB) steganographic technique to embed text messages in image files. The study is based on literature research on data hiding techniques in digital images and the importance of using watermarking as a measure of protection against piracy and image forgery. The paper presents the theoretical concepts involved in the LSB technique, as well as the methods and tools used for the insertion of the digital watermark. The results obtained from tests conducted prove the effectiveness of the LSB technique in securely and efficiently embedding digital watermarks in digital images.

Keywords: cryptography; steganography; security; digital watermark.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ASCII	*American Standard Code for Information Interchange*
BPCS	*Bit-Plane Complexity Segmentation*
CIA	*Confidentiality, Integrity and Availability*
DCT	*Discrete Cosine Transform*
DFT	*Discrete Fourier Transform*
DTFT	*Discrete-time Fourier transform*
DWT	*Discrete Wavelet Transform*
GIF	*Graphics Interchange Format*
IDCT	*Inverse Discrete Cosine Transform*
ISB	*Intermediate Significant Bit*
JPEG	*Joint Photographic Experts Group*
LSB	*Least Significant Bit*
MSB	*Most Significant Bit*
PNG	*Portable Network Graphics*
RGB	*Red, Green and Blue*
SSIM	*Structural Similarity Index*
SVD	*Singular Value Decomposition*

SUMÁRIO

1 INTRODUÇÃO

Com o sucessivo avanço dos meios digitais como meio de armazenamento de informações, cada vez é mais habitual a disponibilização de dados sigilosos apenas em formato digital. Por isso, tornou-se significativo o estudo de como garantir a segurança, os direitos autorais e a autenticidade de informações digitais. Dentre as possíveis técnicas para proteção de direitos autorais e autenticação de dados digitais, as marcas d'água digitais têm conquistado atenção especial. A utilização de marca d'água permite estabelecer um método de comunicação, em que a marca d'água é a mensagem, e o produto assinado é a via de transmissão. Isso constitui um dos princípios da esteganografia, que pode ser vista como um caso particular das marcas d'água.

A esteganografia faz uso de técnicas para que a mensagem sigilosa seja oculta em outro dado a fim de encobrir seu verdadeiro significado. Grande parte das técnicas atualmente utilizadas na área de marcas d'água faz uso de transformadas para extração e inserção da marca. Dentre as mais utilizadas destaca-se a Transformada Discreta do Cosseno (ou DCT da sigla em inglês para *Discrete Cosine Transform*), muito utilizada em processamento de imagens, principalmente no contexto de compressão. Outra possibilidade é realizar a inserção da marca d'água ou da mensagem diretamente no domínio espacial obtendo diferentes características acerca de robustez e imperceptibilidade com relação à alternativas no domínio da transformada.

Além da marca d'água digital e da esteganografia, a criptografia é outra técnica amplamente utilizada para proteção de dados em formato digital. A criptografia permite a proteção e armazenamento de dados ao consistir em transformar o texto original em um texto cifrado, ininteligível para quem não possua a chave de descriptografia. A marca d'água e a esteganografia são utilizadas para autenticação de dados e identificação de autoria, e podem ser complementares à criptografia em termos de segurança de informação.

Assim, o presente trabalho visa fazer uma pesquisa bibliográfica sobre técnicas de ocultação de dados em imagens baseada na transformada discreta do cosseno e no domínio espacial para aplicações de esteganografia e marca d'água digital.

1.1 Objetivos

O objetivo principal deste trabalho é realizar um estudo sobre os principais conceitos e técnicas de ocultação de dados para imagens digitais no contexto de segurança de informação.

1.1.1 Objetivos Específicos

- Estudar a fundamentação teórica da área de ocultação de dados, englobando conceitos dos dois objetos principais de estudo desse trabalho, esteganografia e marca d'água digital;
- Implementar e avaliar uma técnica de esteganografia;
- Implementar e avaliar uma técnica de marca d'água digital;
- Analisar e apresentar os resultados obtidos.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem como finalidade apresentar as definições iniciais sobre criptografia, esteganografia e imagem digital, bem como alguns conceitos históricos sobre os conteúdos discutidos a fim de conhecer as origens de tais técnicas.

2.1 Criptografia

A criptografia, termo que origina-se do grego *cryptos*, que significa secreto ou oculto, analisa os meios para codificar mensagens, permitindo que apenas o remetente e o destinatário consigam traduzir o conteúdo do texto. Existem várias técnicas, uma delas é a assinatura digital, resultado de um processo de criptografia assimétrica, no qual se utilizam algoritmos de chave pública para cifrar uma mensagem. O processo envolve a cifragem da mensagem com a chave pública e a "decifragem"com a chave privada, ou vice-versa, resultando na recuperação da mensagem original. Um exemplo simples de assinatura digital é o criptograma, que é gerado ao cifrar um determinado bloco de dados usando a chave privada da pessoa que assina, em um algoritmo assimétrico. A verificação da assinatura é realizada ao "decifrar"o criptograma com a chave pública correspondente e, se o resultado for satisfatório, a assinatura é considerada autêntica (SILVA, 2014).

Para Stallings (2015) há três objetivos que se almejam obter com segurança, constituindo a trindade para *Confidentiality, Integrity and Availability* (*CIA*) da sigla em inglês:

- **Confidencialidade (dados e usuários)**: que se certifica que informações privadas e sigilosas não estejam à disposição de pessoas não permitidas.
- **Integridade**: compreende-se que os dados precisem ser empregados apenas por pessoas permitidas, bem como o uso dos métodos seja independente de manipulações.
- **Disponibilidade**: os processos precisam atuar de maneira que os serviços estejam sempre disponíveis para os usuários autorizados.

Serviços de segurança são proporcionados por camadas do protocolo de comunicação entre sistemas, que atestam a transferência apropriada dos dados, considerando a segurança e a intangibilidade dos dados. Os serviços, que são orientações de segurança efetuadas pelas técnicas de segurança, são separados em cinco conforme determinado por Stallings (2015):

- **Autenticação**: verifica a autenticidade da comunicação, isto é, assegura ao destinatário que a mensagem tem a procedência de que declara ter vindo. Também necessita certificar que a conexão não passe por interferência, de maneira que um mediador não finja ser uma das partes, para transmitir ou receber de forma não autorizada.

- **Controle de Acesso**: refere-se à competência de controlar o acesso ao sistema através de normas e garantias de acesso.

- **Confidencialidade dos dados**: proteção das informações contra ataques.

- **Integridade dos dados**: assegura que as mensagens sejam recebidas da mesma maneira que foram enviadas, sem repetição, inserção, mudança ou reorganização. Portanto, sendo via ataques ou erros na aplicação, a mensagem enviada precisa ser a mesma no momento da entrada.

- **Irretratabilidade**: Impossibilita a negação da recepção ou emissão de uma nova mensagem a ser transmitida.

2.2 Imagem Digital e Modelo de Cores RGB

Imagens digitais são retratadas por matrizes de tamanho determinado, onde cada elemento dessas matrizes registra um valor de cor que constitui um *pixel* da imagem por meio do modelo *RGB* (*Red, Green, Blue*)(ROCHA, 2010). Para a aplicação da esteganografia em imagens digitais, é necessária a manipulação desses *pixels* e valores de cor. No sistema RGB, as outras cores são decorrentes da arranjo das cores vermelho, verde e azul, vide Figura 1. No contexto de codificação digital, as cores são retratadas por números. Cada uma das três cores que integram o sistema RGB são simbolizadas por números que vão de 0 ao 255. (HONDA, 2011).

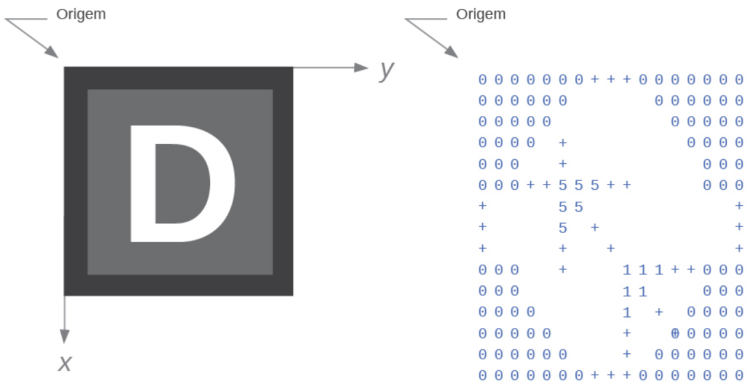
Figura 1 – Cores primárias Vermelho, Verde e Azul (Modelo RGB)

Fonte: ROCHA, 2010.

2.2.1 Representação de imagens digitais

Considerando que uma imagem seja adquirida por intermédio de um sensor matricial, e em seguida, sejam executadas as funções de amostragem e quantização, procedimentos para a digitalização da imagem. É possível definir uma matriz 2D, f(x, y) formada por M linhas e N colunas, em que (x, y) são coordenadas discretas. A origem da imagem é definida por f(0, 0), e o valor subsequente na mesma linha é f(0, 1) (SCHENATTO, 2021). A Figura 2 exibe duas maneiras usuais para reproduzir uma imagem digitalmente, sendo que a primeira delas apresenta como a imagem seria exibida em uma tela, com o nível de cinza correspondente ao valor da função f para cada ponto, variando de 0 para preto até 255 para branco e com níveis intermediários apresentados.

Figura 2 – Representações gráficas de imagem



Fonte: SCHENATTO, 2021.

À vista disso, há somente três valores de intensidade, desse modo cada ponto dispõe o

valor 0, 0.5 ou 1, os quais estão normalizados entre 0 e 1, embora o padrão seja a representação entre 0 e 255 para uma imagem codificada a 8 bits por *pixel*. Assim, quando o computador converte os valores, são apresentadas as cores preto, cinza e branco nesta ordem. A segunda imagem mostra valores numéricos para f(x,y). Essa representação mostra-se significativa para o progresso de algoritmos de processamento de imagens, porque é mediante a variação dos valores da matriz, que se realizam as transformações relevantes para cada situação. No formato de equação, demonstra-se uma matriz numérica M × N como se mostra a seguir (GONZALEZ; WOODS, 2000).

$$\text{f(x,y)} = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix}$$

Para reproduzir uma imagem digital, a matriz correspondente é preenchida em ambos os lados, sendo que o lado direito apresenta os *pixels* da imagem representados por números inteiros entre 0 e 255 (GONZALEZ; WOODS, 2000).

2.3 **Esteganografia**

A esteganografia, técnica de comunicação baseada em técnicas de ocultação, tem registros de uso desde a Idade do Ouro na Grécia, quando se utilizava placas de madeira cobertas com cera como transportadoras para ocultar mensagens. A cera das placas de madeira era derretida e grafada uma mensagem na madeira, e em seguida se passava uma nova camada de cera e era escrito algo insignificante na cera, dessa forma a mensagem relevante ficava escondida (LI *et al.*, 2011). Partindo do mesmo princípio de mascarar dados, no momento atual, a esteganografia é executada digitalmente camuflando dados em outros dados que à primeira vista são insignificantes. Ao passo que na criptografia a presença da comunicação pode ser de fácil detecção, a esteganografia tem o intuito de ocultar para que a comunicação não seja notada (ARTZ, 2001).

2.4 **Critérios para Sistemas Esteganográficos**

Alguns critérios são relevantes e devem existir em qualquer sistema esteganográfico, dentre eles destacam-se:

- **segurança**: o material oculto tem que ser imperceptível tanto visivelmente quanto por métodos estatísticos, com o intuito de não provocar desconfiança, ao passo que tenta gerar uma proteção contra um algoritmo de descoberta. Embora certos conceitos para um sistema protegido ideal exijam conhecimento preciso e recursos computacionais ilimitados, essas circunstâncias não são geralmente aplicáveis para propósitos esteganográficos concretos. Em termos práticos, um processo pode ser visto como seguro, ou esteganograficamente eficaz, se não for viável encontrar a presença de stego-conteúdo utilizando qualquer meio acessível (JULIO *et al.*, 2007);

- **carga útil**: de modo diferente da marca d'água, que necessita embutir apenas uma quantidade reduzida de informações de direitos autorais, a esteganografia é dirigida à comunicação oculta e por isso comumente exige capacidade de inclusão satisfatória. Os critérios para capacidade considerável de dados e segurança são constantemente discordantes (JULIO *et al.*, 2007);

- **robustez**: apesar de robustez contra ataques não ser uma preferência significativa, tal como em marcas d'água, possuir a capacidade de suportar a compressão é decerto almejado, visto que a maior parte das imagens JPEG (*Joint Photographic Experts Group*) coloridas são condensadas antes de serem disponibilizadas on-line (JULIO *et al.*, 2007).

2.5 Técnicas Esteganográficas

O presente trabalho será enfatizado em técnicas apontadas para esteganografia em imagens digitais, havendo várias maneiras distintas de possibilitar o emprego da esteganografia por meios digitais, e em variadas formas de arquivos, como por exemplo imagens, áudio, vídeo, documentos de texto e outros.

Como visto na seção 2.2, as imagens são mídias muito comuns para aplicação de esteganografia, e podem ser manipulados variados formatos tais como JPEG (*Joint Photographic Experts Group*), GIF (*Graphics Interchange Format*) e PNG (*Portable Network Graphics*). A introdução de dados na imagem, é feita no domínio da frequência ou no domínio espacial (FERREIRA, 2020). As mídias digitais, como fotografias, geralmente apresentam quantidades expressivas de ruído gerado durante a conversão de uma cena existente para o meio digital, tornando possível a ocultação de dados no ruído.

2.5.1 Técnicas de inserção no bit menos significativo

Estas técnicas são fundamentadas na alteração dos bits menos significativos (*Least Significant Bit*) dos valores de *pixel* no domínio espacial. Em uma aplicação trivial, estes *pixels* representam o plano LSB inteiro com o stego-dados (JULIO *et.al.*, 2007).

Técnicas apoiadas em LSB podem ser empregues a cada *pixel* de uma imagem codificada em 32 bits por *pixel*, por exemplo. Estas imagens possuem seus *pixels* codificados em quatro *bytes*. Um para o canal alfa (*alpha transparency*), outro para o vermelho (*red*), outro para o verde (*green*) e outro para o azul (*blue*). Efetivamente, é possível eleger um bit (o menos significativo) em cada *byte* do *pixel* para retratando o bit a ser ocultado sem gerar modificações visíveis na imagem. Tais técnicas compõem o modo de ocultação em imagens mais dificultosas de serem identificadas pois podem introduzir informações em *pixels* não sequenciais, fazendo complicada a percepção (WAYNER, 2009).

2.5.2 Técnicas baseadas em Transformadas

Uma das grandes falhas do *LSB* é a compressão, que pode gerar perda dos dados escondidos, enquanto os algoritmos de transformação, como a transformada discreta de *Fourier*, a transformada discreta do cosseno, a transformada *wavelet* discreta, a transformada *wavelet* inteira e a transformada *curvelet* discreta, podem ser considerados mais eficazes nesse ponto. Nesses métodos, os dados são escondidos no domínio de transformação e são lançados por toda a imagem, favorecendo proteção mais eficiente contra processamento de sinal (SCHENATTO, 2021).

- **Transformada Discreta do Cosseno**

  Uma técnica difundida usada para ocultar dados no domínio da frequência, é a modulação do tamanho relativo de dois ou mais coeficientes *Discrete Cosine Transform* (*DCT*) em um bloco de imagem.

  Na metodologia proposta por (COX *et al.*, 1997), a inserção de uma marca d'água W ocorre inicialmente transformando a imagem original H do domínio espacial para o domínio de frequência por meio da DCT. A marca d'água W é então incorporada em alguns dos componentes mais relevantes da imagem transformada. Ao aplicar a transformada discreta inversa do cosseno *(IDCT - Inverse Discrete Cosine Transform)*, obtém-se a imagem marcada HW. A marca W, originalmente inserida em componentes específicos no domínio

de frequência, é agora dispersa por toda a imagem no domínio espacial durante esse processo. Para recuperar a marca d'água extraída WEX, é necessário realizar o processo inverso.

- **Transformada Discreta de Fourier**

  Esta técnica utiliza o dado extraído da *Discrete Fourier Transform* (*DFT*) para escolher os *pixels* da imagem que receberão os dados confidenciais. Neste trabalho, desenvolvemos um sistema esteganográfico para imagens coloridas usando a transformada discreta de *Fourier*. Assim, calcula-se inicialmente o comprimento da mensagem secreta, a qual é convertida para o formato ASCII. Em seguida, a imagem de cobertura do domínio espacial é transformada para o domínio de frequência usando a *DFT*, utilizando a equação apropriada para a transformada discreta de *Fourier* bidimensional. As transformadas de *Fourier* são complexas, com partes real e imaginária, dessa forma as informações secretas são incorporadas apenas nas partes reais da transformada de *Fourier*. Após a inserção das informações secretas, é aplicada a *DFT* inversa, utilizando a equação inversa da transformada discreta de *Fourier*, para obter a imagem esteganográfica. Novamente, no processo de extração da mensagem secreta, a DFT inversa é aplicada à imagem esteganográfica, assim determina-se o comprimento da mensagem e é feita a extração dos coeficientes reais da representação *DFT* até o comprimento da mensagem (HEMACHANDRAN, 2013).

- **Transformada Wavelet Discreta**

  Esta técnica também denominada como *DWT*, do inglês *Discrete Wavelet Transform*, propicia o armazenamento das informações sigilosas mediante o resultado da decomposição *wavelet* da imagem a ser marcada por meio da DWT bidimensional até um certo nível, k. Durante essa decomposição, os coeficientes *wavelet* são obtidos e organizados em sub-bandas de frequências altas e baixas. As faixas de frequência obtidas ao decompor uma imagem através da transformada *wavelet* bidimensional apresentam as seguintes características:

  a) À medida que a escala da faixa de frequência diminui, sua energia diminui e sua resolução em frequência aumenta;

  b) Os coeficientes *wavelets* são mais significativos nas faixas de frequência com menor energia;

  c) A importância visual de um coeficiente *wavelet* aumenta com o aumento de seu valor.

Para remover a marca d'água, aplica-se a *Transformada Wavelet Discreta* bidimensional de nível k na imagem marcada, resultando nos coeficientes *wavelets*. A extração da marca d'água ocorre a partir dos coeficientes *wavelets* encontrados na sub-banda LLk, utilizando um algoritmo específico. A necessidade da imagem original depende do algoritmo empregado durante a inserção da marca d'água (SILVA, 2014).

2.5.3 Técnicas de *Bit-Plane Complexity Segmentation*

O *Bit-Plane Complexity Segmentation* (BPCS) fundamenta-se no caráter da visão humana, no qual uma pessoa não consegue identificar vestígios de informações em um modelo binário confuso, o que constitui atributo de ruído. O propósito seria fragmentar uma imagem, em regiões com e sem ruídos, a fim de mascarar as informações nas regiões que têm ruído. Assim é dificultoso encontrar as mensagens ocultas, já que as regiões complexas da imagem foram modificadas por modelos binários imperceptíveis ao olho humano. Uma região complexa se define como um bloco que possui maior diversidade de informações visuais, e uma localização de dificuldade reduzida com menor diversidade de informações, como, um céu azul limpo que possua apenas a cor azul (KAWAGUCHI; EASON, 1998).

Uma figura com valores variados (P) significando *pixels* de n bits pode ser decomposta em um grupo de imagens binárias n (SUN, 2015). Assim, se a imagem é uma imagem cinza de n bits, ela é exibida como

$$P = (P_1, P_2, ..., P_n) \tag{2.1}$$

e se a imagem for retratada no modelo *RGB*, ela pode ser determinada por

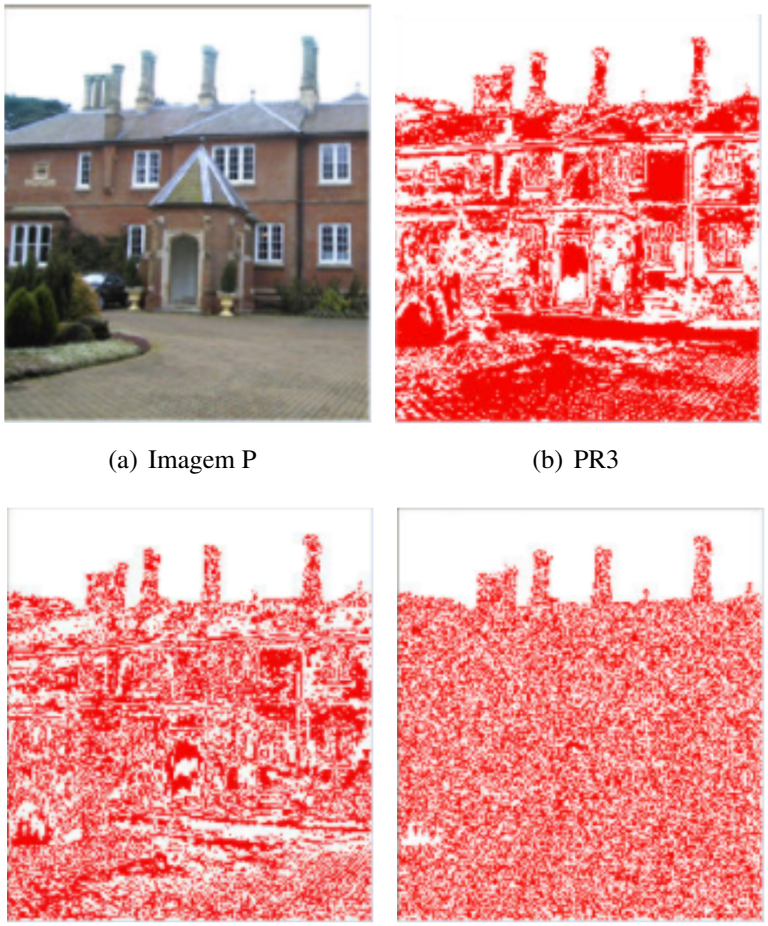
$$P = (PR_1, PR_2, .., PR_n, PG_1, PG_2, .., PG_n, PB_1, PB_2, .., PB_n) \tag{2.2}$$

em que PR_1, PG_1, PB_1 são os planos de bits mais significativos (*MSB*), à medida que PR_n, PG_n, PB_n são os bits menos significativos (*LSB*) (KAWAGUCHI; EASON, 1998).

Os dados da imagem são descritos em número por uma técnica de código binário legítimo. Quanto às camadas de bits de uma imagem, a complexidade de cada camada de bits aumenta do *MSB* (P_1) para o *LSB* (P_n). Eventualmente, a maior parte das camadas *LSB* parecem estar em um modelo casual de bits. A Figura 3 ilustra os planos de bits PR3, PR4 e PR6 de uma imagem colorida P de 24 bits.

Os processos usuais de esteganografia possuem uma capacidade reduzida de ocultação de dados, permitindo a ocultação de apenas 5% a 15% das informações do arquivo operado como máscara. O *BPCS* se difere das técnicas comuns uma vez que tem uma capacidade notável de incorporação, chegando em muitos casos a 50% de proveito na hipótese de uma imagem de 24 bits (SCHENATTO, 2021).

Figura 3 – Camadas de bits.



(a) Imagem P (b) PR3

(c) PR4 (d) PR6

Fonte: KAWAGUCHI; EASON, 1998.

2.5.4 Técnicas de Espalhamento de Espectro

Nesse tipo de técnica, as informações ocultadas são distribuídas ao longo da imagem de cobertura, e uma estego-chave é utilizada para detectar de maneira aleatória os canais de frequência. Os dados que fazem parte da imagem de cobertura são observados como interferência em um *framework* de comunicação. Em conformidade com Julio (2007) "os dados embutidos são primeiramente modulados com pseudo ruídos e então a energia é espalhada sobre uma faixa de frequência larga, alcançando somente um nível muito baixo de força de inclusão".

2.5.5 Técnicas de Filtragem e Mascaramento

As técnicas de esteganografia embasadas em filtragem e mascaramento elaboram estego-imagens mais robustas e resistentes a compressão e recorte em comparação com o bit menos significativo, entretanto, são mais propensas a percepção (WAYNER, 2009). De maneira oposta a técnica de inserção no canal *LSB*, as técnicas de filtragem e mascaramento atuam com alterações nos bits mais significativos das imagens. As imagens de cobertura têm de ser em tons de cinza dado que estas técnicas não são eficientes em imagens coloridas. Isto dá-se pelo motivo de que mudanças em bits mais significativos de imagens em cores produzem muitos artefatos tornando os dados mais propícios de serem detectados.

Tais técnicas são similares a marca d'água visível em que valores de *pixel* em áreas mascaradas são expandidos ou reduzidos em um dado percentual (JULIO *et al.*, 2007).

2.6 **Marca D'água**

O intenso aumento dos sistemas de multimídia interligados pela rede de computadores nos recentes anos mostra um desafio considerável nos cenários como propriedade, integridade e autenticação dos dados digitais (áudio, vídeo e imagens estáticas). Para encarar a provocação de garantir a autenticidade e a integridade de informações em meios digitais, foi estabelecida a ideia de marca d'água digital, que consiste em um sinal transportador de informação, visualmente imperceptível e oculto em uma imagem digital, denominada imagem hospedeira ou imagem marcada. Ainda que algumas técnicas de marca d'água sejam empregues exatamente em tipos distintos de dados digitais, as mídias mais usadas são as imagens estáticas (JULIO *et al.*, 2007). Conclui-se que a marca d'água é uma maneira acessível, no entanto eficaz para segurança contra cópias dolosas de documentos.

Na Figura 4 se visualiza um exemplo de marca d'água empregue em uma cédula, na qual a imagem de um mico leão dourado é inserida como marca d'água ao lado esquerdo da nota e pode ser observada ao posicionar a nota contra a luz.

Figura 4 – Nota de 20 reais.

Fonte: LOPES, 2006.

2.6.1 Marca D'água Digital

O principal intuito da marca d'água digital é introduzir dados (ostensivo, discreto ou oculto, de acordo com a aplicação) na documentação digital a fim de oferecer algum serviço de segurança ou apenas classificá-lo. Vários sistemas possibilitam a recuperação do dado inserido no documento, ou seja, a marca d'água, ainda que ele tenha sido notadamente alterado por ataques, sejam eles maldosos ou não. Em geral, todas as marcas d'águas digitais têm pontos compartilhados: têm um sistema de inserção e um sistema de recuperação. Além disso, a marca d'água pode ser de qualquer gênero, como números, texto ou imagem, e geralmente é composta por um *string* binário.

A chave pode ser empregada de maneira a evidenciar segurança, impedir que alguém não permitido reabilite e/ou modifique a marca d'água. Na verdade, todo processo que utiliza marca d'água para fins comerciais aplica no mínimo uma chave ou ainda a fusão de várias chaves (NUNES, 2008).

2.6.2 Tipos de Marca D'água Digital

As técnicas de marca d'água digital se classificam conforme os tipos dos dados a serem inseridos (BERGHEL, 1997), as quais são categorizadas como:

- Marca d'água para texto;
- Marca d'água para imagens;
- Marca d'água para áudio;
- Marca d'água para vídeo.

Neste trabalho serão estudadas técnicas de marca d'água aplicada a imagens que se dividem em marca d'água visível, invisível robusta, invisível frágil e invisível semi-frágil, a serem apresentadas nas próximas seções (LOPES, 2006). As técnicas para elaborar tais tipos de marca d'água podem ser descritas no domínio espacial ou domínio da frequência.

- Domínio Espacial: a marca d'água *W* é inserida diretamente na imagem *H*, alterando os valores dos *pixels* da imagem para incluir a marca.
- Domínio da Frequência: a marca *W* é inserida na imagem ao modificar os coeficientes espectrais obtidos a partir das transformações em frequência. As transformações mais comumente utilizadas incluem a Transformada Discreta do Cosseno (*DCT*), a Transformada Discreta *Wavelets* (*DWT*) e a Transformada Discreta de *Fourier* (*Discrete Fourier Transform - DFT*) (LOPES, 2006).

2.6.3 Marca d'água visível

Marca d'água visível, como o próprio nome sugere, é um padrão visual, que é introduzido em um vídeo ou imagem. Este tipo de marca d'água é pouco utilizado, devido a sua sensibilidade a ataques, por se saber a posição exata dela. Sendo assim um invasor pode remover a marca, por meio de um fácil recorte. Habitualmente estes métodos são como logotipos, funcionando como um sinal de indicação para mostrar que a mídia digital é de dado possuinte (LOPES *et al.*, 2004).

As marcas d'águas digitais visíveis são utilizadas sobretudo em imagens divulgadas, pela televisão ou internet por exemplo, visando inibir o uso comercial inadequado. Este tipo de marca d'água é comumente utilizado por emissoras de televisão ao introduzirem os logotipos à suas transmissões a fim de mostrar que as imagens que estão sendo observadas são da emissora (NUNES, 2008). A Figura 5 mostra um exemplo de imagem marcada com um sistema de marca d'água visível.

Figura 5 – Imagem com marca d'água visível

Fonte: Globo [1].

2.6.4 Marca d'água invisível

Ao introduzir uma marca d'água altera-se o arquivo em que se está inserindo a marca. Em imagens, os valores dos *pixels* serão modificados. Assim, deseja-se que nas técnicas de marca d'água invisíveis as modificações nos valores dos *pixels* da imagem original H, não sejam visíveis ao olho humano, ou seja, a imagem marcada HW precisa ser visualmente idêntica a imagem original H. Isso se dá pelo fato do sistema visual humano não ser capaz de diferenciar modificações pequenas na escala de cores (LOPES, 2006).

As modificações feitas nos *pixels* de uma imagem para a introdução de uma marca d'água invisível podem ser feitas no domínio espacial ou da frequência. A seleção do domínio ocorre segundo a particularidade a ser considerada no sistema de marca d'água, seja ela robusta, frágil ou semi-frágil (LOPES, 2006). A Figura 6 mostra um exemplo de imagem marcada com um sistema de marca d'água invisível.

Figura 6 – Imagem com marca d'água invisível

Fonte: COIMBRA, 1998.

[1] https://g1.globo.com/jornal-nacional/

2.6.4.1 *Marca d'água invisível robusta*

Este tipo de marca d'água é feito para suportar ações não maliciosas, mas a utilização de marcas d'água robustas também tem sido empregada em cenários que consideram a possibilidade de manipulação maliciosa de objetos digitais. No contexto da venda de livros digitais, por exemplo, é possível marcar o objeto com o CPF do comprador original, a fim de identificar sua autoria. É importante que a marca d'água seja robusta, visto que o comprador pode tentar distribuir o objeto ilegalmente, buscando eliminar a marcação por meio de manipulação maliciosa. É relevante para proteger o direito autoral e combater a pirataria digital extrair a marcação mesmo após a manipulação, possibilitando a identificação do CPF da pessoa que realizou a distribuição ilícita, se a marca d'água resistir aos ataques perpetrados pelo comprador. As marcas d'águas robustas se adequam a aplicações em que seria improvável que alguém manipulasse o documento digital com o intuito de extrair a marca d'água. Em contrapartida, a prática que usa esse tipo de marca com frequência manipula o documento digital, isto é, o emprego habitual do documento não deve modificar o dado oculto, por essa razão a marca d'água precisa ser robusta (NUNES, 2008).

2.6.4.2 *Marca d'água invisível frágil*

As técnicas de introdução de marca d'água frágeis são usadas para certificar a integridade da imagem, isto é, averiguar se a imagem marcada passou por algum tipo de manipulação de imagens. Estas marcas d'água são prontamente adulteradas por qualquer tipo de operação de processamento de imagem empregue sobre a imagem marcada. Desse modo, para saber se uma imagem marcada sofreu manipulação, é preciso extrair a marca d'água introduzida e equiparar o resultado da extração com a marca original. Se diferirem, a imagem marcada sofreu adulteração. Senão, conclui-se que a imagem marcada não sofreu ataque (LOPES, 2006).

2.6.4.3 *Marca d'água invisível semi-frágil*

A técnica de marca d'água invisível semi-frágil é uma técnica de proteção para documentos digitais que permite a realização de manipulações específicas e limitadas sem que haja danos significativos à documentação original, ou seja, é possível modificar o documento de forma controlada sem comprometer sua integridade.

No entanto, é importante ressaltar que essas manipulações não devem ser maliciosas, ou seja, não podem visar a danificar a marca d'água ou prejudicar a autenticidade do documento.

Além disso, essa técnica é indicada para aplicações que não exigem alta robustez, mas que permitem a perda ou modificação do documento original no qual a marca está inserida.

Portanto, a marca d'água semi-frágil pode ser uma alternativa útil para proteger a autoria ou a originalidade de documentos digitais em situações que não exigem uma segurança extrema (NUNES, 2008).

2.6.5 Propriedades de Marca d'água digital

Algumas propriedades são importantes para o desenvolvimento de um sistema de marca d'água, tais como a imperceptibilidade, robustez, capacidade da marca d'água e segurança.

2.6.5.1 *Imperceptibilidade*

A marca d'água invisível deve ser imperceptível ao olho humano e visualmente idêntica à imagem de origem, sem danificar suas propriedades visuais, para isso, é necessário considerar os atributos do sistema visual humano na técnica de inserção. Outra característica desejável é que a marca não seja descoberta ou eliminada por ataques, para isso, é preciso realizar um estudo acerca de propriedades da robustez (LOPES, 2006).

2.6.5.2 *Robustez*

As marcas d'água robustas são projetadas para suportar a maioria dos processos de adulteração de imagens, permitindo que o dado introduzido por meio dessa técnica seja extraído mesmo após a imagem hospedeira sofrer rotação, mudança de escala, mudança de brilho/contraste, compressão com perdas em diferentes níveis de compressão, corte das bordas, entre outros. Uma marca d'água robusta adequada deveria ser inviável de ser retirada a menos que a característica da imagem derivada danifique na iminência de arruinar o seu conteúdo visual. Em outros termos, a relação entre uma imagem marcada e a marca d'água robusta nela colocada deve continuar detectável mesmo após um processamento digital, durante o tempo em que a imagem resultante do processamento ficar visualmente perceptível assim como a imagem original. Portanto, marcas d'água robustas são comumente usadas para averiguação de propriedade ou de *copyright* das imagens (KIM, 2003).

Em seu trabalho, Cox *et al.* (1997) alega que apenas se consegue a robustez se insere-se a marca em componentes visivelmente consideráveis de uma imagem. Isso gera um discordância, pois, conforme visto na subseção 2.6.5.1, a marca d'água precisa ser imperceptível. Pode-se

usar um critério de escala em que se introduz uma proporção da marca nos componentes mais significativos para solucionar o dilema mencionado. Além disso, outra propriedade importante a ser estudada em sistemas de marca d'água é a quantidade de informação suportada por cada técnica.

2.6.5.3 *Watermarking payload*

Watermarking Payload, ou a capacidade de inserção das técnicas de marca d'água, pode ser definida como a quantidade máxima de informação a ser introduzida na imagem inicial. Uma atribuição quase inviável de se realizar previamente é apontar uma quantia máxima para o tamanho da marca a se introduzir, uma vez que as inserções dependem de quais são as finalidades da técnica que está sendo empregada, os atributos de tamanho, cor, níveis de textura e bordas, da imagem inicial. Em geral, em sistemas de marca d'água com robustez o tamanho da marca é cerca de $\frac{1}{16}$ do tamanho da imagem original, isto é, em uma imagem original de tamanho 512 x 512 *pixels*, o tamanho da marca d'água a ser inserida precisaria ser igual a 1024 *pixels* (NUNES, 2008).

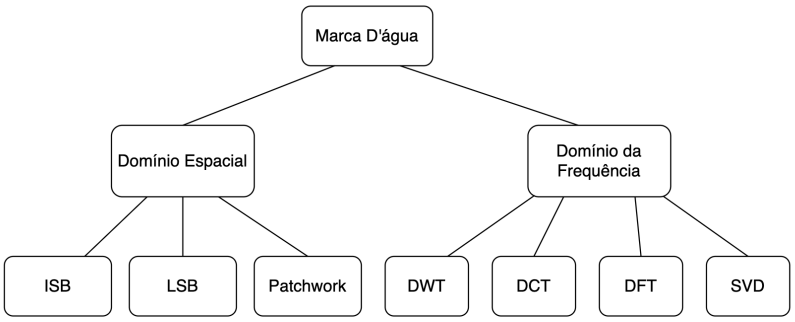
2.6.5.4 *Segurança*

Para uma técnica de marca d'água ser tida como segura os algoritmos de inserção não devem permitir, que uma entidade sem autorização, perceba a existência dela e possa realizar sua extração. Com o objetivo de garantir a segurança da marca d'água, uma opção é utilizar uma chave confidencial durante a sua inserção e remoção, que pode envolver, por exemplo, a troca dos *pixels* da marca. De maneira geral, as técnicas de criptografia têm o potencial de oferecer uma camada adicional de segurança para complementar as técnicas de marca d'água (NUNES, 2008).

2.6.6 Técnicas de Marca d'água em Imagens Digitais

As técnicas de marca d'água são essenciais para proteger o conteúdo digital contra acesso e manipulação não autorizados, e são aplicáveis em diversas áreas, que serão exemplificadas na subseção 2.6.7. As técnicas de marca de água de imagem digital podem ser classificadas com base no domínio do espaço e da frequência, como ilustrado na Figura 7.

Figura 7 – Principais métodos de marca d'água.



Fonte: A autora, 2023.

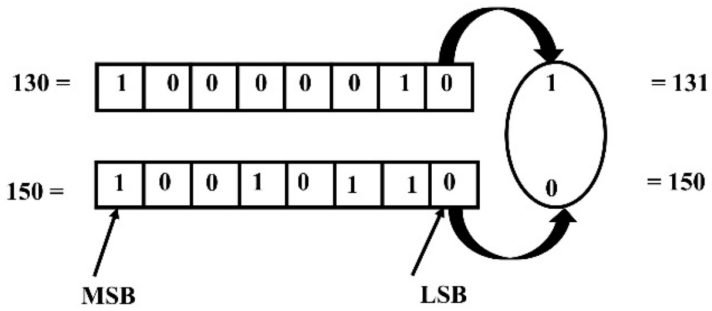
2.6.6.1 *Domínio Espacial*

Na sequência, serão tratados os seguintes métodos do domínio espacial referentes à marca d'água: ISB, LSB e *Patchwork*.

- ***Least Significant Bit (LSB)***: os bits menos significativos de uma imagem podem ser utilizados para a implantação de marca d'água com o intuito de arquivar informações de veracidade, sem comprometer a qualidade visual da imagem. Um exemplo pode ser visto no trabalho de (LIU *et al.*, 2016), que elabora uma ferramenta cega e robusta de marca d'água para direitos autorais de imagens coloridas (FERREIRA, 2020).

  A técnica LSB pode ser exemplificada pela Figura 8, na qual é considerada uma imagem hospedeira com dois valores de *pixels*, sendo eles 130 (10000010) e 150 (10010110). Depois, empregando a técnica, se a marca de água inserida for 10, então os valores dos *pixels* com marca d'água serão 131 (10000011) e 150 (10010110), respectivamente.

Figura 8 – Exemplo da técnica do bit menos significativo (LSB).



Fonte: BEGUM; UDDIN, 2020.

- ***Intermediate Significant Bit (ISB)*:** as técnicas *LSB* em geral são as mais triviais e simples técnicas de marca d'água no domínio espacial, no entanto não asseguram robustez contra ataques. Desta forma, métodos alternativos foram elaborados, como os métodos de bit significativo intermediário (*ISB*), a fim de melhorar a robustez e preservar a qualidade do sistema de marca d'água. Muitos estudos apresentaram métodos *ISB* aplicando diferentes algoritmos, sendo que um destes substitui o método clássico *LSB* por *ISB*, o que resguarda a imagem da marca d'água de vários ataques e reduz a modificação da imagem da marca d'água (BEGUM; UDDIN, 2020).

- ***Patchwork***: esta é uma técnica estatística pseudo-aleatória, que é acrescentada numa imagem original aplicando códigos de padrões difusos por uma distribuição gaussiana. Os métodos de *patchwork* apresentam melhor robustez contra alterações não geométricas máximas da imagem e o processo independe do conteúdo da imagem original. Este método é apropriado para grandes áreas de textura aleatória, mas não para imagens de texto. A marca d'água pode ser introduzida utilizando uma codificação de padrões redundantes numa imagem, e a marca d'água pode ser removida manuseando uma chave secreta referente ao algoritmo de descodificação (BEGUM; UDDIN, 2020).

2.6.6.2 *Domínio da Frequência*

A seguir, serão discutidos os seguintes métodos de marca d'água do domínio da frequência: DWT, DCT e DFT.

- **Transformada *Wavelet* Discreta (DWT)**

  Esse método, que utiliza a transformada *wavelet* para descobrir regiões de interesse na imagem que podem armazenar a marca d'água, consiste em amostrar de forma discreta as *wavelets* numa *DWT*. Uma das vantagens da DWT sobre as transformadas de Fourier (DCT e DFT) é a resolução temporal, fazendo a DWT um tema de investigação mais atrativo, reunindo várias características da informação, como localização no tempo e frequência. A transformada *wavelet*, que utiliza um grupo de *wavelets* representadas por funções matemáticas, é empregue para decompor o sinal, se adequando ao processamento digital do sinal, compressão de imagem, e na remoção do ruído do sinal (BEGUM; UDDIN, 2020). A DWT de um sinal x[n] é determinada pelas equações a seguir:

$$W_{\phi}[j_{0,\mathrm{k}}] = \frac{1}{\sqrt{M}} \sum_{n} x[n] \phi_{\mathrm{j0,k}}[n] \tag{2.3}$$

$$W_{\psi}[j,k] = \frac{1}{\sqrt{M}} \sum_{n} x[n] \psi_{\mathrm{j,k}}[n] \tag{2.4}$$

em que j $\geq j_0$, $W_{\phi}[j_{0,\mathrm{k}}]$ são os coeficientes de aproximação e $W_{\psi}[j,k]$ são os coeficientes de detalhe.

A transformada inversa é dada por:

$$x[n] = \frac{1}{\sqrt{M}} \sum_{k} W_{\phi}[j_{0,\mathrm{k}}] \phi_{\mathrm{j0,k}}[n] + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{J} \sum_{k} W_{\psi}[j,k] \psi_{\mathrm{j,k}}[n] \tag{2.5}$$

em que

$$n = 0,1,2,...,M-1, j = 0,1,2,...,J-1, k = 0,1,2,...,2^j - 1 \tag{2.6}$$

onde M é o número de amostras a serem transferidas = 2^J, J é o número de níveis de transferência, $\phi_{\mathrm{j,k}}$[n] e $\psi_{\mathrm{j,k}}$[n] são duas funções básicas, ϕ[n] indica a função de escala, e ψ[n] indica a função *wavelet*.

- **Transformada Discreta do Cosseno (DCT)**

  A Transformada Discreta do Cosseno decompõe uma imagem nos seus coeficientes de frequência correspondentes transformando as componentes de frequência, que podem ser apresentadas como um somatório de funções cosseno. A *DCT* possui uma sequência finita de pontos de dados e somente números reais podem ser usados aqui. A variância indica a finalidade dos coeficientes da DCT. A DCT se mostra relevante, por exemplo, para a compressão de imagem, no formato de imagem *JPEG* (BEGUM; UDDIN, 2020). A DCT unidimensional (1D) é determinada pela equação a seguir:

$$y(k) = \alpha(k) \sum_{n=0}^{N-1} x(n) cos\left(\frac{\pi(2n+1)k}{2N}\right), k = 0,1,...,N-1 \tag{2.7}$$

e a transformada inversa é dada por:

$$x(n) = \sum_{k=0}^{N-1} \alpha(k)\, y(n)\, cos\left(\frac{\pi(2n+1)k}{2N}\right), n = 0, 1, ..., N-1 \tag{2.8}$$

em que

$$a(0) = \sqrt{\frac{1}{N}}, k = 0 e \alpha(k) = \sqrt{\frac{2}{N}}, 1 \leq k \leq N-1 \tag{2.9}$$

onde N é o número de determinadas amostras de dados: x(0), . . x(N - 1), x(n) é a amostra de dados de entrada, y(k) é o coeficiente de DCT, e α(k) é o fator de escala.

- **Transformada Discreta de *Fourier* (DFT)**

  A Transformada Discreta de *Fourier* é realizada usando amostras espaçadas harmonicamente para modificar uma sequência fixa de números de amostras uniformemente espaçadas de uma função em uma sequência de amostras uniformemente espaçadas de igual comprimento na Transformada de *Fourier* de tempo discreto (DTFT). A *DTFT* utiliza um grupo de funções exponenciais complexas (magnitude e fase) associadas de forma harmônica, enquanto a *DFT* representa a sequência de entrada original no domínio da frequência e gera um sinal discreto. Alguns exemplos de aplicações práticas em que é empregada a *DFT* abrangem processamento de sinal, processamento de imagem, filtros, operações de convolução, análise do espectro senoidal, e análise de *Fourier* (BEGUM; UDDIN, 2020). A equação a seguir define uma DFT unidimensional:

$$y(k) = \sum_{n=0}^{N-1} x(n)\, exp\left(-j\frac{2\pi}{N}kn\right), k = 0, 1, ..., N-1 \tag{2.10}$$

A transformada inversa é dada por

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} y(k)\, exp\left(j\frac{2\pi}{N}kn\right), n = 0, 1, ..., N-1 \tag{2.11}$$

em que

$$j = \sqrt{-1} \tag{2.12}$$

e N é o número de amostras de dados: x(0), . . . x (N - 1), y(k) são os coeficientes da DFT, e x(n) é a amostra de dados de entrada.

2.6.7 Aplicações da Marca D'água digital

2.6.7.1 *Prova de Propriedade*

Uma marca d'água pode ser usada não só para identificar o autor de uma obra, mas também para comprovar que uma pessoa é a autora de uma determinada imagem, mesmo quando o símbolo de *copyright* © é modificado, já que a marca d'água permanece existindo. Ademais, caso a marca d'água seja degradada, ela não poderá ser totalmente eliminada, permitindo que o autor prove, mediante a imagem original, que a imagem alterada origina-se de sua imagem (SANS, 2008).

2.6.7.2 *Monitoramento de Transmissão*

Uma aplicação comum da marca d'água é no monitoramento de transmissão, o qual pode ser feito de duas formas: ativa e passiva. No passivo, cada transmissão se compara com uma base de dados com todos os trabalhos exercidos na área a fim de entender qual comercial, filme, programa, está sendo transmitido. No entanto, existe o dilema de administrar uma base de dados com milhões de entradas e ter uma procura imediata que possa encontrar, nos milhões de bits de cada *frame* de informação, a assinatura equivalente à entrada, além do desgaste de sinal que a transmissão pode enfrentar. No monitoramento ativo, um sinal imperceptível ao olho humano é propagado junto com o conteúdo do programa e identificado por um computador, permitindo a colocação de marcas d'água sem causar grande mudança na transmissão (SANS, 2008).

2.6.7.3 *Autenticação de Conteúdo*

A autenticidade de uma informação é fundamental em muitas aplicações, e uma das técnicas mais conhecidas para garantir isso é a assinatura digital, em que uma assinatura da mensagem é criptografada e colocada no contexto da mesma. Para uso dessa técnica de criptografia, existem dois métodos mais empregados: a criptografia de chave simétrica ou chave secreta e a criptografia de chave assimétrica ou chaves pública/privada.

No entanto, existem muitos pontos negativos com relação a tais técnicas, como o fato de que a assinatura deve ser transportada com a mensagem em um cabeçalho, o que torna comum a

perda desse dado. Uma alternativa a tais técnicas de criptografia são as marcas d'água já que são embutidas exatamente na mensagem (SANS, 2008).

2.6.7.4 *Controle de Cópias*

O principal propósito dessa área é evitar que sejam feitas cópias ilegítimas de um trabalho por meio da inserção de uma marca d'água no trabalho e de detectores nas ferramentas capazes de ler o trabalho. Dessa maneira, se uma cópia não autorizada é detectada, é possível saber a origem das cópias não autorizadas, removendo-se a marca d'água, que aponta a quem foi entregue o arquivo marcado original. A principal objeção dessa técnica é impor os fabricantes a instalarem tais sistemas em seus aparelhos e também, obrigar os consumidores a obter aparelhos que apenas leiam trabalhos originais (SANS, 2008).

2.6.7.5 *Transporte de informação adicional*

O uso de marca d'água possibilita determinar um método de comunicação, no qual a marca d'água é a mensagem, e o item com a marca é o canal de transmissão. Assim, no transporte de informação adicional a robustez do sistema de marca d'água não é levada em conta, visto que o intuito é camuflar o máximo de informação de maneira oculta em um dado multimídia. Esse tipo de comunicação é bastante usada no meio militar, em métodos que abrangem segredos de estado e entre instituições financeiras onde o sigilo precisa ser mantido (LOPES, 2006).

3 PROPOSTA E DESENVOLVIMENTO

Este capítulo descreve a metodologia utilizada para desenvolver a proposta de implementação de algoritmos esteganográficos em imagens digitais. Itens como linguagem de programação escolhida, algoritmos implementados e eficácia serão abordados a seguir.

3.1 Seleção das técnicas e algoritmos

Um dos algoritmos de esteganografia estudados foi escolhido para ser testado de acordo com as métricas estabelecidas. O método de esteganografia escolhido foi a inserção no bit menos significativo (*LSB*), porque é fácil de implementar e amplamente utilizado em aplicações de esteganografia e marcas d'água.

3.2 Linguagem de programação

A linguagem de programação *Python*, que é de alto nível de tipagem dinâmica e forte, será utilizada tanto para realizar a aplicação da esteganografia quanto para executar as análises. Essa linguagem compreende um conjunto de bibliotecas que possibilitam a manipulação de imagens e matrizes (formato como as imagens são representadas computacionalmente), como *numpy* e *matplotlib*. Também será utilizado o package *scikit-image* que permite comparar a imagem original e o estego-objeto, que é o produto final, ou seja, a imagem com dados ocultos.

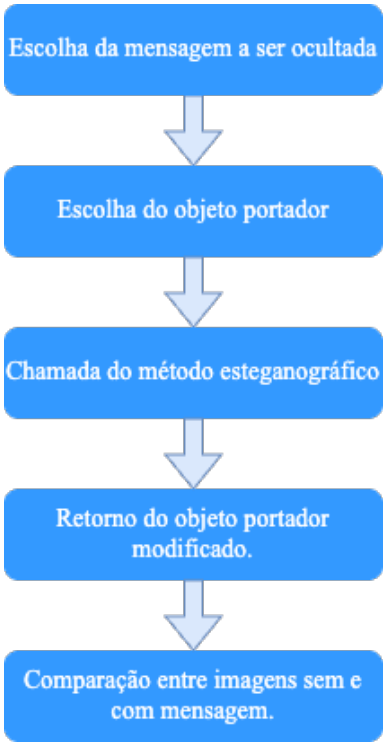
- Numpy: é uma biblioteca que permitem trabalhar com dados, *arrays* multidimensionais, tabelas, análises, manipulações de dados.
- Matplotlib: é uma biblioteca para visualização de dados que permite a criação de gráficos e plotagem 2D.
- Scikit-image: é um pacote *Python* de processamento de imagem que funciona com matrizes NumPy, que é uma coleção de algoritmos para processamento de imagens.

3.3 Desenvolvimento

Esta seção visa explicar o desenvolvimento do projeto, apontando as etapas seguidas, desde a escolha da imagem, a inserção da mensagem na imagem, a geração das métricas de

comparação e o cálculo de erro entre a imagem original e o estego-objeto. A Figura 9 mostra qual será o fluxo padrão da aplicação, até a geração do estego-objeto.

Figura 9 – Processo esteganográfico de ocultação da mensagem.



Fonte: A autora, 2023.

No método esteganográfico utilizado, recebe-se como parâmetro uma mensagem a ser ocultada, e, após carregar um objeto portador, cria um vetor de inteiros que recebe o valor ASCII (*American Standard Code for Information Interchange*) das letras da mensagem. Para escolher a mensagem a ser ocultada na imagem, optou-se por uma mensagem que ocupasse mais espaço na imagem (aproximadamente 40% da imagem), com o intuito de observar melhor as diferenças, e a mensagem escolhida é mostrada no anexo A.

Como mencionado anteriormente, o método utilizado para inserir a mensagem é o *LSB*, para tal foi necessário inicialmente converter a mensagem que se quer ocultar em um vetor de inteiros que recebe o valor *ASCII* de cada letra da mensagem. A Figura 10 exibe o algoritmo *Python* responsável por converter a mensagem em algoritmo binário.

Figura 10 – Processo esteganográfico de ocultação da mensagem.

```python
import matplotlib.pyplot as plt
import numpy as np
import math
from skimage.metrics import structural_similarity as ssim

msg = "Before the early 1960s, computers were mainly used for number-

# Função que converte um texto em uma sequência binária
def text2Binary(msg):
    l, m = [], []
    for i in msg:
        l.append(ord(i))
    for i in l:
        m.append(bin(i)[2:].zfill(7))
    return ''.join(m)

binary_msg = text2Binary(msg)
print("Sequência de bits", binary_msg)
print("Quantidade de bits:", len(binary_msg))
```

Fonte: A autora, 2023.

A Figura 11 exibe a saída do algoritmo exibido na Figura 10.

Figura 11 – Saídas do algoritmo

```
Sequência de bits: 1000010110010111001101101111111001011001010100
1100010111001011011001100001110011010110001000001100011110111110
1100101010000011011011100001110100111011101101100111100101000011
1110110111000101100101111001001011011100011111001011101011101110
0111100100100000111010011010001100001110111001000001100110111011
1000100000110110111001011101101110111111100101111001010000011101
1100111100101000001100101111100011100001100101110111011100111010
0010111100101110011010000011011111100110111010011001011101110010
1011111101110110110011111001010100000011011001000001100010110100111
0100000110001111010001100001111001011000011100011111010011001011
```

Quantidade de bits: 28344

(a) Sequência de bits convertida (b) Quantidade de bits

Fonte: A autora, 2023.

No contexto deste trabalho, optou-se por utilizar uma imagem em escala de cinza como objeto portador, e a Figura 12 exibe a imagem escolhida para tal fim, que foi convertida para preto e branco utilizando apenas um dos canais de cor. A imagem portadora, com tamanho de 256x256 e codificada a 8 bits por pixel, será utilizada para ocultar a mensagem selecionada.

Figura 12 – Imagem original.

Fonte: A autora, 2023.

É necessário converter a imagem em uma matriz de vetores, contendo 256 linhas e 256 colunas, de acordo com o tamanho da imagem. A Figura 13 exibe o algoritmo *Python* responsável por essa conversão.

Figura 13 – Imagem original.

```
21  #Imprime a imagem em forma matricial
22  img = plt.imread("4.1.01.tiff")
23  # Seleciona um dos canais de cor para obter uma foto em preto e branco
24  img = img[:, :, 0]
25  print(img)
26  plt.imshow(img, cmap='gray')
27  plt.show()
```

Fonte: A autora, 2023.

A Figura 14 exibe a saída do algoritmo mostrado anteriormente e a Figura 15 exibe a matriz convertida em binário, etapa também necessária nesse processo.

Figura 14 – Imagem convertida em sequência de vetores.

```
[[ 52  47  50 ... 137 126 126]
 [ 55  50  54 ... 129 129 121]
 [ 46  49  52 ... 126 123 118]
 ...
 [  4   3   3 ...  60  84  98]
 [ 11  12  12 ...  60  86 100]
 [ 20  19  20 ...  55  70  93]]
```

Fonte: A autora, 2023.

Figura 15 – Matriz convertida em binário.

```
[['00110100' '00101111' '00110010' ... '10001001' '01111110' '01111110']
 ['00110111' '00110010' '00110110' ... '10000001' '10000001' '01111001']
 ['00101110' '00110001' '00110100' ... '01111110' '01111011' '01110110']
 ...
 ['00000100' '00000011' '00000011' ... '00111100' '01010100' '01100010']
 ['00001011' '00001100' '00001100' ... '00111100' '01010110' '01100100']
 ['00010100' '00010011' '00010100' ... '00110111' '01000110' '01011101']]
```

Fonte: A autora, 2023.

A próxima etapa inclui a implementação do método esteganográfico, de maneira que cada bit da sequência convertida deve substituir o bit menos significativo de cada item da matriz convertida. A Figura 16 exibe o algoritmo que implementa este método, isso é feito baseado no tamanho da sequência de bits que foi convertida e são utilizados dois laços *for*, no qual um "varre"as colunas e outro as linhas da matriz. Após a substituição no bit menos significativo, a matriz, até então em binário, é convertida novamente em inteiro.

Figura 16 – Algoritmo de implementação do método *LSB*.

```
32  # Inserção da sequência de bits no plano de bits especificado
33  x, y = img.shape
34  tam = len(binary_msg)
35  count = 0
36
37  list_msg = list(binary_msg)
38  new_img = img.copy()
39
40  for i in range(x):
41    for j in range(y):
42
43      # Convertendo para binário
44      bin_num = bin(img[i, j])[2:].zfill(8)
45
46      # Alterando o bit correspondente
47      bin_num = list(bin_num)
48      bin_num[plane] = list_msg[count]
49
50      # Convertendo para inteiro
51      new_img[i, j] = int(''.join(bin_num), 2)
52
53      count += 1
54
55      if (count >= tam):
56        break
57    if (count >= tam):
58        break
```

Fonte: A autora, 2023.

A Figura 17 exibe a saída do algoritmo anterior, que consiste em uma nova matriz já com as devidas substituições.

Figura 17 – Nova matriz com a mensagem inserida.

```
[[ 53  46  50 ... 137 127 126]
 [ 54  51  54 ... 129 128 121]
 [ 47  48  52 ... 126 122 119]
 ...
 [  4   3   3 ...  60  84  98]
 [ 11  12  12 ...  60  86 100]
 [ 20  19  20 ...  55  70  93]]
```

Fonte: A autora, 2023.

A etapa final do projeto permite realizar comparações entre a imagem original e o estego-objeto de três formas: comparando visualmente, comparar por meio de uma métrica objetiva e comparando visualmente o plano de bits de ambas imagens.

A Figura 18 apresenta o algoritmo responsável por mostrar visualmente ambas as imagens original e com a mensagem inserida.

Figura 18 – Algoritmo que permite comparação visual entre imagens.

```
61  # Comparação visual entre a imagem original
62  # e com a mensagem inserida
63  f, axarr = plt.subplots(1,2)
64  axarr[0].imshow(img, cmap='gray')
65  axarr[1].imshow(new_img, cmap='gray')
```

Fonte: A autora, 2023.

Para comparar as imagens por meio de métrica de similaridade foi utilizado o algoritmo da Figura 19.

Figura 19 – Algoritmo que permite comparação por meio de métrica.

```
68  # Calculando uma métrica de similaridade
69  ssim = ssim(img, new_img)
70  print("SSIM:", ssim)
71
```

Fonte: A autora, 2023.

Para implementação do algoritmo da Figura 21, o qual permite comparar visualmente o plano de bits de cada imagem, foi preciso criar uma função mostrada na Figura 20 que possibilita extrair um plano de bits de uma imagem.

Figura 20 – Função que extrai plano de bits de imagem.

```
74  # Função auxiliar para extrair um plano de bits de uma imagem
75  def getBitPlane(img, plane):
76      bit_plane_image = np.zeros(img.shape)
77
78      x, y = img.shape
79      for i in range(x):
80          for j in range(y):
81              bin_num = bin(img[i, j])[2:].zfill(8)
82
83              bin_num = list(bin_num)
84              bit_plane_image[i, j] = int(bin_num[plane])
85
86      return bit_plane_image
```

Fonte: A autora, 2023.

Figura 21 – Algoritmo que permite comparação visual do plano de bits.

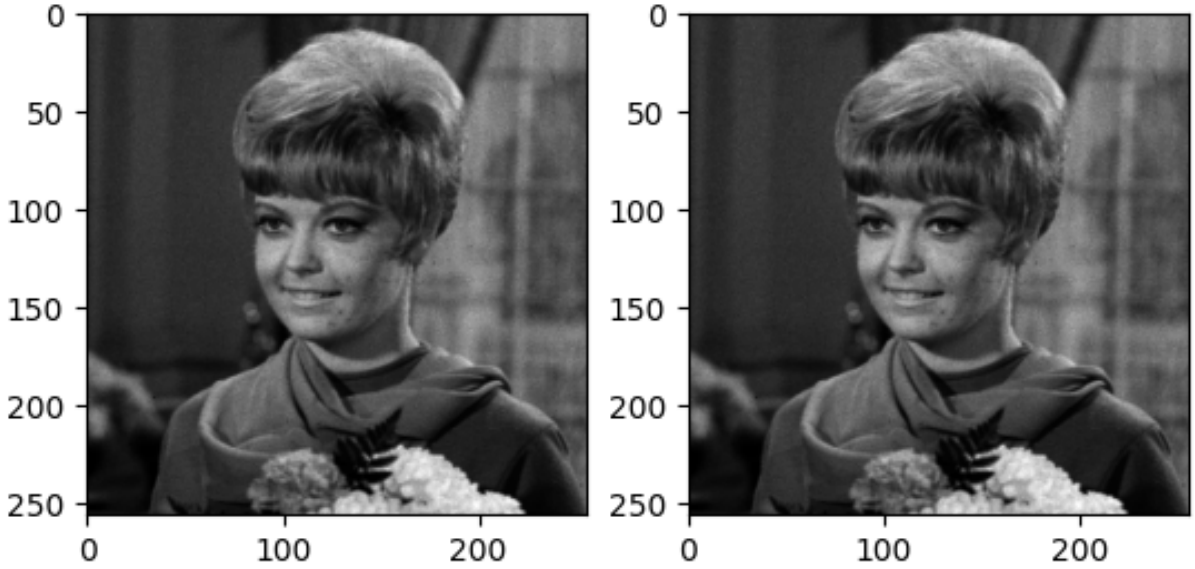
```
88  # Comparação visual do plano de bits
89
90  f, axarr = plt.subplots(1,2)
91  axarr[0].imshow(getBitPlane(img, plane), cmap='gray')
92  axarr[1].imshow(getBitPlane(new_img, plane), cmap='gray')
93  plt.show()
```

Fonte: A autora, 2023.

4 RESULTADOS E DISCUSSÃO

Após a criação do algoritmo de implementação da técnica LSB visando obter uma imagem com uma mensagem oculta, foi possível visualizar o *stego-objeto*. Conforme mencionado na Seção 3.3, a Figura 22 permite comparar visualmente a imagem original e a imagem com a mensagem inserida.

Figura 22 – Comparação visual entre a imagem original e o *stego-objeto*.



Fonte: A autora, 2023.

Além disso, foi utilizada a métrica *SSIM* (*Structural Similarity Index*), que consiste em uma métrica de similaridade, com o intuito de constatar a diferença entre ambas as imagens, no qual o valor obtido está entre 0 e 1 (0 = completamente diferente / 1 = igual). O *SSIM* é um método para avaliar a qualidade de imagens e vídeos digitais. Ele usa uma imagem de referência sem distorção como base e leva em conta o mascaramento de luminância e contraste. Isso reduz a visibilidade de distorções em regiões claras e com texturas significativas. Ele estima erros relativos baseando-se na forte interdependência dos *pixels*, que carregam informações importantes sobre a estrutura dos objetos na cena visual. O índice *SSIM* é calculado em várias janelas de uma imagem. A medida entre duas janelas x e y de tamanho comum N x N é:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{\mathrm{xy}} + c_2)}{(\mu^2{}_{\mathrm{x}} + \mu^2{}_{\mathrm{y}} + c_1)(\sigma^2{}_{\mathrm{x}} + \sigma^2{}_{\mathrm{y}} + c_2)} \tag{4.1}$$

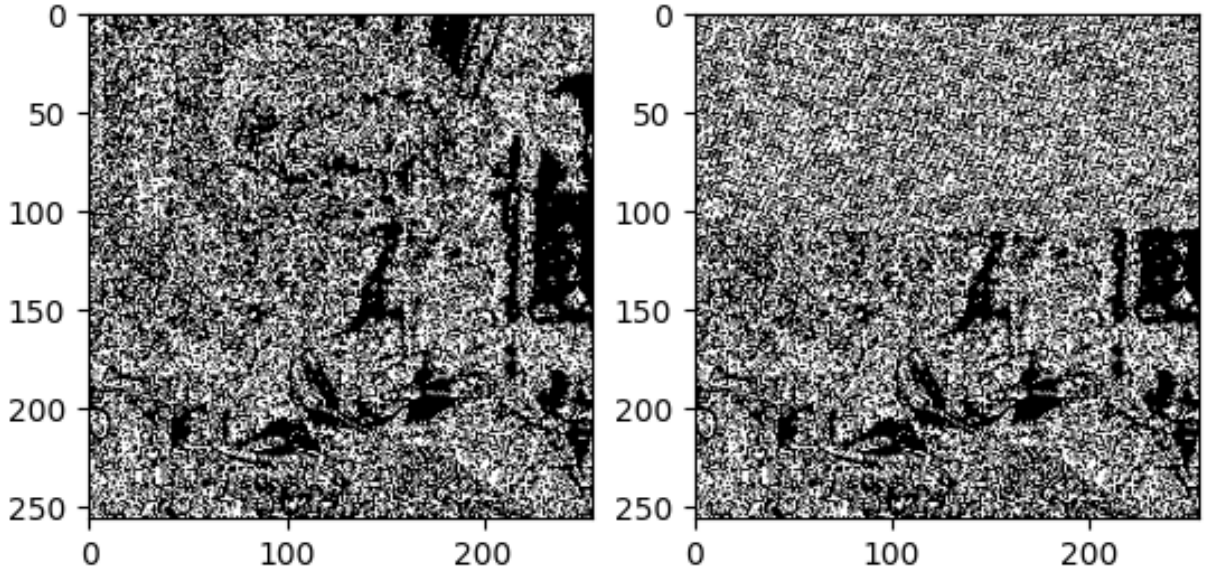
em que:

- μ_x é a média da amostra de *pixels* de x.
- μ_y é a média da amostra de *pixels* de y.
- $\sigma^2{}_{\mathrm{x}}$ é a variância de x.
- $\sigma^2{}_{\mathrm{y}}$ é a variância de y.
- σ_{xy} é a covariância de x e y.
- $c_1 = (k_1 L)^2, c_2 = (k_2 L)^2$ são duas variáveis para estabilizar a divisão com denominador fraco.
- L é a faixa dinâmica dos valores de *pixels*.
- $k_1 = 0.01$ e $k_2 = 0.03$ por padrão.

Assim, foi aplicada a métrica e obtido o valor ***SSIM: 0.9986812026773805***, o qual por ser bem próximo de 1, evidencia uma alta similaridade entre as imagens, indicando que a inserção da mensagem afeta pouco a qualidade visual da imagem.

A última etapa da comparação exibe uma comparação visual do plano de bits especificado da imagem original (esquerda) e da imagem com a mensagem inserida (direita). Na Figura 23 é possível perceber que a inserção da mensagem deixa um rastro no plano de bits que pode ser observado na porção superior da imagem. Essa pode ser considerada uma das limitações desse método, pois a exibição do plano de bits revela o local onde a mensagem foi inserida, o que representa uma falha.

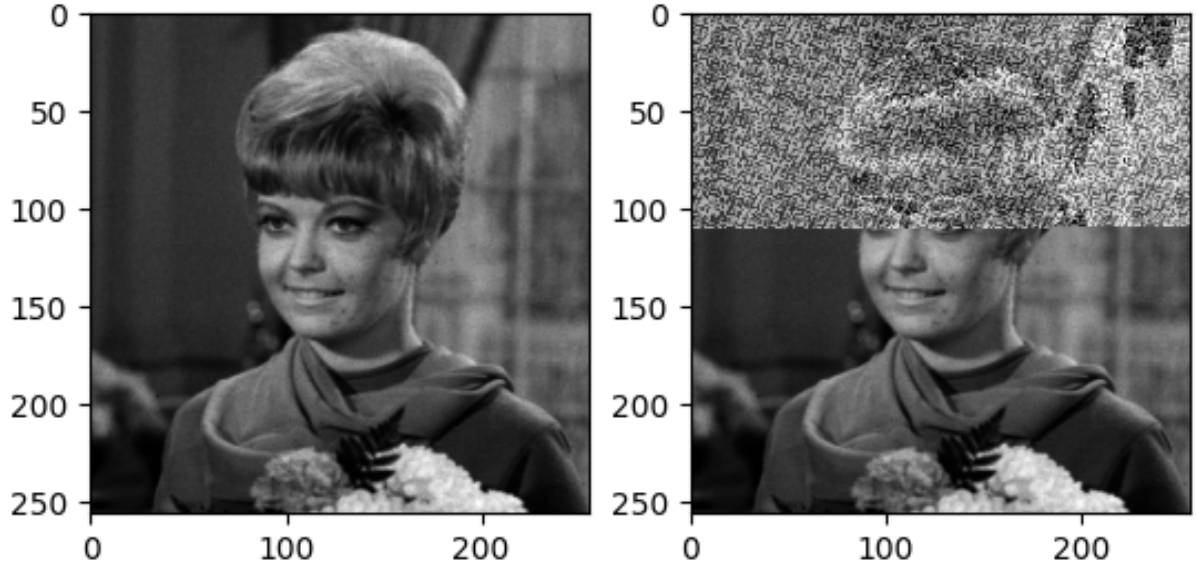
Figura 23 – Comparação visual do plano de bits das imagens.



Fonte: A autora, 2023.

Na Figura 24, a mensagem foi inserida no bit mais significativo (MSB) com o único propósito de avaliar a quantidade de degradação da imagem. Enquanto a inserção no bit menos significativo (LSB) tem um impacto mínimo na aparência visual da imagem, a inserção no MSB leva a uma degradação significativa da qualidade visual da imagem. Também foi aplicada a métrica SSIM para comparação da similaridade entre as imagens e o resultado obtido foi ***SSIM: 0.5683237396340645***, o que evidencia a degradação visual da imagem.

Figura 24 – À esquerda, imagem original, à direita imagem modificada.



Fonte: A autora, 2023.

5 CONCLUSÕES

A garantia da segurança da informação é um desafio diante do grande número de técnicas que podem violar a privacidade dos dados digitais. Para impedir que pessoas não autorizadas tenham acesso a informações confidenciais, diversas técnicas estão sendo utilizadas, incluindo a esteganografia. A esteganografia é considerada uma proteção eficiente quando se trata de segurança digital, pois permite a privacidade nas comunicações pela rede de computadores ao ocultar informações, porém é possível que essa privacidade esteja exposta a pessoas mal-intencionadas.

No projeto de conclusão de curso apresentado e avaliado, foi utilizado o método de esteganografia LSB aplicado em imagens, que se mostrou altamente benéfico e eficaz, principalmente quando se trata de inserir uma pequena quantidade de informação. No entanto, à medida que a quantidade de caracteres inseridos nas imagens aumenta, a probabilidade de serem identificadas imperfeições também aumenta.

Dessa forma, em decorrência dos resultados oferecidos, pode-se concluir que a utilização da técnica esteganográfica LSB em imagem é viável, uma vez que permite uma comunicação segura entre pessoas independentemente do local onde estejam, conservando assim a privacidade e mantendo o conteúdo da mensagem em sigilo.

Como sugestões para trabalhos futuros propõe-se focar em aprimorar a capacidade de inserção sem comprometer a integridade visual, explorar métodos esteganográficos alternativos, realizar testes abrangentes para avaliar resistência a ataques, estudar a quantidade ideal de dados ocultos e expandir para outros formatos de mídia. Além disso, o desenvolvimento de ferramentas de detecção mais sofisticadas e uma análise mais profunda do impacto na integridade da imagem podem contribuir para avanços significativos na compreensão e aplicação da ocultação de dados em imagens digitais, fortalecendo a segurança da informação.

REFERÊNCIAS

ARTZ, D. Digital steganography: hiding data within data. **IEEE Internet computing**, USA, v. 5, n. 3, p. 75–80, 2001. DOI: https://doi.org/10.1109/4236.935180. Disponível em: https://ieeexplore.ieee.org/document/935180. Acesso em: 27 nov. 2022.

BEGUM, M.; UDDIN, M. S. Digital image watermarking techniques: a review. **Information**, Bangladesh, v. 11, n. 2, p. 110, 2020. DOI: https://doi.org/10.3390/info11020110. Disponível em: https://www.mdpi.com/2078-2489/11/2/110. Acesso em: 13 fev. 2023.

BERGHEL, H. Watermarking cyberspace. **Communications of the ACM**, ACM New York, NY, USA, v. 40, n. 11, p. 19–24, 1997. DOI: https://doi.org/10.1145/265684.265687. Disponível em: https://www.cis.upenn.edu/ lee/00cis640/papers/berghel.pdf. Acesso em: 27 jan. 2023.

COX, I. J. *et al.* Secure spread spectrum watermarking for multimedia. **IEEE transactions on Image Processing**, v. 6, n. 12, p. 1673–1687, 1997. DOI: https://doi.org/10.1109/83.650120. Disponível em: https://ieeexplore.ieee.org/document/650120. Acesso em: 19 jan. 2023.

FERREIRA, W. D. **Detecção de imagens falsificadas baseada em descritores locais de textura e rede neural convolucional**. 151 p. Tese (Doutorado em Engenharia Elétrica e da Computação) — Universidade Federal de Goiás, Goiânia, 2020. Disponível em: http://repositorio.bc.ufg.br/tede/handle/tede/10824. Acesso em: 15 fev. 2023.

HEMACHANDRAN, K. Study of image steganography using lsb, dft and dwt. **International Journal of Computers & Technology**, Assam University, Silchar, v. 11, n. 5, p. 2618–2627, 2013. DOI: https://doi.org/10.24297/ijct.v11i5.1143. Disponível em: https://rajpub.com/index.php/ijct/article/view/1143. Acesso em: 07 abr. 2023.

HONDA, R. R. **Análise e Implementação de Algoritmos para Manipulação de Esteganografia em Imagens**. 55 p., 2011. Trabalho de Conclusão de Curso (Bacharelado em Ciencia da Computacao) – Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha de Marília, 2011. Disponível em: http://hdl.handle.net/11077/870. Acesso em: 8 dez. 2022.

JULIO, E. P. **Uma arquitetura de sistemas de detecção de intrusão em redes ad hoc sem fio usando esteganografia e mecanismos de reputação**. 2007. 104 p. Dissertação (Mestrado em Processamento Paralelo e Distríbuido) – Universidade Federal Fluminense, Niterói, 2007. Disponível em: https://app.uff.br/riuff/handle/1/17833. Acesso em: 14 dez. 2022.

KAWAGUCHI, E.; EASON, R. O. Principles and applications of bpcs steganography. **Proceedings of SPIE: Multimedia Systems and Applications**, Boston, Massachusetts, v. 3528, p. 464–472, 1998. DOI: https://doi.org/10.1117/12.337436. Disponível em: https://link.springer.com/chapter/10.1007/11554028_41. Acesso em: 12 nov. 2022.

KIM, H. Y. Marcas d'água frágeis de autenticação para imagens em tonalidade contínua e esteganografia para imagens binárias e meio-tom. **Revista de Informática Teórica e Aplicada**, Instituto de Informática da UFRGS, v. 10, n. 1, p. 97–125, 2003. Disponível em: https://www.inf.ufrgs.br/ revista/docs/rita10/rita_v10_n1_p97a125.pdf. Acesso em: 07 abr. 2023.

LI, B. *et al.* A survey on image steganography and steganalysis. **Journal of Information Hiding and Multimedia Signal Processing**, National Kaohsiung University of Applied Sciences, v. 2, n. 2, p. 142–172, 2011. Disponível em: https://www.researchgate.net/publication/228527555_A_survey_on_image_steganography_and_steganalysis. Acesso em: 01 fev. 2023.

LIU, L. *et al.* Median robust extended local binary pattern for texture classification. **IEEE Transactions on Image Processing:a publication of the IEEE Signal Processing Society**, v. 25, n. 3, p. 1368–1381, 2016. DOI: https://doi.org/10.1109/TCSVT.2019.2896270. Disponível em: https://ieeexplore.ieee.org/document/7393828. Acesso em: 14 fev. 2023.

LOPES, I. O. **Marca d'água digital: uma técnica para verificação de autenticidade ou proteção de direitos autorais**. 2006. 138 p. Dissertação (Mestrado em Ciências Exatas e da Terra) – Universidade Federal de Uberlândia, Uberlândia, 2006. Disponível em: https://repositorio.ufu.br/handle/123456789/12560. Acesso em: 07 jan. 2023.

LOPES, I. O. *et al.* Introdução à marca d'água digital. In: **XV Jornada de Matemática de Catalão**. Catalão - GO: Simpósio de Matemática, 2004. v. 1, p. 1–9. Disponível em: https://www.academia.edu/42005939/INTRODUÇAO_A_MARCA_DAGUA. Acesso em: 21 dez. 2022.

NUNES, S. L. P. **Marca d'água digital**: autenticação de imagens digitais. 54 p., 2008. Trabalho de Conclusão de Curso (Bacharelado em Ciencia da Computacao) — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: https://lume.ufrgs.br/handle/10183/16106. Acesso em: 11 dez. 2022.

ROCHA, J. C. Cor luz, cor pigmento e os sistemas rgb e cmyk. **Revista Belas Artes**, v. 2, n. 3, p. 1–19, 2010. Disponível em: https://www.belasartes.br/wp-content/uploads/2023/05/cor-luz-cor-pigmento-e-os-sistemas-rgb-e-cmy.pdf. Acesso em: 12 fev. 2023.

SANS, D. R. **Identificação de propriedade em imagens com marcas d'água no domínio da transformada wavelet**. 2008. 113 p. Dissertação (Mestrado em Informática) – Universidade Federal do Paraná, Curitiba, 2008. Disponível em: http://hdl.handle.net/1884/17768. Acesso em: 10 mar. 2023.

SCHENATTO, M. **Criptografia e esteganografia aplicadas em imagens médicas no padrão dicom**. 87 p., 2021. Trabalho de Conclusão de Curso (Bacharelado em Ciencia da Computacao) — Universidade de Caxias do Sul, Rio Grande do Sul, 2021. Disponível em: https://repositorio.ucs.br/11338/10012. Acesso em: 12 dez. 2022.

SILVA, J. F. **Inserção e extração de marca d'água em imagens digitais usando a transformada wavelet**. 140 p. Tese (Doutorado em Engenharia Elétrica) — Universidade Estadual Paulista Júlio de Mesquita Filho, Faculdade de Engenharia de Ilha Solteira, 2014. Disponível em: http://www.athena.biblioteca.unesp.br/exlibris/bd/cathedra/23-04-2015/000823589.pdf. Acesso em: 09 mar. 2023.

SUN, S. A new information hiding method based on improved bpcs steganography. **Advances in Multimedia**, Hindawi Limited London, UK, United Kingdom, v. 2015, p. 1–7, 2015. DOI: https://doi.org/10.1155/2015/698492. Disponível em: https://www.hindawi.com/journals/am/2015/698492/. Acesso em: 06 abr. 2023.

ANEXO A – MENSAGEM INSERIDA NA IMAGEM

Before the early 1960s, computers were mainly used for number-crunching rather than for text, and memory was extremely expensive. Computers often allocated only 6 bits for each character, permitting only 64 characters—assigning codes for A-Z, a-z, and 0-9 would leave only 2 codes: nowhere near enough. Most computers opted not to support lower-case letters. Thus, early text projects such as Roberto Busas Index Thomisticus, the Brown Corpus, and others had to resort to conventions such as keying an asterisk preceding letters actually intended to be upper-case. Fred Brooks of IBM argued strongly for going to 8-bit bytes, because someday people might want to process text; and won. Although IBM used EBCDIC, most text from then on came to be encoded in ASCII, using values from 0 to 31 for (non-printing) control characters, and values from 32 to 127 for graphic characters such as letters, digits, and punctuation. Most machines stored characters in 8 bits rather than 7, ignoring the remaining bit or using it as a checksum. The near-ubiquity of ASCII was a great help, but failed to address international and linguistic concerns. The dollar-sign was not as useful in England, and the accented characters used in Spanish, French, German, Portuguese, and many other languages were entirely unavailable in ASCII (not to mention characters used in Greek, Russian, and most Eastern languages). Many individuals, companies, and countries defined extra characters as needed—often reassigning control characters, or using values in the range from 128 to 255. Using values above 128 conflicts with using the 8th bit as a checksum, but the checksum usage gradually died out. These additional characters were encoded differently in different countries, making texts impossible to decode without figuring out the originators rules. For instance, a browser might display ¬A rather than if it tried to interpret one character set as another. The International Organization for Standardization (ISO) eventually developed several code pages under ISO 8859, to accommodate various languages. The first of these (ISO 8859-1) is also known as Latin-1, and covers the needs of most (not all) European languages that use Latin-based characters (there was not quite enough room to cover them all). ISO 2022 then provided conventions for switching between different character sets in mid-file. Many other organisations developed variations on these, and for many years Windows and Macintosh computers used incompatible variations. The text-encoding situation became more and more complex, leading to efforts by ISO and by the Unicode Consortium to develop a single, unified character encoding that could cover all known (or at least all currently known) languages. After some conflict,[citation needed] these efforts were unified. Unicode currently allows for 1,114,112 code values, and assigns codes covering nearly

all modern text writing systems, as well as many historical ones, and for many non-linguistic characters such as printers dingbats, mathematical symbols, etc. Text is considered plain text regardless of its encoding. To properly understand or process it the recipient must know (or be able to figure out) what encoding was used; however, they need not know anything about the computer architecture that was used, or about the binary structures defined by whatever program (if any) created the data. Perhaps the most common way of explicitly stating the specific encoding of plain text is with a MIME type. For email and HTTP, the default MIME type is text/plain – plain text without markup. Another MIME type often used in both email and HTTP is text/html; charset=UTF-8 – plain text represented using the UTF-8 character encoding with HTML markup. Another common MIME type is application/json – plain text represented using the UTF-8 character encoding with JSON markup. When a document is received without any explicit indication of the character encoding, some applications use charset detection to attempt to guess what encoding was used.