

UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
CURSO DE CIÊNCIA DA COMPUTAÇÃO

JOÃO PAULO DE FREITAS COSTA SILVA

CRIPTOGRAFIA E ESTEGANOGRAFIA APLICADAS A IMAGENS DIGITAIS

MOSSORÓ – RN
2017

JOÃO PAULO DE FREITAS COSTA SILVA

CRIPTOGRAFIA E ESTEGANOGRAFIA APLICADAS A IMAGENS DIGITAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Ciência da Computação da Universidade Federal Rural do Semi-Árido como requisito para a obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Leandro Carlos de Souza

Coorientadora: Prof.ª Mª. Flávia Estélia Silva Coelho

MOSSORÓ-RN

2017

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei n° 9.279/1996 e Direitos Autorais: Lei n° 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos.

S586c Silva, João Paulo de Freitas Costa.
Criptografia e esteganografia aplicadas a imagens digitais / João Paulo de Freitas Costa Silva. - 2017.
98 f. : il.

Orientador: Leandro Carlos de Souza.
Coorientadora: Flávia Estélia Silva Coelho.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Ciência da Computação, 2017.

1. LSB com Rejeição. 2. LSB Matching. 3. LSB Replacement. 4. Esteganografia. 5. Criptografia. I. Souza, Leandro Carlos de, orient. II. Coelho, Flávia Estélia Silva, co-orient. III. Título.

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC´s) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

JOÃO PAULO DE FREITAS COSTA SILVA

CRIPTOGRAFIA E ESTEGANOGRAFIA APLICADAS A IMAGENS DIGITAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Ciência da Computação da Universidade Federal Rural do Semi-Árido como requisito para a obtenção do grau de Bacharel em Ciência da Computação.

APROVADO EM: 22/05/2017

BANCA EXAMINADORA:

Leandro Carlos de Souza

Prof. Dr. Leandro Carlos de Souza – UFERSA.
Presidente

Flávia Coelho

Prof.ª Ma. Flávia Estélia Silva Coelho – UFERSA.
1º Membro

Paulo Gabriel Gadelha Queiroz

Prof. Dr. Paulo Gabriel Gadelha Queiroz – UFERSA.
2º Membro

Matheus Menezes

Prof. Dr. Matheus da Silva Menezes – UFERSA.
3º Membro

RESUMO

O Processamento Digital de Imagens, a Criptografia e a Esteganografia podem ser combinados para garantir a confidencialidade de informações. Este trabalho propõe um processo para acrescentar confidencialidade à informações sigilosas, dispostas sob a forma de imagens digitais. O processo para acrescentar confidencialidade é composto por duas etapas. A primeira é criptografar a imagem. A segunda é aplicar a esteganografia. O Método do *Bit* Menos Significativo com Rejeição (LSBR) é uma técnica composta por um algoritmo de criptografia de imagens digitais e um algoritmo de esteganografia, em que busca-se que informações dispostas sob a forma de imagens possam ser camufladas em outras imagens. Os objetivos principais deste trabalho são apresentar o LSBR como uma proposta de esteganografia para imagens digitais, além de realizar um comparativo entre essa técnica e os métodos LSB *Replacement* e LSB *Matching*. Para a comparação entre esses métodos foi realizado um conjunto de testes, nos quais foram avaliadas métricas de qualidade para imagens digitais, como MSE, PSNR e Entropia. Foi utilizado um banco de imagens para a obtenção das imagens que participaram dos testes e essas imagens foram separadas nos conjuntos de imagens de cobertura e imagens secretas. Cada teste foi feito aplicando-se os métodos em análise, realizando-se a incorporação de imagens de um grupo em imagens do outro. Em seguida foram comparados os resultados dos testes. O método LSBR mostrou-se superior aos outros dois métodos na avaliação perceptual de histograma e na análise de entropias, além de apresentar bons resultados para a análise de PSNR.

Palavras-chave: LSB com Rejeição. LSB *Matching*. LSB *Replacement*. Esteganografia. Criptografia.

ABSTRACT

Digital Image Processing, Encryption and Steganography can be combined to ensure the confidentiality of information. This paper proposes a process to add confidentiality to confidential information, arranged in the form of digital images. The process for adding confidentiality consists of two steps. The first is to encrypt the image. The second is to apply steganography. The Least Significant Bit Method with Rejection (LSBR) is a technique composed by a digital image encryption algorithm and a steganography algorithm, in which information arranged in the form of images can be camouflaged in other images. The main objectives of this work are to present the LSBR as a proposal of steganography for digital images, besides comparing this technique with the LSB Replacement and LSB Matching methods. In order to compare these methods, a set of tests was performed, in which quality metrics for digital images such as MSE, PSNR and Entropy were evaluated. A repository was used to obtain the images that participated in the tests and these images were separated into the sets of cover images and secret images. Each test was performed by applying the methods under analysis, incorporating images of one group into images of the other. The results of each of the tests were then compared. The LSBR method proved to be superior to the other two methods in the histogram perceptual evaluation and in the entropy analysis, besides presenting good results for the PSNR analysis.

Key words: LSB with Rejection. LSB Matching. LSB Replacement. Steganography. Encryption.

LISTA DE FIGURAS

Figura 1 – Representação Matricial de uma imagem digital……...16
Figura 2 – Imagem em escala de cinza e imagem separada em bandas RGB…….17
Figura 3 – Composição de uma imagem colorida…….17
Figura 4 – Amostragem……....18
Figura 5 – Quantização…….18
Figura 6 – Representação do esquema de cores RGB…….19
Figura 7 – Esquema de criptografia…….20
Figura 8 – Processo de cifragem por transposição……...21
Figura 9 – Aplicação da Cifra de César……....21
Figura 10 – Processo de cifragem por Vigenère……...23
Figura 11 – Processo de esteganografia……....25
Figura 12 – Esquema para transmissão de dados secretos……25
Figura 13 – Funcionamento do LSB *Replacement*……..27
Figura 14 – Funcionamento do LSB *Matching*……..28
Figura 15 – Sequência seguida pela criptografia do LSBR……..33
Figura 16 – Processo de inversão em espiral……....36
Figura 17 – Manipulação de submatrizes…….37
Figura 18 – Matriz de intensidades vetorizada e vetor com posições aleatórias…….38
Figura 19 – Novo vetor de intensidades após aleatorização……....39
Figura 20 – Processo de cifragem de Vigenère…….41
Figura 21 – Processo reverso de criptografia……....42
Figura 22 – Local de incorporação de *bits* pelo LSBR…….44
Figura 23 – Processo de ocultação do LSBR para sequências equivalentes…….45
Figura 24 – Processo de ocultação do LSBR para sequências não equivalentes……..46
Figura 25 – Variabilidade nos *bits* menos significativos……...47
Figura 26 – Procedimento geral de esteganografia do LSBR……...50
Figura 27 – Processo reverso da esteganografia baseada no LSBR…….52
Figura 28 – Procedimento global para ocultação de imagens pelo LSBR……....53
Figura 29 – Procedimento global para extração de imagens pelo LSBR……..54
Figura 30 – Imagem extraída sem ser decriptada…….54
Figura 31 – Metodologia de testes……....55
Figura 32 – Conjunto de imagens de Cobertura……..56

Figura 33 – Conjunto de imagens secretas……....56
Figura 34 – Imagens e seus histogramas……..….60
Figura 35 – Anomalias na distribuição de frequências……...…..61
Figura 36 – Imagens usadas no teste 1……..62
Figura 37 – Estego-imagens geradas……...….63
Figura 38 – Imagens secretas extraídas……....63
Figura 39 – Histograma da imagem original X Histograma das estego-imagens……64
Figura 40 – Valor da diferença entre imagens originais e estego-imagens……..66
Figura 41 – Imagens usadas no teste 2……..68
Figura 42 – Estego-imagens geradas……..….68
Figura 43 – Imagens secretas extraídas……....69
Figura 44 – Histograma da imagem original X Histograma das estego-imagens……....70
Figura 45 – Valor da diferença entre imagens originais e estego-imagens……..71
Figura 46 – Imagens utilizadas no teste 3……73
Figura 47 – Estego-imagens geradas……....74
Figura 48 – Imagens secretas extraídas……....74
Figura 49 – Histograma da imagem original X Histograma das estego-imagens……75
Figura 50 – Valor da diferença entre imagens originais e estego-imagens…….….77
Figura 51 – Imagens utilizadas no teste 4……79
Figura 52 – Estego-imagens geradas……....79
Figura 53 – Imagens secretas extraídas……80
Figura 54 – Histograma da imagem original X Histograma das estego-imagens……....80
Figura 55 – Valor da diferença entre imagens originais e estego-imagens……..82
Figura 56 – Imagens utilizadas no teste 5……84
Figura 57 – Estego-imagens geradas……....84
Figura 58 – Imagens secretas extraídas……85
Figura 59 – Histograma da imagem original X Histograma das estego-imagens……86
Figura 60 – Valor da diferença entre imagens originais e estego-imagens……..87

LISTA DE TABELAS

Tabela 1 – Métricas obtidas (Teste 1)……...…….....67
Tabela 2 – Métricas obtidas (Teste 2)……...…….....72
Tabela 3 – Métricas obtidas (Teste 3)……...…….....78
Tabela 4 – Métricas obtidas (Teste 4)……...…….....83
Tabela 5 – Métricas obtidas (Teste 5)……...…….....88

LISTA DE QUADROS

Quadro 1 – Tabela de Vigenère…….22
Quadro 2 – Possível correspondência entre a Tabela ASCII e o conjunto C para N = 3…….34
Quadro 3 – Tabela de Vigenère adaptada…….40
Quadro 4 – Métrica MOS…….59
Quadro 5 – Relação entre o PSNR e a métrica MOS……...59

SUMÁRIO

1 INTRODUÇÃO……...……...…11

1.1 PROBLEMA……...…12

1.2 OBJETIVOS…….....12

1.3 JUSTIFICATIVA…….…13

1.4 ORGANIZAÇÃO…….....13

2 REFERENCIAL TEÓRICO……15

2.1 PROCESSAMENTO DIGITAL DE IMAGENS…….....15

2.1.1 Representação das imagens digitais……15

2.1.2 Sistema de cor *Red*, *Green*, *Blue*……..……..18

2.2 CRIPTOGRAFIA…….....19

2.3 ESTEGANOGRAFIA…….....23

2.3.1 O método do *bit* menos significativo…….....26

2.3.2 O método do *bit* menos significativo com realocação……26

2.3.3 O método do *bit* menos significativo com correspondência……...27

2.3.4 O método do *bit* menos significativo com correspondência revisitada…….....28

2.4 TRABALHOS CORRELATOS……..29

3 CRIPTOGRAFIA E ESTEGANOGRAFIA BASEADA NO *BIT* MENOS SIGNIFICATIVO COM REJEIÇÃO……..32

3.1 CRIPTOGRAFIA……...….32

3.1.1 Geração da chave de vigenère…….….33

3.1.2 Geração da semente…….……..35

3.1.3 Inversão em espiral…….……...….36

3.1.4 Manipulação de submatrizes……36

3.1.5 Aleatorização……..38

3.1.6 Cifragem de vigenère…….....39

3.1.7 Processo reverso de criptografia……..42

3.2 ESTEGANOGRAFIA…….....43

3.2.1 Processo de esteganografia baseada no LSBR…….....48

3.2.2 Processo reverso de esteganografia baseada no LSBR……..51

3.3 VISÃO GLOBAL…….....53

4 METODOLOGIA...……...55
4.1 MÉTRICAS DE AVALIAÇÃO……..….57
4.1.1 Entropia (Entropia de Shannon)……..57
4.1.2 *Mean squared error* (MSE)……...58
4.1.3 *Peak Signal-to-Noise Ratio* (PSNR)……..58
4.2 AVALIAÇÃO PERCEPTUAL……....59

5 RESULTADOS……..…….62
5.1 CONFIGURAÇÃO DE TESTE 1……...62
5.2 CONFIGURAÇÃO DE TESTE 2……...68
5.3 CONFIGURAÇÃO DE TESTE 3……...73
5.4 CONFIGURAÇÃO DE TESTE 4……...78
5.5 CONFIGURAÇÃO DE TESTE 5……...84
5.6 DISCUSSÃO DOS RESULTADOS……....89

6 CONCLUSÃO E TRABALHOS FUTUROS……...92

REFERÊNCIAS……..94

1 INTRODUÇÃO

O Processamento Digital de Imagens (PDI) visa o processamento de imagens digitais com o propósito de gerar outra imagem digital modificada. Esta área envolve aplicações e técnicas de filtragem, como suavização e aguçamento, reconhecimento de padrões e manipulações gerais de imagens digitais (GONZALEZ; WOODS, 2010).

Com a popularização da *Internet*, surge a necessidade de proteção de informações que transitam na rede. Segundo Cert.br (2017), somente entre 2011 e 2015, foram reportados um total de 2.987.705 incidentes de segurança em computadores. Esses incidentes incluem ataques *Denial of Service* (DoS), invasões, ataques *Web*, varreduras em computadores, fraudes na *Internet*, entre outros.

Esse cenário de insegurança na internet demonstra a necessidade por haver medidas que proporcionem segurança aos usuários da rede. Segundo Rocha *et al*. (2004), a criptografia, em conjunto com a esteganografia, apresenta-se como uma tecnologia capaz de permitir que as pessoas aumentem sua privacidade on-line.

O PDI, a criptografia e a esteganografia podem ser combinados para garantir a confidencialidade de informações. A criptografia tem o propósito de tornar o conteúdo de uma mensagem secreto, de forma que pessoas não autorizadas a ter acesso a esse conteúdo o tenham. A esteganografia visa tornar oculta a existência de uma mensagem, de forma que não seja possível perceber a existência dessa mensagem, exceto para o emissor e o destinatário. Um procedimento utilizado para esse fim é manipular os *pixels* das imagens em nível de *bits*. Esse procedimento pode fundir duas imagens, utilizando *bits* de cada uma, em uma terceira imagem. Essa terceira imagem seria uma imagem híbrida, composta por *bits* das duas imagens usadas na codificação.

O processo para acrescentar confidencialidade é composto por duas etapas. A primeira é criptografar a imagem. A segunda é aplicar a esteganografia. Assim, este projeto visa aplicar com os conceitos de PDI aliados à criptografia e à esteganografia em um contexto em que se busca proporcionar confidencialidade às informações presentes em imagens. O método proposto baseia-se na incorporação de dados encriptados de uma imagem à outra, por meio de um processo de esteganografia. O método apresenta como vantagem a possibilidade de incorporação de um a sete *bits* por *pixel* da imagem usada para os deixar encobertos, realizando a modificação de apenas um *bit* por *pixel*.

1.1 PROBLEMA

A exposição à *Web*, programas maliciosos, invasões a computadores, entre outros problemas, proporciona insegurança a quem possui informações que precisam estar no meio digital. O motivo dessa insegurança deve-se ao fato de que essas informações não podem cair em mãos erradas, de forma não autorizada, em um ambiente no qual o número de ataques a sistemas computacionais, visando o roubo de informações ou causar quaisquer tipos de danos tem crescido.

A segurança da informação sugere três metas, quais sejam: confidencialidade, integridade e disponibilidade. A primeira meta é muito comum no contexto da segurança da informação, pois trata não apenas da aplicação no armazenamento, mas também à transmissão de informações, pois é necessário ocultá-las durante a transmissão (FOROUZAN; MOSHARRAF, 2013). Para Goodrich e Tamassia (2013), manter a informação secreta é muitas vezes a essência da segurança de informação.

Considerando o problema do número crescente de ataques digitais e a necessidade de proteção de informações, o problema abordado por este trabalho é resumido em um questionamento: como proporcionar confidencialidade às informações presentes em imagens?

1.2 OBJETIVOS

O objetivo do projeto é desenvolver um método que possibilite aplicar confidencialidade ao armazenamento e compartilhamento de informações dispostas sob a forma de imagens, mantendo a qualidade visual das imagens processadas semelhante à qualidade das imagens originais. Como objetivo geral, busca-se desenvolver um método que permita que informações dispostas sob a forma de imagens possam ser camuflados em outro conjunto de dados, também dispostos sob a forma de imagem. Busca-se comparar os resultados atingidos em testes pelo método proposto com os obtidos pelos métodos LSB *Matching* e LSB *Replacement*. Como objetivos principais do trabalho, tem-se:

- Realizar avaliação perceptual da qualidade visual das imagens originais e as geradas por meio de criptografia e esteganografia pelos métodos em análise;
- Realizar avaliação perceptual da distribuição de frequências das imagens originais e as geradas por meio de criptografia e esteganografia pelos métodos em análise;

- Encontrar medidas de desempenho para os métodos em análise, considerando os testes realizados, por meio de métricas de qualidade de imagens como MSE, PSNR e Entropia;
- Realizar um comparativo entre o método de criptografia e esteganografia proposto e dois outros métodos que trabalham com o plano do *bit* menos significativo, o LSB *Matching* e o LSB *Replacement*.

1.3 JUSTIFICATIVA

Este trabalho possui como motivação para seu desenvolvimento a necessidade de proporcionar confidencialidade à informações em comunicações na *Internet*. Com a expansão da *Internet*, o número de ataques que visam o roubo de informações ou espionagem tem crescido substancialmente. Isto faz com que seja necessário desenvolver métodos de proteção da informação. O método proposto contribui para a proteção contra esses riscos, proporcionando uma maneira de tornar confidenciais as informações presentes em imagens.

O método proposto realiza o tratamento seguro de informações, pois tem seu desenvolvimento baseado no PDI em conjunto com a criptografia e esteganografia. O PDI auxilia na realização da esteganografia manipulando a imagem para permitir a aplicação das técnicas esteganográficas. A criptografia dos componentes da imagem permite que caso haja uma quebra da esteganografia, a informação oculta na imagem esteja ininteligível.

1.4 ORGANIZAÇÃO

Além deste capítulo introdutório, neste trabalho são apresentados outros cinco capítulos:

- **Capítulo 2 – Referencial Teórico:** Neste capítulo são apresentados os conceitos básicos necessários para a compreensão do trabalho. São apresentados conceitos sobre PDI, além de mostrado como uma imagem digital é representada. Conceitos sobre sistemas de cores são apresentados. Conceitos sobre criptografia são apresentados, além da Cifra de Vigenère. Conceitos sobre esteganografia também são apresentados, além de métodos esteganográficos comuns.

- **Capítulo 3 – Criptografia e Esteganografia baseada no *bit* menos significativo com rejeição:** Neste capítulo é apresentado o funcionamento do método proposto, considerando as etapas de criptografia e esteganografia pertencentes a ele.
- **Capítulo 4 – Metodologia:** Neste capítulo é apresentada a metodologia adotada no trabalho para a realização dos testes. São apresentadas as definições de métricas utilizadas na avaliação da qualidade de imagens, como MSE, PSNR e Entropia. Além disso, a avaliação perceptual de histogramas é introduzida.
- **Capítulo 5 – Resultados:** Neste capítulo são apresentados os testes realizados. Em cada teste foi realizada a comparação do método de esteganografia proposto com os métodos do *bit* menos significativo com realocação e o método do *bit* menos significativo com correspondência.
- **Capítulo 6 – Conclusões e trabalhos futuros:** Neste capítulo são apresentadas conclusões acerca dos testes realizados e faz apontamentos para a realização de trabalhos futuros.

2 REFERENCIAL TEÓRICO

O referencial teórico necessário para a compreensão do método desenvolvido neste trabalho é apresentado neste capítulo. São apresentados conceitos relativos ao PDI, à representação de imagens digitais e sistemas de cores. Além disso, são apresentados conceitos sobre criptografia e esteganografia.

2.1 PROCESSAMENTO DIGITAL DE IMAGENS

O interesse no PDI vem da busca por melhora em informações visuais para a interpretação humana e processamento de dados de imagens para o seu tratamento automático por máquinas (GONZALEZ; WOODS, 2010). O PDI é um conjunto de técnicas para a manipulação de imagens digitais com o objetivo de facilitar a extração de informações. Esse conjunto de técnicas é capaz de processar imagens monocromáticas e multiespectrais, cuja representação é feita em várias faixas do espectro (IBGE, 2001).

Gonzalez e Woods (2010) definem o PDI como o processamento de imagens digitais por um computador digital. Esse processamento pode ser entendido como a manipulação de imagens por meio de métodos de processamento. Embora as formas de manipulação de imagens sejam praticamente infinitas, elas podem ser classificadas nos seguintes grupos (QUEIROZ, 2003):

- Retificação e Restauração de Imagens;
- Realçamento de Imagens;
- Classificação de Imagens;
- Combinação de Dados (*data merging*).

Algumas das aplicações do processamento de imagens são a medicina nuclear, astronomia, angiografia, inspeção industrial, microscopia, sensoriamento remoto, previsão do tempo, entre outras (GONZALEZ; WOODS, 2010).

2.1.1 Representação das imagens digitais

Uma imagem é definida como uma função bidimensional $f(x,y)$, em que x e y são coordenadas espaciais no plano e a amplitude de f em qualquer ponto (x,y) é chamada de

intensidade ou nível de cinza da imagem nesse ponto. Cada ponto *(x,y)* é chamado de *pixel.* Um *pixel* é a menor unidade representativa de uma imagem, e uma imagem digital possui uma quantidade inteira de *pixels* (GONZALEZ; WOODS, 2010).

A representação de uma imagem digital pode então ser feita por uma matriz como na Figura 1,

Figura 1 – Representação Matricial de uma imagem digital.

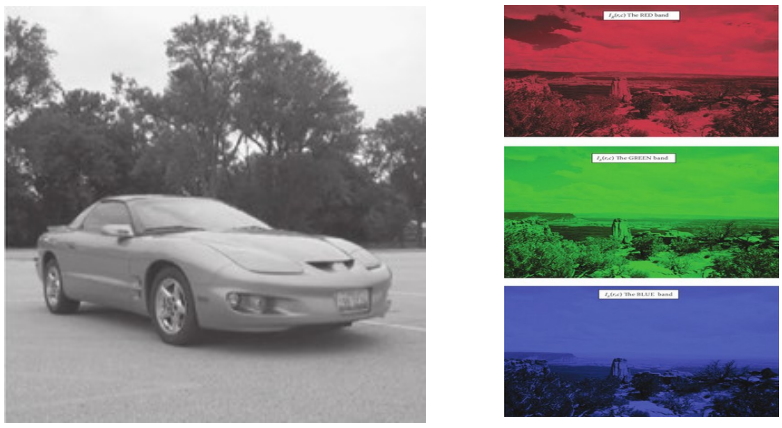
$$f(x,y) = \underbrace{\left.\begin{bmatrix} 43 & 44 & 46 & \dots & 42 & 42 \\ 44 & 44 & 44 & \dots & 39 & 39 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 89 & 91 & 91 & \dots & 30 & 33 \end{bmatrix}\right\}_{h=384}}_{w=512}$$

Fonte: Oliveira (2016).

em que w e h são a largura e altura da imagem, respectivamente, e cada elemento da matriz representa a intensidade ou cor do *pixel*.

Além de outros tipos, existem imagens em escala de cinza e imagens coloridas. As imagens em escala de cinza possuem apenas informação de brilho, de forma que o número de *bits* usados por *pixel* definem o número de níveis de brilho disponíveis. Já as imagens coloridas podem ser modeladas como a união de imagens monocromáticas divididas em três bandas, cada uma representando uma cor. Essas cores são o vermelho (R), o verde (G) e o azul (B), formando as imagens RGB (UMBAUGH, 2010). Um exemplo de imagem em escala de cinza e uma imagem separada nas suas bandas R, G e B é ilustrado na Figura 2.

Figura 2 – Imagem em escala de cinza e imagem separada em bandas RGB.

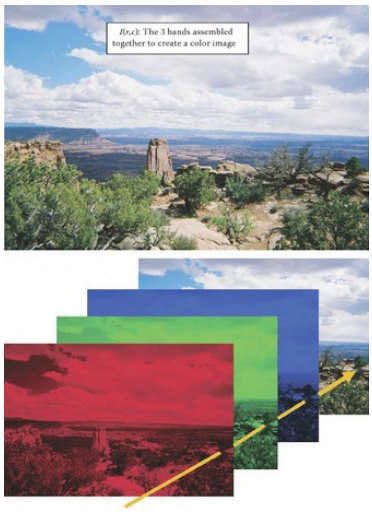


(a) Escala de cinza (b) Bandas RGB

Fonte: Umbaugh (2010).

A união das três bandas de cor pode criar uma única imagem colorida, como é visto na Figura 3. A seta indica que um *pixel* de uma imagem colorida é composto pelas informações das três bandas de cor (R, G e B).

Figura 3 – Composição de uma imagem colorida.

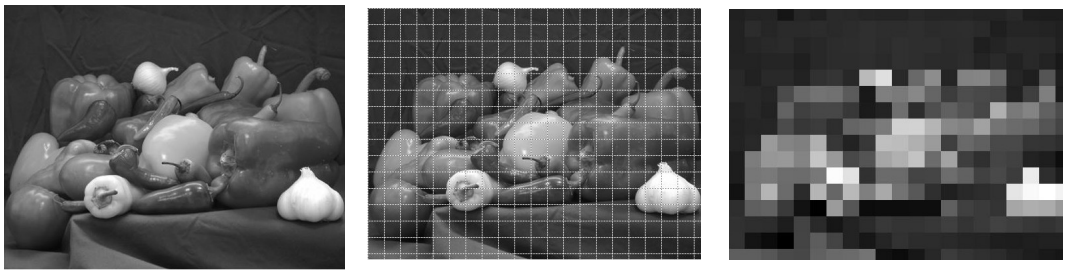


Fonte: Umbaugh (2010).

Para que uma imagem seja convertida em formato digital, é necessário que haja uma digitalização sobre a imagem real, sobre ambas as coordenadas e na amplitude. Chama-se amostragem o processo de representação digital das coordenadas e chama-se quantização o processo de representação digital das amplitudes das amostras (THYAGARAJAN, 2011). As

amostras são os *pixels* e as amplitudes das amostras são os níveis de intensidade dos *pixels*. O processo de amostragem é representado na Figura 4.

Figura 4 – Amostragem.

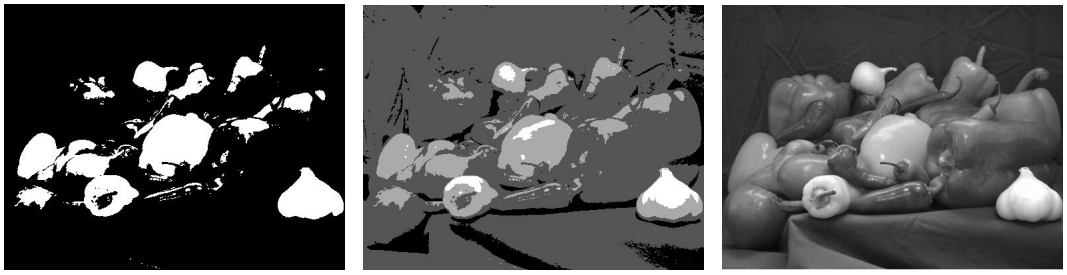


(a) Imagem contínua (b) Grid de amostragem (c) Imagem amostrada

Fonte: Oliveira (2016).

A amostragem determina as dimensões da imagem em *pixels*, que é a menor divisão da imagem. A quantização de imagens é ilustrada na Figura 5.

Figura 5 – Quantização.



(a) Quantização com 1 *bit* (b) Quantização com 2 *bits* (c) Quantização com 8 *bits*

Fonte: Oliveira (2016).

A quantização define o nível de representação de cores por *pixel*, de forma que quanto maior o nível da quantização, mais níveis de cor podem ser representados por *pixel*.

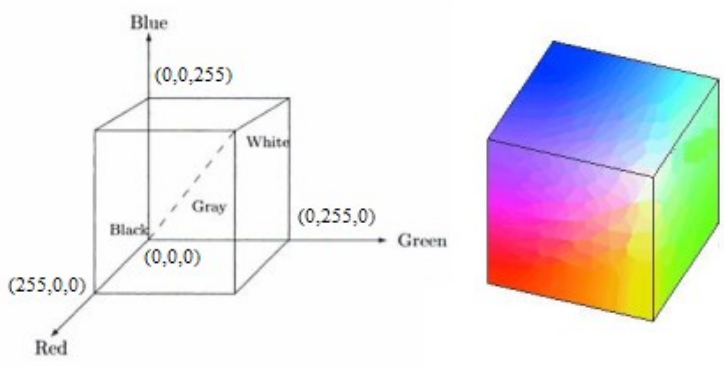
2.1.2 Sistema de cor *Red*, *Green*, *Blue*

A finalidade de um modelo de cores ou espaço de cores, é tornar mais fácil a representação de cores em uma forma padrão, de ampla aceitação. Um modelo de cor é representado por sistema de coordenadas e um subespaço dentro desse sistema, no qual cada cor é representada por um ponto único. Em termos de processamento digital de imagens, os

modelos mais utilizados na atualidade são o RGB, o CMY, o CMYK e o HSI (GONZALEZ; WOODS, 2010).

O sistema de cores do modelo RGB é representado, por meio do cubo RGB, na Figura 6.

Figura 6 – Representação do esquema de cores RGB.



Fonte: adaptado de Alves (2010).

Os valores das dimensões desse cubo são as intensidades de cor e estão no intervalo *I = [0, 255]*. O vértice sobre a origem (0, 0, 0) representa o preto, o vértice (255, 0, 0) representa o vermelho, o vértice (0, 255, 0) representa o verde, o vértice (0, 0, 255) representa o azul e o vértice (255, 255, 255) representa o branco. Todas as outras cores são representadas por pontos únicos nesse cubo, ou seja, por combinações das intensidades dos componentes R, G e B. Imagens em tons de cinza são representadas por pontos ao longo da diagonal principal, a partir da origem. Isto significa que imagens em tons de cinza possuem o mesmo valor para as componentes R, G e B (ALVES, 2010).

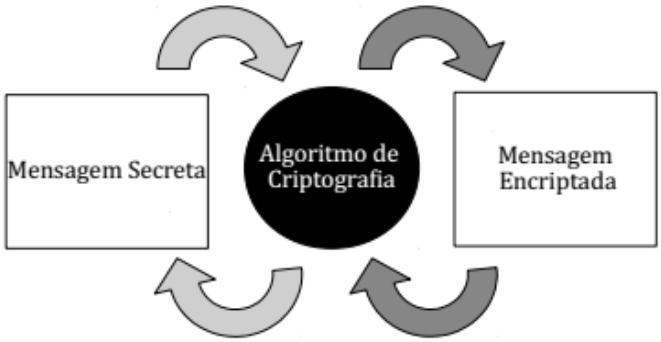
Em uma imagem com cores de 24 *bits*, cada *pixel* é representado por três *bytes*, cada um representando um canal de cor. Como cada *byte* pode representar 256 valores ou níveis de cores diferentes, cada *pixel* pode ter até 16,777,216 cores diferentes (LI; DREW; LIU, 2014).

2.2 CRIPTOGRAFIA

A criptografia é derivada da palavra grega *kriptos*, cujo significado é oculto, escondido. No entanto, a finalidade da criptografia não é fazer com que a existência de uma mensagem se torne oculta, mas sim o seu significado. O processo de ocultação do significado de uma mensagem é denominado encriptação (MARQUES, 2013). Goodrich e Tamassia (2013) descrevem a encriptação como uma forma de fazer com que dois participantes de uma

comunicação estabeleçam uma comunicação confidencial por um canal desprovido de segurança e sujeito a intromissões. Um esquema de criptografia é ilustrado pela Figura 7.

Figura 7 – Esquema de criptografia.



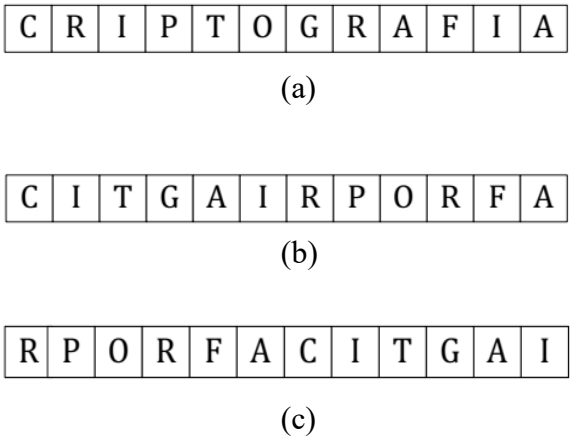
Fonte: autoria própria (2017).

De acordo com a Figura 7, a aplicação de um algoritmo de criptografia a uma mensagem secreta a transforma em mensagem cifrada, também sendo possível decifrar essa mensagem por meio do algoritmo.

Um processo de encriptação transforma a mensagem secreta em uma mensagem sob a forma de cifras, que são definidas por alguma forma de substituição de símbolos, em que um símbolo de uma mensagem é substituído por outro, de uma forma conhecida entre o emissor e o receptor (CRUZ, 2009). A definição do conceito e tipos de cifras faz-se necessária, pois este conceito é utilizado pelo algoritmo de criptografia proposto. A criptografia e todas as suas técnicas são baseadas nas técnicas de transposição e substituição (STALLINGS, 2008).

As cifras de transposição consistem na reorganização dos símbolos dentro da mensagem, de forma que esses símbolos permanecem inalterados, apenas trocando de posição entre si (CRUZ, 2009). Um processo de cifragem por transposição é ilustrado pela Figura 8.

Figura 8 – Processo de cifragem por transposição.



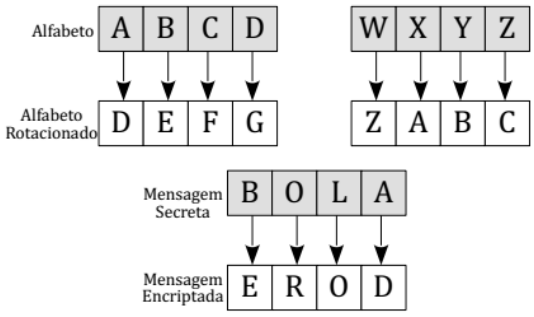
Fonte: autoria própria (2017).

Na Figura 8 (a) tem-se a palavra secreta CRIPTOGRAFIA. Em (b) tem-se o anagrama gerado pela cifra de transposição que escreve em ordem na cifra os símbolos de posição ímpar na palavra secreta e depois os de posições pares. Em (c) tem-se o anagrama gerado pela mesma cifra, mas agora os símbolos de posições pares são escritos primeiro.

Uma cifra de substituição é uma técnica em que símbolos do texto claro (mensagem original) são substituídos por outros símbolos (STALLINGS, 2008). Entre as cifras de substituição estão as cifras monoalfabéticas e as polialfabéticas (CRUZ, 2009).

A cifra de César é uma cifra monoalfabética. Ela consiste em criar um alfabeto alternativo, no qual a sequência de símbolos é definida pela rotação do alfabeto original em um determinado número. Com uma rotação de 1, por exemplo, a sequência ABCDE passaria a ser BCDEA, pois pela posição, A corresponde a B no novo alfabeto, e assim por diante. O mesmo raciocínio é estendido para outros valores de rotação. A aplicação de uma cifra de César com alfabeto rotacionado em 3 é ilustrada pela Figura 9.

Figura 9 – Aplicação da Cifra de César.



Fonte: autoria própria (2017).

A cifra de César é usada como base para uma cifra polialfabética, a Cifra de Vigenère, sendo que esta é composta por uma sequência daquelas com diferentes deslocamentos. O conceito de Cifra de Vigenère foi diretamente aplicado ao algoritmo de criptografia proposto.

A Cifra de Vigenère é polialfabética, de forma que uma letra do texto a ser cifrado pode ser trocada por várias letras diferentes. Isto evita que a mensagem sofra um ataque por meio da análise de frequências de letras. Por isso, diferentes alfabetos de cifra são utilizados (FIARRESGA, 2010).

Para cada letra do texto original há 26 possibilidades de troca, dependendo da letra de uma palavra-chave em análise. A Tabela de Vigenère pode ser vista no Quadro 1.

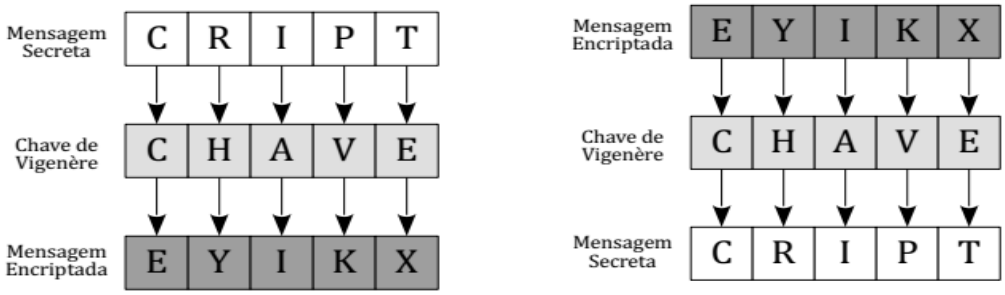
Quadro 1 – Tabela de Vigenère.

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

Fonte: Bonfim (2017).

No Quadro 1, a primeira linha e a primeira coluna são especiais. A primeira linha indica as letras da mensagem que deve ser cifrada e a primeira coluna indica as letras da chave usada. No processo de cifragem, a mensagem é dividida em blocos do tamanho da chave. Para cada bloco da palavra a ser cifrada, cada letra é substituída pela letra existente na interseção da coluna representada pela letra da palavra secreta com a linha representada pela letra da palavra-chave correspondente. O processo de cifragem da palavra CRIPT utilizando a palavra-chave CHAVE é ilustrado pela Figura 10.

Figura 10 – Processo de cifragem por Vigenère.



(a) Processo de cifragem (b) Processo de decifragem

Fonte: autoria própria (2017).

Na Figura 10 (a) ocorre o processo de cifragem. Em (b), ocorre o processo de deciframento. Para decifrar uma palavra cifrada, deve ser feita a correspondência de cada letra sua com a letra na posição correspondente da palavra-chave. Primeiro encontra-se em que coluna a letra cifrada está, dentro da linha da letra chave. Em seguida, a letra que representar a coluna da letra cifrada será a letra decifrada.

2.3 ESTEGANOGRAFIA

Desde o surgimento da internet a segurança da informação tem sido um ponto da Tecnologia da Informação e comunicação. Com o intuito de manter o segredo da comunicação, a criptografia foi criada para criptografar e descriptografar dados secretos. Nem sempre se deseja manter apenas o conteúdo de uma mensagem em segredo, pois muitas vezes é preciso manter a própria existência da mensagem em segredo. A esteganografia é responsável por manter a existência de uma mensagem em segredo (MORKEL; ELOFF; OLIVIER, 2005).

A transmissão de uma mensagem pode sofrer ameaças, como interceptação (em que alguém a lê durante a transmissão), alteração de seu conteúdo, fabricação (em que uma mensagem falsa poderia ser criada) e interrupção (em que a mensagem não chega a seu destino). A criptografia pode proteger uma mensagem das três primeiras ameaças relatadas, mas não da quarta. Para sanar essa deficiência, ocorreu aos poucos o surgimento da esteganografia (OLIVEIRA, 2007).

A esteganografia é uma arte que tem como objetivo ocultar informações, por meio de métodos e técnicas, visando o alcance de uma comunicação em segredo. Esta arte busca

incorporar uma mensagem confidencial dentro de outra de tal forma que a alteração da mensagem portadora não seja perceptível (PETRI, 2004).

Para Gil *et al*. (2008), esteganografia (do grego “escrita escondida”) é uma técnica que busca esconder informações de maneira que ninguém, a não ser o seu criador e o destinatário possam ao menos notar a existência dessas informações.

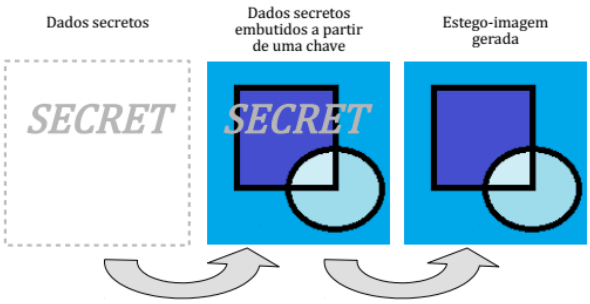
A diferença entre esteganografia e criptografia reside na forma de ocultação de dados secretos. Ao passo que a esteganografia esconde a existência da mensagem que contém os dados secretos, a criptografia torna essa mensagem ininteligível por meio de transformações na mensagem (STALLINGS, 2008).

A desvantagem da esteganografia é que no momento em que uma mensagem secreta é descoberta, essa técnica falhou em seu objetivo. A desvantagem da criptografia é que ela sugere um tráfego de informações como importante, podendo identificar um dos envolvidos como alguém que tem algo a esconder. Uma alternativa para barrar essas desvantagens é criptografar uma mensagem e só então escondê-la por meio da esteganografia (STALLINGS, 2008). Essa ação faz com que não se perceba que há algum dado importante envolvido em troca ou armazenamento de informações e caso isso seja detectado, eles estarão seguros.

É importante que alguns termos existentes no processo de esteganografia sejam conhecidos. O dado embutido (*embedded data*) é uma informação que se deseja manter em segredo. Este dado é escondido em uma mensagem conhecida como mensagem de cobertura (*cover-message*). As mensagens de cobertura podem ser chamadas de imagem de cobertura, áudio de cobertura ou texto de cobertura, a depender da mídia que as representa. Após o processo de ocultação, é obtido o estego-objeto (*stego-object*), que é uma mensagem de menos importância portando dados secretos. Uma estego-chave (*stego-key*) é utilizada para controlar o processo de ocultamento, restringindo a descoberta dos dados ocultos (ROCHA, 2003).

O processo de esteganografia com esses objetos é ilustrado na Figura 11, em que um dado secreto é embutido em uma imagem de cobertura a partir de uma estego-chave, gerando uma estego-imagem.

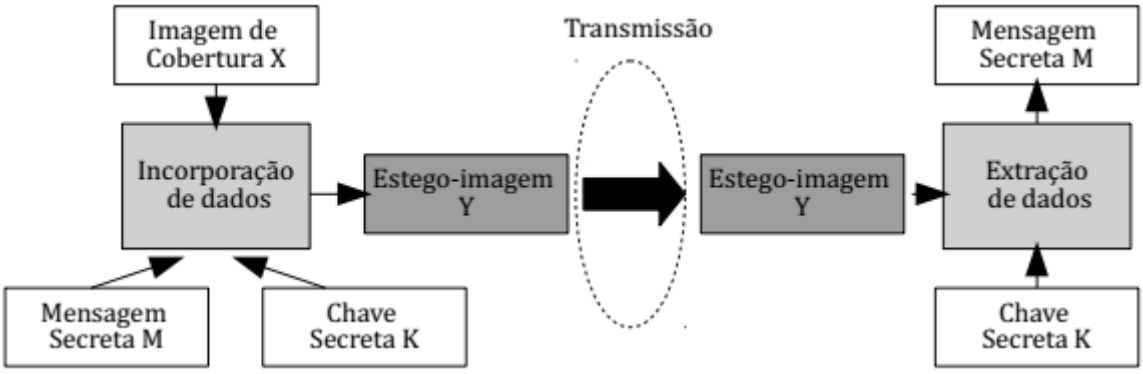
Figura 11 – Processo de esteganografia.



Fonte: autoria própria (2017).

Um esquema para a transmissão de dados secretos por meio de esteganografia é apresentado na Figura 12 (LI *et al*., 2011).

Figura 12 – Esquema para transmissão de dados secretos



Fonte: adaptado de Li *et al*. (2011).

A Figura 12 mostra que os dados secretos são incorporados a uma imagem de cobertura com o auxílio de uma estego-chave, criando uma estego-imagem. Em seguida, após a transmissão e usando uma estego-chave idêntica à primeira, os dados secretos são extraídos da estego-imagem.

Métodos de filtragens, mascaramento e transformações são, em conjunto com o LSB, meios comuns de ocultação de mensagens em imagens, cada um deles com diferente grau de sucesso. Por grau de sucesso entende-se a efetividade e a qualidade no ocultamento de dados secretos (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Uma das técnicas comuns de ocultação de dados baseia-se na manipulação de planos LSB, por meio da substituição de *bits* menos significativos de uma imagem de cobertura por

bits secretos (CHAN; CHENG, 2003). A técnica do LSB possui algumas variações que buscam aperfeiçoar a técnica original.

2.3.1 O método do *bit* menos significativo

O método do *bit* menos significativo (do inglês *Least Significant Bit* ou LSB) baseia-se na alteração nos planos de *bits* que compõem uma imagem digital (TAVARES; LIMA; MADEIRO, 2012).

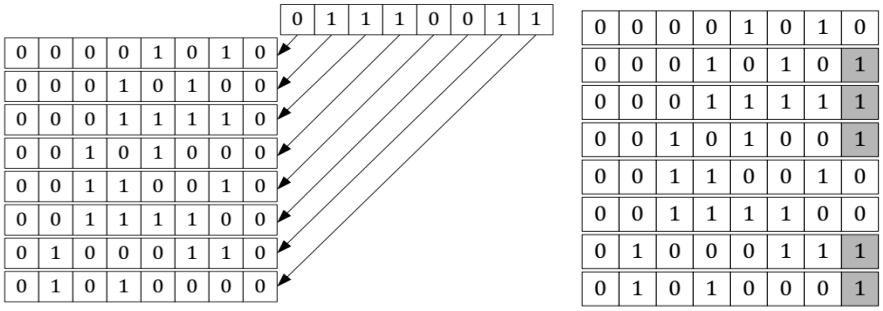
A forma mais comum para inserir mensagens secretas em imagens envolve as técnicas baseadas no LSB aplicadas a cada byte de uma imagem com profundidade de 32 *bits*. A inserção dos dados a serem ocultados é efetuada por meio da modificação dos últimos *bits* de cada byte. Uma implementação do método LSB consiste na substituição do plano dos *bits* menos significativos das componentes de cor da imagem pelos dados que devem ser ocultados (TAVARES; LIMA; MADEIRO, 2012; ROCHA *et al*., 2004).

É possível selecionar um *bit* em cada byte do *pixel* de cobertura para que o *bit* a ser ocultado seja representado pelo *bit* selecionado. Este método não causa alterações perceptíveis na imagem (JULIO; BRAZIL; ALBUQUERQUE, 2007). Existem diferentes variações do método LSB. As modificações de *pixels* no plano menos significativo são imperceptíveis ao olho humano. Entre algumas variações deste método estão o LSB *Replacement*, o LSB *Matching* e o LSB *Matching Revisited*, descritos a seguir.

2.3.2 O método do *bit* menos significativo com realocação

O método de esteganografia do *Bit* Menos Significativo com Realocação **(**LSB *Replacement*) faz com que os *bits* menos significativos dos *pixels* da imagem de cobertura sejam trocados pelos *bits* da mensagem que se pretende ocultar. Nessa versão do método, antes do ocultamento da informação, a mensagem secreta deve ser transformada em sua forma binária. Assim, seus *bits* podem ser inseridos de forma sequencial no local onde estão os *bits* menos significativos nos *pixels* de cobertura (KAUR; KAUR; KUMAR, 2015; DARABKH *et al*., 2014). O funcionamento do LSB *Replacement* é ilustrado pela Figura 13.

Figura 13 – Funcionamento do LSB *Replacement*.



(a) Incorporação dos *bits* (b) Nova configuração

Fonte: autoria própria (2017).

Na Figura 13 (a) tem-se a representação de oito *pixels* de cobertura em seu formato binário. O método LSB aplicado nesse caso inseriu cada *bit* da sequência 01110011 no *bit* menos significativo dos *pixels* de cobertura. Após esse processo, tem-se a nova configuração dos *pixels* de cobertura em (b), na qual os *bits* menos significativos destacados sofreram alteração em relação aos seus valores originais e os não destacados permaneceram com seu valor original, pois esse era igual ao valor do *bit* que estava sendo ocultado.

As vantagens dessa variação são o fato de a perda da qualidade da imagem original não ser acentuada e de haver uma maior capacidade de ocultação de dados secretos. Entretanto, a baixa robustez e pequenas alterações na imagem podem destruir os dados ocultos (KAUR; KAUR; KUMAR, 2015). A baixa robustez dessa variação se refere ao fato de que ela não oferece proteção em níveis elevados contra ataques de esteganálise. Além disso, simples ataques como borramento, rotação, zoom, entre outras ações praticadas sobre a composição da imagem, podem fazer com que dados ocultos sejam perdidos.

2.3.3 O método do *bit* menos significativo com correspondência

O Método do *Bit* Menos Significativo com Correspondência (LSB *Matching*) é uma melhoria do método LSB *Replacement*. Essa variação utiliza o processo de somar ou subtrair, randomicamente, o valor 1 ao valor do *pixel* da imagem de cobertura sempre que o *bit* menos significativo do *pixel* de cobertura tiver um valor diferente do *bit* da mensagem secreta a ser ocultado (KAUR; KAUR; KUMAR, 2015; VASHISHTHA; DUTTA; SUR, 2013). O funcionamento do LSB *Matching* é ilustrado pela Figura 14.

Figura 14 – Funcionamento do LSB *Matching*.



Fonte: autoria própria (2017).

Uma das vantagens dessa variação é que a esteganografia realizada pelo LSB *Matching* possui uma detecção mais difícil que a realizada pelo LSB *Replacement* (VASHISHTHA; DUTTA; SUR, 2013). O processo de somar ou subtrair o valor 1 de forma aleatória ao *pixel*, cujo *bit* menos significativo é diferente do *bit* a ser oculto, pode evitar a assimetria criada pelo LSB *Replacement* (JINDAL; KAUR, 2016).

2.3.4 O método do *bit* menos significativo com correspondência revisitada

No método do *Bit* Menos Significativo com Correspondência Revisitada (LSB *Matching Revisited*), há melhorias em relação às outras variações do LSB. Nesta variação é possível diminuir a taxa de modificação de *bits*, o que significa que pode haver menos modificações na imagem de cobertura que nos métodos LSB *Replacement* e LSB *Matching*, embora utilizando uma mesma carga útil a ser ocultada (JINDAL; KAUR, 2016).

Esta variação usa uma unidade de incorporação de *bits* formada por um par de *bits* adjacentes e sequenciais. Esse processo é capaz de incorporar até dois *bits* secretos por unidade de incorporação. Uma unidade de incorporação é composta por um conjunto de dois *pixels* consecutivos da imagem, sendo que não há sobreposição entre essas unidades. O *bit* menos significativo do primeiro *bit* dessa unidade representa um *bit* da mensagem secreta, enquanto outro *bit* é extraído da relação entre os dois *bits* da unidade de incorporação. Como vantagem, o LSB *Matching Revisited* permite que seja incorporada em uma imagem, a mesma quantidade de informação que o LSB *Matching*. No entanto, a aplicação do LSB *Matching Revisited* ocasiona menos alterações à imagem de cobertura que o LSB *Matching*. Logo, esse fato torna a detecção do LSB *Matching Revisited* mais difícil que a do LSB *Matching* (LUO; HUANG; HUANG, 2010; MIELIKAINEN, 2006).

2.4 TRABALHOS CORRELATOS

Na literatura, existem diversos trabalhos que propõem a aplicação de esteganografia, criptografia ou de ambas em imagens digitais.

Rocha (2003) desenvolveu um produto de *software* que permitisse a comunicação segura pela internet por meio da utilização de técnicas esteganográficas em imagens digitais. O trabalho proposto visou implementar três variantes de técnicas esteganográficas, a fim de acompanhar o funcionamento das mesmas.

Chan e Cheng (2003) propôs um esquema de ocultamento de dados pela simples substituição LSB. A qualidade da estego-imagem produzida pelo método pode ser melhorada por meio da aplicação do processo *Optimal Pixel Adjustment Process* (OPAP).

Mielikainen (2006) propôs uma modificação ao método LSB *Matching*. O método proposto, chamado de LSB *Matching Revisited*, é realizado para imagens de cobertura em escala de cinza e a incorporação é realizada em unidades de incorporação formadas por dois *pixels* da imagem de cobertura por vez. O valor de um dos *bits* secretos é o LSB do primeiro *pixel* da unidade, enquanto o valor do próximo *pixel* secreto é uma função dos dois *pixels* da unidade de incorporação.

Oliveira (2007) trabalhou a junção de criptografia e esteganografia para proteger a informação. Neste trabalho é feito um estudo de esteganografia em uma sequência de imagens. Ele propõe uma esteganografia mais agressiva nos coeficientes da transformada discreta de cosseno.

Brazil (2008) propôs um aperfeiçoamento e busca de melhores soluções no processo de esteganografia. Para isso, é apresentada uma heurística híbrida que combina algoritmos genéticos e reconexão de caminhos. Ele propõe a utilização da reconexão de caminhos e a possibilidade de ocultar informações em imagens coloridas pode melhorar o desempenho dos algoritmos genéticos na esteganografia, pois o espaço disponível para ocultação é aumentado, devido a uma melhor utilização dos *bits* menos significativos.

Carvalho (2008) propôs um método para esteganografia em vídeos comprimidos por meio da exploração da estrutura do padrão de vídeo MPEG-4. O método, denominado MP4Stego, se propõe a recuperar informações sem perda e apresentar maior capacidade de inserção de dados ocultos.

Cheddad *et al*. (2008) propôs uma nova técnica que aprimora a esteganografia de imagens. Nesta técnica, os dados secretos podem ser incorporados a quadros de arquivos de

vídeo. Para a localização do *pixel* onde os dados serão incorporados, o vídeo é dividido em forma de quadros uma região específica é escolhida para a incorporação, produzindo um estego-vídeo.

Hospodar (2009) propôs três abordagens para sistemas de esteganografia em imagens digitais. O objetivo deste trabalho é ocultar a maior quantidade possível de informação nos coeficientes do domínio da transformada discreta do cosseno (DCT) de imagens digitais, usando uma parte desses coeficientes para a escrita da mensagem e reservando o restante deles para a restauração ou compensação da estatística da imagem original.

Cantanhede (2009) mostrou a implementação de um software por meio da utilização da técnica de esteganografia LSB. O software se propõe a incluir texto em arquivos de imagem e em um arquivo de áudio, a fim de comparar os arquivos originais e os arquivos que possuem mensagens ocultas para apontar diferenças entre os mesmos.

Cahú (2009) apresentou um algoritmo baseado em BSP *Tree* para a aplicação de esteganografia em imagens digitais. O método proposto considera o valor de RGB de cada *pixel* como um ponto no espaço tridimensional englobado por um volume limitante.

Gutub (2010) propôs uma técnica melhorada de esteganografia em que o aproveitamento dos 24 *bits* em cada *pixel* nas imagens com canais RGB é feito usando-se dois *bits* menos significativos de um dos canais para indicar a presença de dados nos outros dois canais. A *Pixel Indicator Technique* (PIT) é uma técnica para esteganografia em imagens utilizando os seus canais RGB.

Seivi, Mariadhasan e Shunmuganathan (2012) propuseram um método para preservar características estatísticas e visuais na esteganografia. É proposto um novo esquema de esteganografia que pode incorporar dados secretos em regiões de arestas mais nítidas em imagens, de acordo com um limiar definido pelo tamanho da mensagem oculta.

Gutte e Chincholkar (2012) proporam um método para esteganografia de texto aliada à criptografia. O método proposto utiliza a técnica de ocultação de dados na posição LSB. Foi realizada a comparação da ocultação de dados em uma e duas posições LSB, avaliando medidas de desempenho como MSE, Entropia, entre outras.

Mandal e Das (2012) sugeriram uma técnica para incorporar os dados secretos nos três componentes de cor de uma imagem. Os três componentes de cor são separados de cada *pixel* e são formadas três matrizes R, G e B. Então o método PVD (*Pixel Value Differencing*) é aplicado a cada matriz. Então o primeiro *pixel* secreto é incorporado ao primeiro bloco da matriz R, o segundo *pixel* secreto ao primeiro bloco da matriz G e o terceiro *pixel* secreto ao

primeiro bloco da matriz B. O processo segue analogamente até incorporar todos os *bits* secretos.

Kumar e Sharma (2013) propuseram uma nova técnica para ocultação de informação na qual a técnica *Hash*-LSB é usada para ocultar a existência de uma mensagem secreta. Nessa técnica, o algoritmo de criptografia RSA é utilizado para transformar a mensagem secreta em uma mensagem humanamente não legível.

Renza, L. e Rincón (2016) propuseram um método que melhora os resultados do método *Block Pixel Hiding Method* (BPHM). O método é baseado na seleção de banda e em um algoritmo de busca global, sendo denominado *Improved Pixel Hiding Method* (IPHM). Os resultados obtidos em testes do IPHM são melhores que os do BPHM e similares ao *Quantization Index Modulation* (QIM).

Tavares e Madeiro (2016) fizeram a apresentação do LSB *Word Hunt* (LSB WH). Esse método consiste em uma nova visão sobre o método LSB e é inspirado em um jogo de caça-palavras. O principal objetivo do método proposto é reduzir o Número Esperado de Modificações por *Pixel* (*Expected Number of Modifications per Pixel* - ENMPP) em relação a outros métodos.

França e Madeiro (2016) abordaram a esteganografia LSB apresentando um novo método de esteganografia que se baseia em sequências de baixa discrepância. O método proposto orienta a distribuição dos *bits* a serem ocultos por meio do uso de uma chave criptográfica.

Kaur e Mahajan (2016) proporam em seu trabalho uma representação híbrida para a incorporação de dados. O método utiliza a incorporação de padrões aleatórios em conjunto com a criptografia, a fim de elevar a segurança da esteganografia. O método proposto tem o objetivo de aumentar a segurança na codificação sequencial e decodificação de dados em vídeos.

Atee *et al*. (2017) propôs uma nova abordagem para esteganografia de imagens com alto desempenho, em que o algoritmo Extreme Learning Machine (ELM) é modificado para criar um modelo matemático supervisionado. Essa nova abordagem visa determinar a localização ótima para incorporar a mensagem secreta precisamente com uma distorção mínima da imagem de destino.

O presente trabalho aplica a esteganografia por meio da manipulação dos *bits* menos significativos de um *pixel*, trabalhando assim, no domínio espacial das imagens, manipulando seus planos de *bits*.

3 CRIPTOGRAFIA E ESTEGANOGRAFIA BASEADA NO *BIT* MENOS SIGNIFICATIVO COM REJEIÇÃO

Neste capítulo o método do *Bit M*enos Significativo com Rejeição (LSBR) é introduzido e descrito. O LSBR é o método proposto por este trabalho para realizar esteganografia auxiliada por criptografia em imagens digitais. O LSBR é composto por dois processos, que são a criptografia e a esteganografia. A criptografia é responsável por tornar o conteúdo de uma imagem ininteligível. A esteganografia é responsável por incorporar a informação secreta criptografada a uma imagem de cobertura.

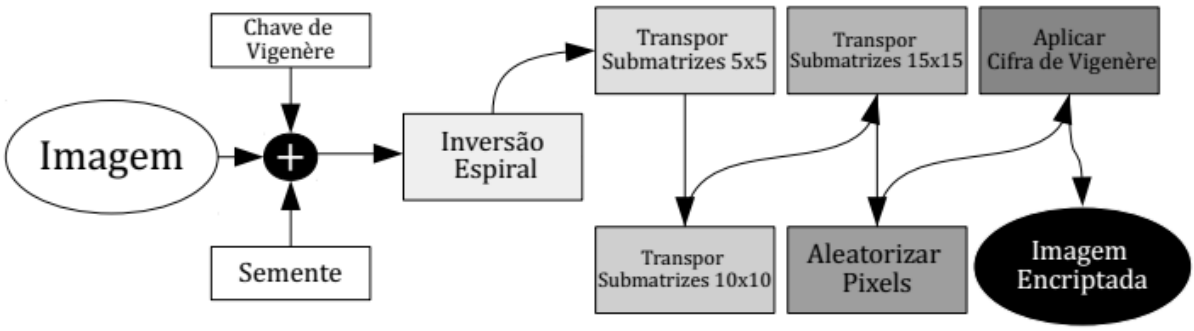
3.1 CRIPTOGRAFIA

O LSBR propõe a união de conceitos de criptografia e esteganografia em imagens digitais. A criptografia, nesse contexto, tem a finalidade de prover mais uma camada de segurança à incorporação de dados em outro meio, incorporação essa que é realizada por meio de esteganografia. O fato de a informação incorporada a outro meio já estar encriptada faz com que, caso essa informação seja recuperada indevidamente, ainda seja preciso quebrar um processo de criptografia. Isso torna os dados secretos mais protegidos contra o acesso não autorizado.

O processo de criptografia proposto atua sobre o domínio espacial das imagens, diretamente com suas matrizes de *pixels*, reposicionamento de *pixels* e alteração de valores de intensidades das matrizes. Esse processo é composto por quatro sub-rotinas, que são a manipulação de submatrizes transpostas, a inversão em espiral, a cifragem adaptada de Vigenère e a aleatorização. Para a execução dessas rotinas é necessário que se conheçam a chave de Vigenère e uma imagem da qual será obtida uma semente para a geração de sequências pseudoaleatórias para o reposicionamento de *pixels*.

A criptografia de uma imagem é realizada em seis passos, seguindo-se uma ordem de execução das sub-rotinas componentes do processo, conforme a ilustração na Figura 15.

Figura 15 – Sequência seguida pela criptografia do LSBR.



Fonte: autoria própria (2017).

Após a execução do processo de criptografia, a imagem secreta estará pronta para ser incorporada à imagem de cobertura por meio do processo de esteganografia proposto.

3.1.1 Geração da chave de Vigenère

Para o correto funcionamento do método de criptografia proposto, é necessário que uma chave seja fornecida. Essa chave irá ser utilizada no processo de cifragem de Vigenère. A chave fornecida pelo usuário deve ser um texto codificado no formato ASCII. Apesar de o texto fornecido pelo usuário necessitar estar codificado no formato ASCII, nem todos os caracteres dessa tabela podem ser usados para compor a chave, isto é, apenas os caracteres representados pelos códigos de 32 a 126. Com base na Tabela ASCII, observa-se que esses caracteres são os caracteres imprimíveis.

Há uma correspondência entre o valor numérico de cada caractere representado pelos códigos ASCII de 32 a 126 e os números do conjunto C. O conjunto C é formado pelos números que podem ser representados considerando a variação de N *bits* mais significativos de um *byte* (considerando o restante dos *bits* como iguais a zero), em que N equivale à quantidade de *bits* de um *pixel* envolvidos no processo de ocultação. Para N = 3, temos que C = {0, 32, 64, 96, 128, 160, 192, 224}. Uma possível configuração para essa correspondência é verificada no Quadro 2.

Quadro 2: Possível correspondência entre a Tabela ASCII e o conjunto C para N = 3.

ASCII	C	ASCII	C	ASCII	C	ASCII	C	ASCII	C
32	64	52	64	72	224	92	0	112	128
33	128	53	224	73	128	93	192	113	96
34	64	54	128	74	64	94	96	114	192
35	160	55	32	75	192	95	64	115	0
36	96	56	192	76	96	96	160	116	96
37	192	57	160	77	0	97	0	117	224
38	128	58	0	78	160	98	96	118	128
39	160	59	224	79	32	99	32	119	160
40	32	60	96	80	128	100	224	120	0
41	160	61	160	81	32	101	64	121	64
42	64	62	32	82	160	102	0	122	224
43	160	63	192	83	64	103	192	123	128
44	96	64	128	84	192	104	96	124	96
45	192	65	64	85	0	105	32	125	192
46	32	66	224	86	96	106	160	126	32
47	224	67	0	87	224	107	0		
48	64	68	128	88	32	108	224		
49	224	69	64	89	128	109	128		
50	0	70	192	90	96	110	224		
51	192	71	32	91	160	111	32		

Fonte: Autoria Própria.

Os números correspondentes da sequência ASCII são gerados em uma sequência aleatória, fazendo-se cada valor ASCII corresponder a um número do conjunto C gerado aleatoriamente. Essa sequência deve ser gerada a partir da semente informada no início do processo. A razão para essa correspondência é a necessidade de a chave ser formada apenas pelos números que podem ser formados variando-se apenas N *bits* de um *byte* e considerando os demais como zero. Isso faz com que todos os valores trabalhados pela tabela de Vigenère sejam valores representáveis pela quantidade de *bits* adotada. Para o caso de uma quantidade de *bits* diferente de 3 ser adotada para o processo, a correspondência exemplificada no Quadro 2 deve ser alterada, de forma que os valores representáveis pela quantidade de *bits* adotada para o processo sejam representados naquele Quadro.

Dessa forma, a Tabela de Vigenère usada no presente trabalho foi adaptada. Essa tabela passa a ser composta pelos valores pertencentes ao conjunto C, apresentando o mesmo padrão de distribuição de seus elementos que a Tabela de Vigenère original.

A chave de Vigenère terá o mesmo número de elementos que a chave informada em formato ASCII. Cada caractere ASCII vai gerar um número da chave de Vigenère pertencente ao conjunto C, considerando a representação decimal ASCII e a respectiva correspondência desse número no Quadro 2 e suas variações.

3.1.2 Geração da semente

A semente usada para a geração de sequências pseudoaleatórias nos processos de criptografia e esteganografia propostos é um número inteiro obtido por meio de operações sobre o domínio espacial de uma imagem informada. Para tais operações, além da manipulação das matrizes RGB, as matrizes YIQ são manipuladas.

O Modelo YIQ é um modelo de cores que funciona como uma recodificação do sistema RGB, com a finalidade de manter a compatibilidade com padrões de TV monocromática na transmissão. O Y representa a luminância de uma imagem, enquanto que o I e o Q representam a informação de cores. A conversão entre RGB e YIQ pode ser feita por meio das equações mostradas nas Equações 1, 2 e 3 (GONZALEZ; WOODS, 2000).

$$Y = 0{,}299\,R + 0{,}587\,G + 0{,}114\,B \tag{1}$$

$$I = 0{,}596\,R - 0{,}275\,G - 0{,}321\,B \tag{2}$$

$$Q = 0{,}212\,R - 0{,}523\,G + 0{,}311\,B \tag{3}$$

Na aplicação da Equação 4, os parâmetros obtidos da análise das matrizes R, G, B, Y, I e Q das representações de cor RGB e YIQ da imagem informada são usados para calcular o valor da semente.

$$S = (maxY * maxI * maxQ) * ((\frac{maxR}{255}) * (\frac{maxG}{255}) * (\frac{maxB}{255})) + (maxR * maxG * maxB) \tag{4}$$

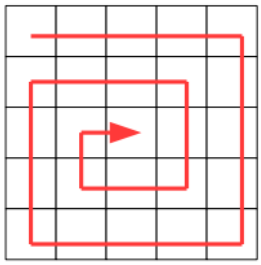
Na Equação 4, os parâmetros maxY, maxI, maxQ, maxR, maxG e maxB representam, respectivamente, as intensidades com maior frequência nas matrizes Y, I, Q, R, G e B. Seus valores pertencem ao intervalo *I = [0, 255]*. Nesta Equação são considerados os valores inteiros das divisões, a fim de que o valor da semente seja um inteiro.

3.1.3 Inversão em espiral

No processo de criptografia proposto existe a etapa de inversão em espiral. Essa etapa consiste em fazer a leitura de cada *pixel* da matriz de intensidades da imagem na ordem de uma espiral que se inicia no *pixel* (0, 0) e termina no centro da imagem.

A ordem de leitura dos *pixels* em uma imagem 5x5 é indicada na Figura 16 (a). A leitura é iniciada no *pixel* (0, 0) e finalizada no centro, no *pixel* (2, 2). A cada leitura, o valor é registrado em um vetor. Após a leitura de todos os *pixels* da imagem, a inversão ocorre reinserindo-se na imagem os valores lidos, na ordem do último elemento do vetor que foi preenchido para o primeiro. A sequência de inserção dos valores na imagem segue a mesma sequência de leitura apresentada na Figura 16 (a). Na Figura 16 (b) tem-se um exemplo de imagem original com seus valores antes do processo de inversão em espiral ser aplicado e na Figura 16 (c), a mesma imagem após o processo de inversão em espiral. Esse processo de inversão pode ser aplicado a imagens de quaisquer dimensões.

Figura 16 – Processo de inversão em espiral.



(a)

0	0	0	0	0
0	55	55	55	0
0	55	55	55	0
0	55	55	55	0
0	0	0	0	0

(b)

55	55	55	55	55
0	0	0	0	55
0	0	0	0	55
0	0	0	0	55
0	0	0	0	55

(c)

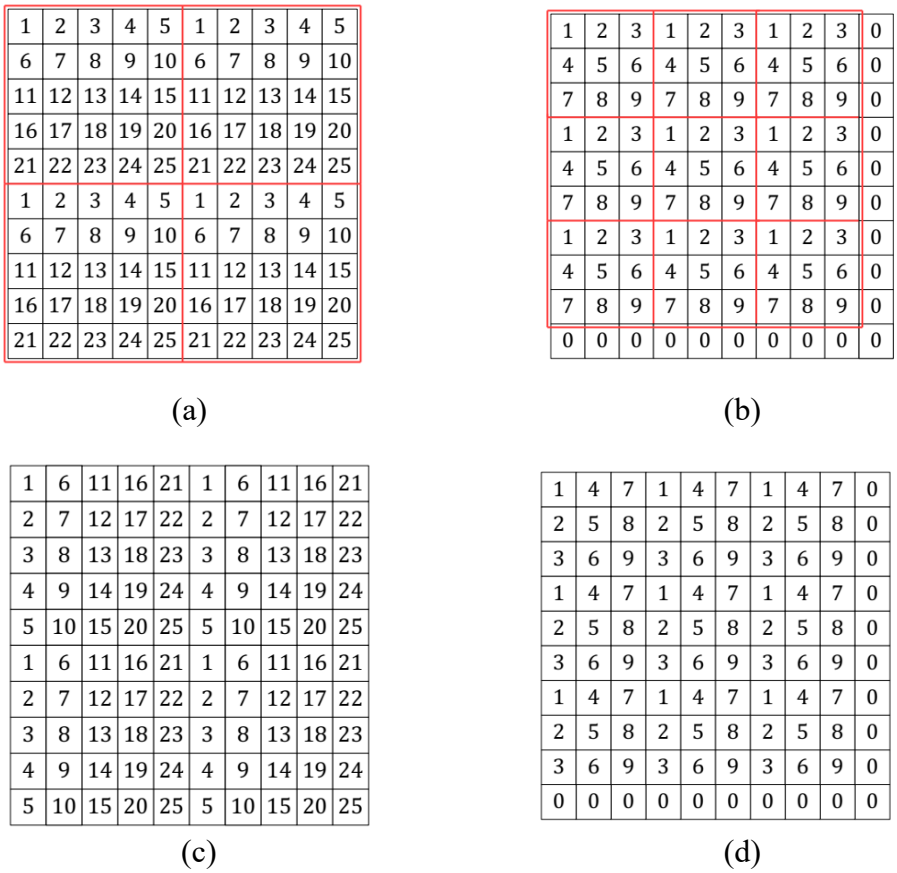
Fonte: autoria própria (2017).

3.1.4 Manipulação de submatrizes

No processo de criptografia da imagem, uma das etapas é a manipulação de submatrizes para encontrar suas transpostas. Esse procedimento faz parte da manipulação espacial da imagem, reposicionando seus *pixels*, para assim modificar as características da imagem e torná-la ininteligível.

O processo de transposição de submatrizes consiste em dividir a imagem em submatrizes quadradas de forma que não haja sobreposição entre elas e então realizar a transposição em cada uma delas. A divisão de uma imagem em submatrizes quadradas é ilustrada, de duas formas diferentes, na Figura 17.

Figura 17 – Manipulação de submatrizes.



Fonte: autoria própria (2017).

Na Figura 17 (a) é mostrada uma imagem com sua matriz *pixels* de 10x10 dividida em submatrizes quadradas 5x5. O número em cada *pixel* refere-se à intensidade de cor daquele *pixel*. Nesse caso, a imagem foi coberta completamente por submatrizes, pelo fato de suas dimensões serem múltiplas do tamanho das submatrizes.

Na Figura 17 (b) é mostrada uma imagem dividida em submatrizes quadradas de 3x3. Nesse caso, a imagem não foi completamente coberta pelas submatrizes, ficando a última linha e a última coluna descobertas. Na manipulação de submatrizes transpostas, isso acontece sempre que alguma das dimensões da imagem não for múltipla de alguma das dimensões da submatriz. Se a imagem em (b) possuísse dez linhas e nove colunas, apenas a última linha não seria coberta.

Na Figura 17 (c) é exibida a nova disposição dos *pixels* da imagem (a) após a transposição das submatrizes indicadas. Na Figura 17 (d) é exibida a nova disposição dos *pixels* da imagem (b) após a transposição das submatrizes indicadas, sendo que nesses casos as colunas e/ou linhas que não estão cobertas pelas submatrizes não sofrem modificação.

3.1.5 Aleatorização

Para a troca de posições dos *pixels* é necessário que a matriz original seja vetorizada. Isso é feito criando-se um vetor de intensidades de *m x n* posições, em que m e n são as dimensões da matriz de intensidades. A matriz é percorrida da esquerda para a direita e de cima para baixo, e cada valor lido é inserido na posição corrente do vetor, que é acessado a partir da posição zero.

Após esse procedimento, um vetor com o mesmo tamanho do primeiro é definido. Esse vetor vai ser preenchido com números aleatórios sem repetição, no qual cada número representa uma posição do vetor e pertence ao intervalo *I = [0, m x n – 1]*. Na Figura 18 é mostrado um vetor que representa uma matriz de intensidades vetorizada e um vetor com posições aleatórias.

Figura 18 – Matriz de intensidades vetorizada e vetor com posições aleatórias.

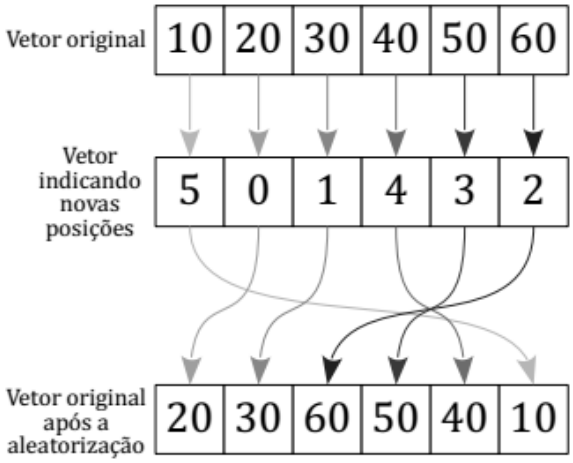


(a) (b)

Fonte: autoria própria (2017).

O valor de uma posição do vetor de números aleatórios indica qual a nova posição que a posição correspondente do vetor de intensidades ocupará após a aleatorização. Como exemplo, o valor da posição zero do vetor de números aleatórios indica qual a nova posição do *pixel* representado pela posição zero do vetor de intensidades. Dessa forma, a posição do novo vetor de intensidades, indicada pelo valor da posição zero do vetor de números aleatórios, será preenchida com a intensidade presente na posição zero do vetor de intensidades. Na Figura 19 é ilustrado como ficará o vetor de intensidades da Figura 18 (a) após a aleatorização.

Figura 19 – Novo vetor de intensidades após aleatorização.



Fonte: autoria própria (2017).

Após o processo de aleatorização do vetor de intensidades, a matriz de intensidades é novamente formada. Isso é feito percorrendo-se a nova matriz da esquerda para a direita e de cima para baixo. Cada *pixel* da matriz será preenchido com a intensidade presente na posição corrente do vetor aleatorizado, que é acessado a partir da posição zero.

3.1.6 Cifragem de vigenère

Uma outra etapa inclusa no processo de criptografia proposto é a cifragem de Vigenère. Esta etapa consiste na aplicação da cifra de Vigenère aos valores dos *pixels* presentes na matriz de intensidades da imagem. Essa etapa tem como finalidade trocar valores verdadeiros das intensidades das imagens por valores falsos, que não condizem com a composição verdadeira dos seus valores. Isso faz com que a imagem que passe por esse procedimento perca os valores reais de suas intensidades e assuma valores incorretos, distorcendo a sua composição verdadeira.

Esse procedimento é baseado no uso de uma chave de Vigenère e no uso de uma Tabela de Vigenère adaptada, que pode ser vista na Quadro 3.

Quadro 3 – Tabela de Vigenère adaptada.

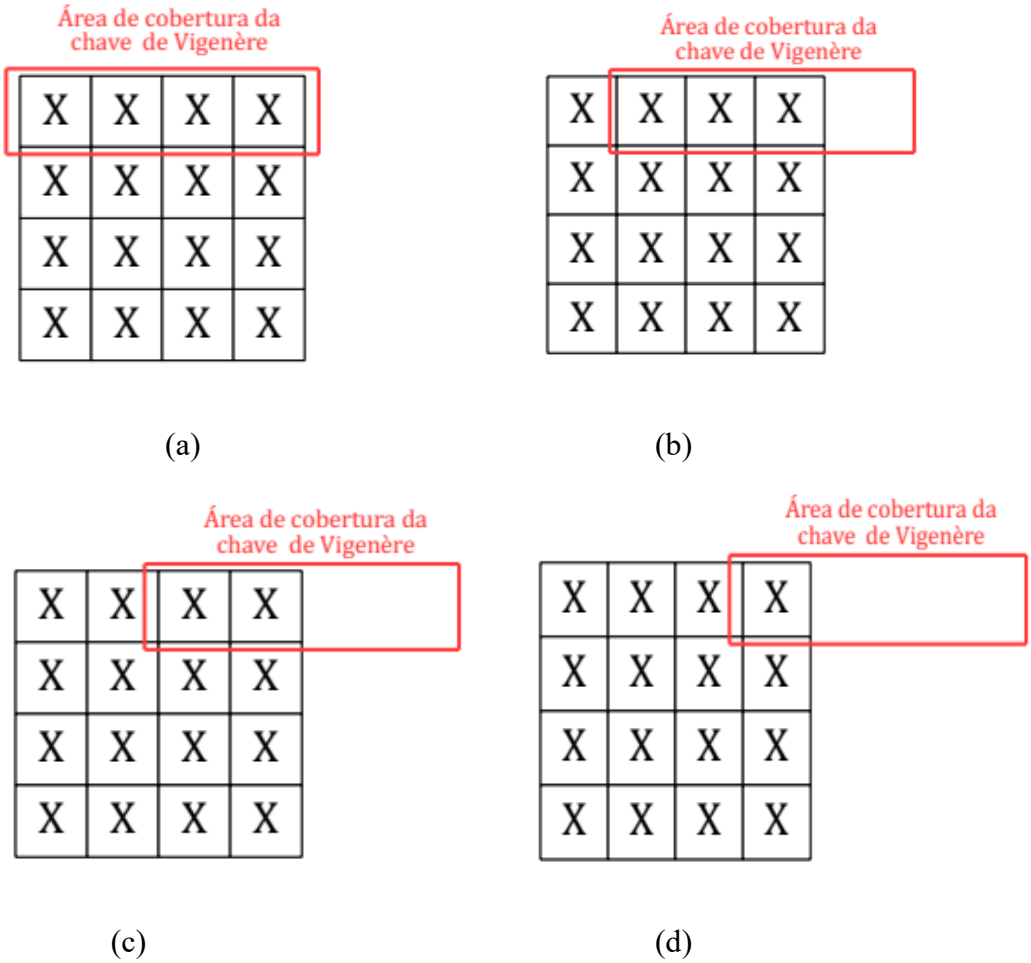
	0	32	64	96	128	160	192	224
0	0	32	64	96	128	160	192	224
32	32	64	96	128	160	192	224	0
64	64	96	128	160	192	224	0	32
96	96	128	160	192	224	0	32	64
128	128	160	192	224	0	32	64	96
160	160	192	224	0	32	64	96	128
192	192	224	0	32	64	96	128	160
224	224	0	32	64	96	128	160	192

Fonte: autoria própria (2017).

Dependendo da quantidade de *bits* ocultos com que se está trabalhando, a tabela do Quadro 3 pode mudar. Para cada quantidade de *bits* usados na esteganografia há uma nova tabela, pois ela é preenchida com os números que podem ser formados considerando-se apenas os n *bits* mais significativos de um *byte*, ou seja, com os outros *bits* sendo zero. A tabela do Quadro 3 é a tabela para o uso de três *bits* na esteganografia. O preenchimento de outras tabelas segue o mesmo padrão da apresentada no Quadro 3, com a diferença de usar apenas os números que podem ser gerados para a quantidade de *bits* em uso.

O processo de cifragem consiste na análise de N elementos da matriz de intensidades em conjunto com a chave de Vigenère de N elementos. A cada análise, um número N de elementos sequenciais da matriz de intensidades é selecionado para que a correspondência dentro da Tabela de Vigenère adaptada seja encontrada para a chave de N elementos. Na Figura 20 é ilustrado o processo de cifragem ocorrido em uma linha de uma imagem 4x4.

Figura 20 – Processo de cifragem de Vigenère.



Fonte: autoria própria (2017).

Para esse caso, uma chave de 4 elementos foi usada. Logo, a cada análise, um conjunto de 4 *pixels* em sequência foi utilizado para encontrar a devida correspondência dentro da Tabela de Vigenère. O processo de cifragem utilizado desconsidera posições fora do espaço matricial da imagem, como ocorre na Figura 20 (b), (c) e (d). Nesses casos, a correspondência dentro da Tabela de Vigenère é feita apenas para os elementos que se encontram dentro do espaço matricial da imagem. Como exemplo, na Figura 20 (c) apenas dois primeiros *pixels* da área coberta (terceiro e quarto *pixels* da linha 1, respectivamente) são levados em consideração para ser realizada a correspondência na Tabela de Vigenère com os dois primeiros elementos da chave. Na Figura 20 (d), apenas o elemento sob a área coberta é levado em consideração em conjunto com o primeiro elemento da chave, e assim sucessivamente para os demais casos.

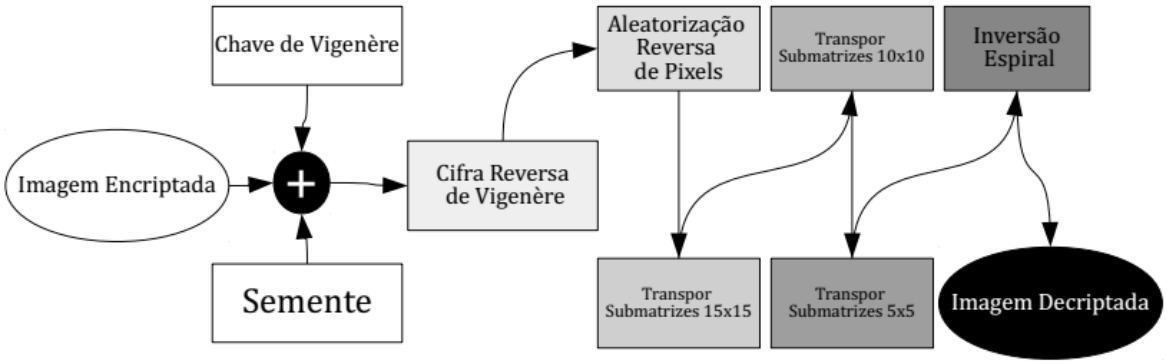
De acordo com o valor encoberto e o valor da respectiva posição na chave de Vigenère, o valor do *pixel* em questão é trocado por um valor da Tabela de Vigenère. O

processo de cifragem ocorre tomando como base para o início da área de cobertura para a seleção do conjunto a ser cifrado, cada *pixel* de uma linha por vez, iniciando-se pelo primeiro. Cada linha é percorrida, iniciando-se pela primeira. Assim, toda a imagem é modificada pela Cifra de Vigenère.

3.1.7 Processo reverso de criptografia

O processo reverso de criptografia ocorre seguindo-se as mesmas etapas do processo original, mas de forma inversa. Este processo é ilustrado na Figura 21. O processo reverso da Cifragem de Vigenère ocorre da mesma forma que o processo reverso da Cifra de Vigenère em sua forma geral, mas utilizando-se a tabela de Vigenère adaptada.

Figura 21 – Processo reverso de criptografia.



Fonte: autoria própria (2017).

O processo de aleatorização reverso ocorre gerando-se a mesma sequência de reordenamento de *pixels* por meio da mesma semente usada no processo original. Com essa sequência gerada, para cada posição do vetor de aleatórios, seu valor indica em qual posição do vetor de intensidades aleatorizado e advindo da matriz criptografada está o valor da matriz original na posição em análise. Então é feita a reordenação dos valores às suas posições originais e a imagem original é formada.

O processo reverso de manipulação de submatrizes transpostas ocorre aplicando-se a manipulação em ordem inversa. O resultado é igual à configuração original da matriz inicial, pois ao transpor uma matriz que já foi transposta uma vez, a matriz obtida será igual à inicial.

Logo, ao transpor uma sequência de matrizes e transpor novamente, mas na sequência inversa, a matriz resultante será igual à original.

A inversão em espiral reversa ocorre da mesma forma que a inversão inicial e segue a lógica de desfazer o que já estava feito. Ao inverter as posições de uma sequência de número que já havia sido invertida uma vez, o resultado é uma sequência igual à original.

3.2 ESTEGANOGRAFIA

O LSBR preserva características encontradas nos métodos LSB convencionais, como a alteração do *bit* menos significativo de cada *pixel* no processo de incorporação de informações que devem ser ocultadas. A proposta do método LSBR é trocar os *bits* menos significativos de uma imagem de cobertura por um *bit* indicador, chamado de *bit* sinalizador.

Nas formas tradicionais do LSB, cada *bit* alterado no conjunto de *pixels* da mensagem original representa um *bit* advindo da mensagem secreta. Dessa forma, após as substituições de *pixels* realizadas no processo de esteganografia, a mensagem ou imagem original será composta em parte por seus *bits* originais e em parte pelos *bits* da mensagem ou imagem secreta. O conjunto de *bits* alterados na imagem corresponderá ao conjunto de *bits* da mensagem ou imagem secreta.

A variação existente no método proposto, utilizado e avaliado neste trabalho, reside no real significado que o *bit* alterado no processo de incorporação de informações possui. No LSBR, o *bit* menos significativo de cada *pixel* presente em uma imagem é responsável por indicar se naquele *pixel*, em especial, ocorreu ou não uma incorporação de informação secreta. Dessa forma, o *bit* sinalizador indica se há ou não incorporação de informações naquele *pixel*. Assim, a informação oculta no *pixel* não é representada por seu *bit* menos significativo.

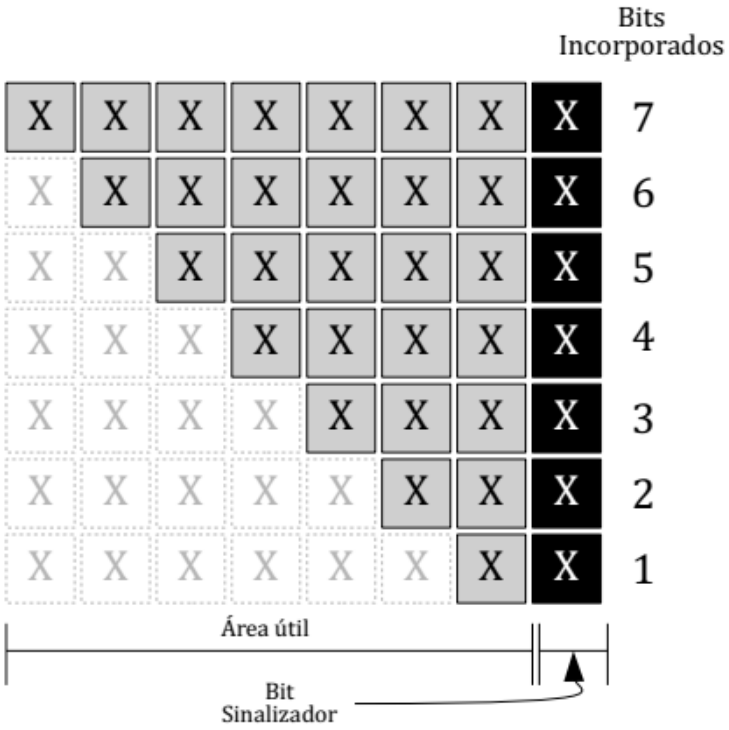
Com essa configuração do LSBR, é preciso que a informação a ser ocultada nos *bits* do *pixel* de cobertura selecionado não necessite utilizar o *bit* menos significativo como portador da informação oculta.

O LSBR permite incorporar, na imagem de cobertura, de um a sete *bits* por *pixel*. Esses *bits* incorporados são os *bits* mais significativos de um *pixel* da imagem secreta. Ao se selecionar um *pixel* na imagem de cobertura para receber *bits* de uma imagem que deve ser ocultada, a imagem de cobertura poderá, ou não, armazenar os *bits* da imagem secreta no *pixel* selecionado. A ação de incorporar ou não os *bits* da imagem secreta depende da configuração dos *bits* do *pixel* selecionado para a incorporação. O *bit* de sinalização do *pixel*

selecionado informará se os seus vizinhos representam uma informação oculta ou apenas a informação da própria imagem de cobertura.

O cerne da esteganografia do método LSBR está representado na Figura 22, na qual está a representação de como a incorporação de dados ocultos é feita em um *pixel*.

Figura 22 – Local de incorporação de *bits* pelo LSBR.



Fonte: autoria própria (2017).

Na Figura 22 são representadas sete configurações possíveis de incorporação de dados secretos para um *pixel* e seus *bits*. O funcionamento do método LSBR pode ser explicado pela divisão existente nessa ilustração. O LSBR divide cada *pixel* de cobertura em duas áreas, sendo uma a chamada área útil, responsável por abrigar os *pixels* secretos. É nessa área que os *bits* secretos serão representados. A outra área é responsável por guardar o *bit* sinalizador. O *bit* sinalizador está abrigado na posição de *bit* menos significativo, e é ele que informará se a área útil possui ou não informação secreta.

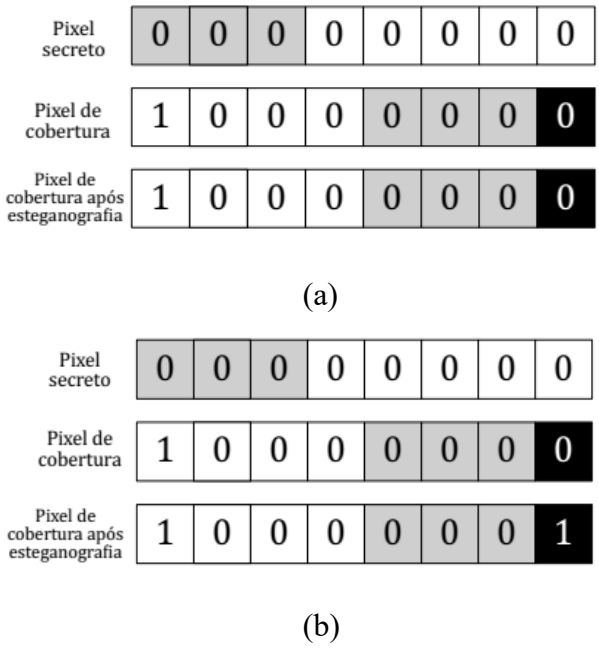
Um ponto relevante para a aplicação do LSBR é a escolha do *bit* sinalizador. Essa escolha é feita sorteando-se entre 0 e 1 para representar o *bit* sinalizador a cada tentativa de incorporação de *bits* secretos.

O LSBR verifica se os n *bits* de cobertura mais próximos do *bit* sinalizador do *pixel* de cobertura equivalem aos n *bits* mais significativos do *pixel* que se pretende ocultar, para $0 < n$

< 8. Em seguida, é feito um sorteio para decidir se o valor que representará equivalência entre os *bits* que se deseja ocultar e os *bits* de cobertura será 0 ou 1. Com essa decisão tomada, caso as sequências de *bits* sejam equivalentes, o *bit* de sinalização assumirá o valor decidido no sorteio para representar equivalência. Caso as sequências não sejam equivalentes, rejeita-se o *pixel* selecionado para a incorporação e o *bit* sinalizador assumirá o valor decidido no sorteio para representar a não equivalência.

Esse procedimento permite que não se determine qual *bit* indica a existência de uma informação oculta, pois em determinados momentos esse valor é 1 e em outros é 0. Na Figura 23 é ilustrado o processo de ocultação de *bits* realizado pelo LSBR no qual os *bits* a serem ocultados equivalem à sequência de *bits* de cobertura.

Figura 23 – Processo de ocultação do LSBR para sequências equivalentes.

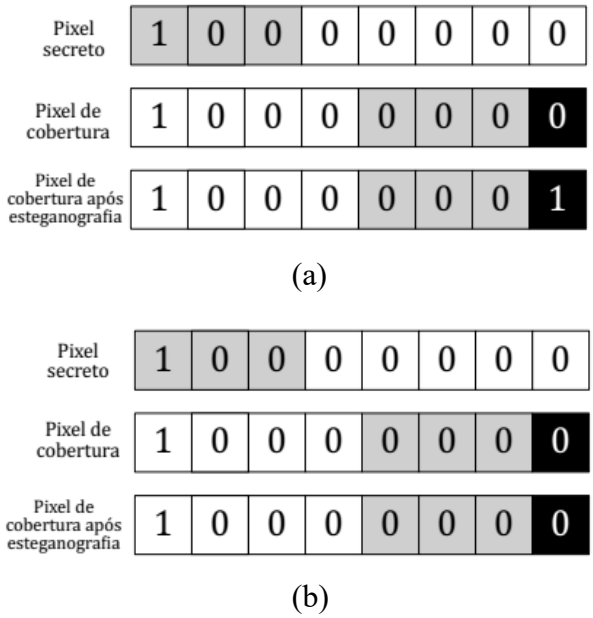


Fonte: autoria própria (2017).

Na Figura 23 são destacados os *bits* a serem ocultados, no *pixel* a ser ocultado, e os *bits* de cobertura, no *pixel* de cobertura. No primeiro momento, em (a), por meio do sorteio foi decidido que o *bit* sinalizador para a presença de informação oculta seria 0. No segundo momento, em (b), decidiu-se que tal *bit* seria 1. Como as sequências de *bits* secretos e *bits* de cobertura envolvidas nesse caso são idênticas, ao final do processo o *bit* sinalizador do *pixel* de cobertura assume o valor escolhido pelo sorteio para representar a presença de informação oculta.

Na Figura 24 é ilustrada a situação inversa, na qual a sequência de *bits* a serem ocultados não corresponde à sequência de *bits* de cobertura.

Figura 24 – Processo de ocultação do LSBR para sequências não equivalentes.



Fonte: autoria própria (2017).

De forma análoga à análise feita na Figura 23, verifica-se que as sequências de *bits* não são equivalentes. Portanto, no primeiro momento, em (a), o *bit* de sinalização do *pixel* de cobertura assume o valor 1 após o processo de esteganografia, pois o valor decidido no sorteio para representar a presença de conteúdo oculto foi 0. No segundo momento, em (b), o *bit* de sinalização do *pixel* de cobertura assume o valor 0 após o processo de esteganografia, pois o valor decidido no sorteio para representar a presença de conteúdo oculto foi 1.

A ocultação de informações, como etapa primordial do LSBR, pode ser descrita de uma forma geral pela sequência de passos:

1. Conhecer a sequência de *bits* a serem ocultos;
2. Conhecer a sequência de *bits* de cobertura;
3. Escolher o *bit* de sinalização que indica a presença de informação oculta;
4. Comparar as sequências de *bits*;
5. Alterar o *bit* menos significativo do *pixel* de cobertura, de acordo com o *bit* de sinalização escolhido e o resultado da comparação das sequências de *bits*.

Inicialmente, é preciso obter a sequência de *bits* a serem ocultados e a sequência de *bits* de cobertura. Com a posse dessa informação, é feita a escolha de um *bit* de sinalização para indicar a presença de informação oculta, o qual informará se os *bits* especiais de cobertura representam ou não a informação oculta. Após a comparação entre essas duas sequências de *bits*, ocorre a alteração do *bit* menos significativo do *pixel* de cobertura.

A escolha do n *bits* mais próximos do *bit* sinalizador para representar a informação oculta possui motivação no fato de a variação de configurações das sequências de *bits* nessa região ser alta. Essa variação ocorre de forma mais frequente nos *bits* menos significativos de um *pixel*, pois com a variação de intensidade de um *pixel* a variação nas regiões de *bits* menos significativos ocorre de forma mais acentuada que nas regiões de *bits* mais significativos. Isso faz com que a probabilidade de se encontrar uma sequência de *bits* de cobertura equivalente à sequência de *bits* secretos seja maior na região menos significativa de um *pixel*, facilitando o processo de incorporação da informação. Esse fato é ilustrado na Figura 25.

Figura 25 – Variabilidade nos *bits* menos significativos.

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

Fonte: autoria própria (2017).

Na Figura 25 são mostrados dezesseis valores de intensidades de *pixel,* no formato binário, sendo esses valores compostos por todos os números entre 240 e 255. Percebe-se que, em um conjunto de dezesseis números, os quatro *bits* menos significativos de todos os números variaram entre um número e outro. Enquanto isso, os quatro *bits* mais significativos

não variaram. Esses *pixels* mais significativos de uma imagem apenas irão variar de forma ampla caso a imagem possua *pixels* representando grande parte das intensidades possíveis, pertencentes ao conjunto *I = [0, 255]*. Para imagens com pouca variação de regiões de intensidade (como por exemplo, imagens que possuem apenas *pixels* de intensidade mais elevada), a variação nos *bits* mais significativos de seus *pixels* é baixa, conforme foi verificado na Figura 25.

3.2.1 Processo de esteganografia baseada no LSBR

O método proposto possui um procedimento específico geral para a realização da esteganografia nas imagens. Para o ocultamento de informações, é preciso que sejam fornecidas a imagem de cobertura, a semente para a geração de sequências de números aleatórios e a imagem a ser ocultada. O método precisa receber como parâmetros as matrizes que representam os canais de cor das duas imagens envolvidas no processo, além das dimensões de cada imagem. No processamento de imagens em escala de cinza, apenas uma das matrizes de cada imagem é necessária, uma vez que para imagens em escala de cinza têm-se que os canais de cor possuem valores iguais entre si, em todos os *pixels*.

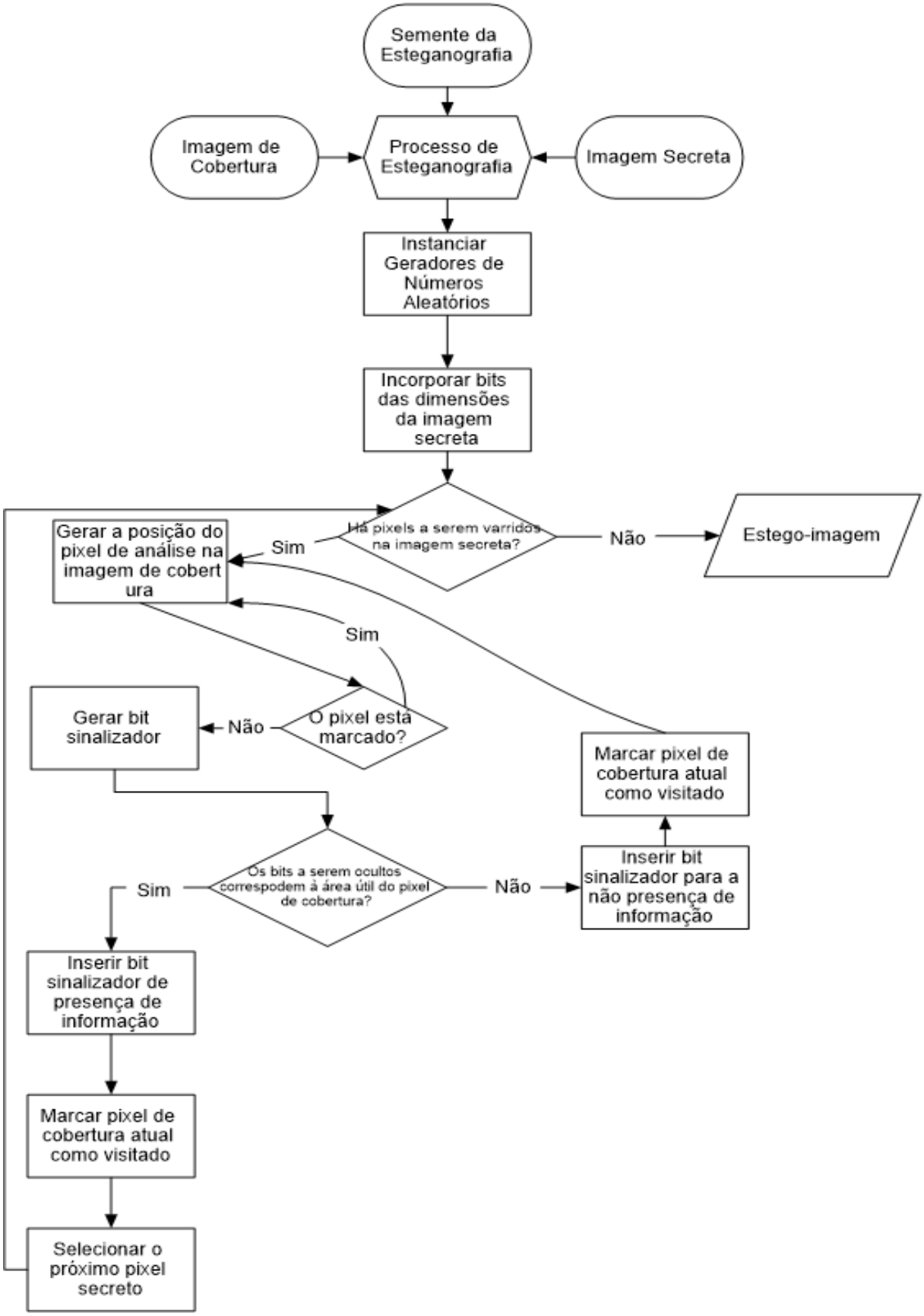
Com a posse dessas informações, são instanciados objetos para a geração de números aleatórios. Uma das sequências geradas é utilizada para a escolha de posições dentro da imagem de cobertura e a outra é utilizada para a escolha do *bit* de sinalização de informações ocultas. A etapa seguinte consiste em ocultar as dimensões da imagem secreta nos *pixels* da imagem de cobertura. A necessidade dessa ocultação vem do fato de no momento da tentativa de descoberta da imagem secreta não se ter conhecimento das dimensões dessa imagem secreta. Um processo de esteganografia para esconder essa informação associa mais segredo ao processo, pois recebe uma estego-imagem não saberá sequer o tamanho da imagem secreta, a princípio. Além disso, para descobrir qual é a imagem secreta é necessário que antes se descubra quais são suas dimensões. Os *bits* que compõem o valor de cada dimensão da imagem secreta são inseridos diretamente nos *bits* menos significativos de *pixels* aleatórios da imagem de cobertura, no princípio do processo.

Outro ponto relevante é a marcação de *pixels* visitados. Na execução da esteganografia, o método seleciona, por meio da geração de números pseudoaleatórios com base na semente informada, *pixels* da imagem de cobertura. Cada vez que um *pixel* é selecionado, caso não tenha sido visitado ainda, ele é marcado como visitado. O conhecimento acerca dos *pixels* já visitados pelo método é necessário, pois assim se evitará

que um *pixel* que já possui informação sobre a presença ou não de dados secretos tenha essa informação de sinalização sobrescrita por outra comparação. Isso tornaria inviável o processo de descoberta da imagem secreta, pois se em uma das visitas o *bit* sinalizador informar que há mensagem oculta ali, o *pixel* da imagem recuperada ia ser recomposto com a informação de outro *pixel* não correspondente àquele, pois sua informação poderia ter sido sobrescrita e perdida

A próxima etapa é a geração do *bit* sinalizador de informação oculta e a comparação entre o *pixel* que deve ser ocultado e o *pixel* de cobertura. Se os *bits* que se deseja ocultar forem iguais aos da área útil do *pixel* de cobertura, nas posições adequadas necessárias para a cobertura, o *bit* sinalizador assume o valor selecionado para a presença de informação e o *pixel* de cobertura é marcado como visitado. Se não forem, o *pixel* de cobertura é marcado como visitado e outro é selecionado aleatoriamente. Para cada *pixel* da imagem secreta a ser ocultado, serão percorridos tantos *pixels* da imagem de cobertura quanto forem necessários, até que sua informação secreta seja incorporada à imagem de cobertura. Na Figura 26 é ilustrado o procedimento geral de esteganografia do LSBR.

Figura 26 – Procedimento geral de esteganografia do LSBR.



Fonte: autoria própria (2017).

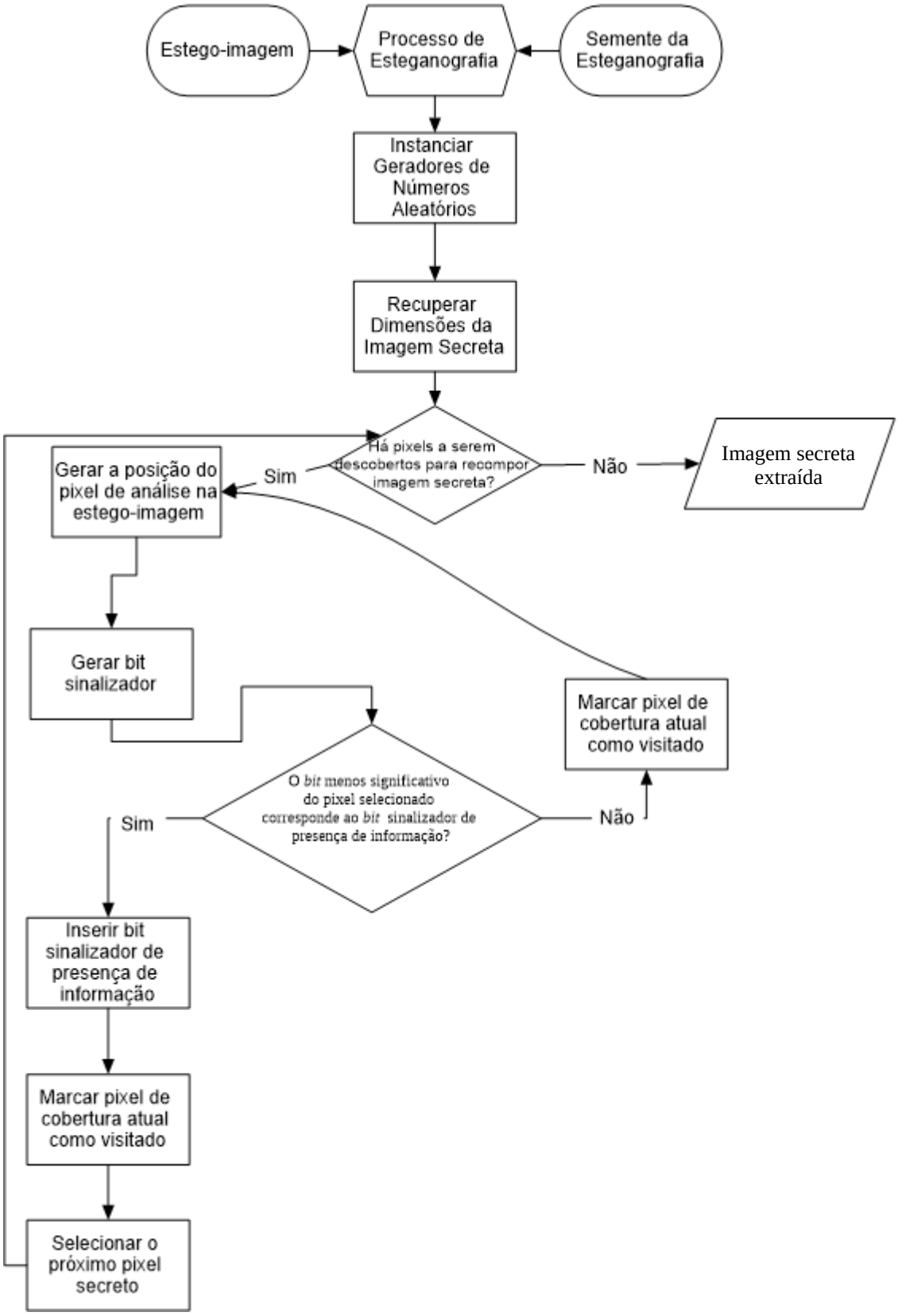
Após a finalização do processo para cada *pixel* da imagem secreta, ela estará incorporada à imagem de cobertura.

3.2.2 Processo reverso de esteganografia baseada no LSBR

O processo reverso de esteganografia consiste na extração da imagem secreta que está oculta nos *pixels* de uma imagem de cobertura. Esse processo consiste, em primeiro lugar, na extração das dimensões da imagem secreta que estão ocultas na imagem de cobertura. Para isso, a mesma sequência aleatória do processo de esteganografia é gerada, de forma que os *pixels* da imagem de cobertura são percorridos nesta sequência. A cada *pixel* visitado, o *bit* menos significativo é extraído para compor uma dimensão em formato binário. As dimensões são extraídas na sequência em que foram ocultadas, isto é, se a altura foi ocultada primeiro, então ela será extraída primeiro. Da mesma forma para a largura. As dimensões da imagem secreta devem ser extraídas para que a imagem secreta seja recuperada, baseando-se no seu tamanho.

Após o conhecimento das dimensões da imagem secreta, cada *pixel* desta deve ser recuperado. Para cada *pixel* a ser recuperado, percorre-se a mesma sequência de *pixels* na imagem de cobertura. A cada *pixel* da imagem de cobertura visitado, sorteia-se um *bit* sinalizador para presença de informação oculta e verifica-se se seu valor é igual ao *bit* menos significativo do *pixel* de cobertura visitado. Se for, os *bits* da área útil do *pixel* de cobertura são recuperados para formar o *pixel* atual da imagem secreta e o *pixel* de cobertura é marcado como visitado. Se não for, marca-se esse *pixel* da imagem de cobertura como visitado e outro *pixel* de cobertura é selecionado para continuar a busca. Para cada *pixel* da imagem secreta a ser recuperado, são percorridos tantos *pixels* de cobertura quanto forem necessários, até que se ache a informação oculta. Na Figura 27 é ilustrado o processo reverso da esteganografia baseada no LSBR.

Figura 27 – Processo reverso da esteganografia baseada no LSBR.



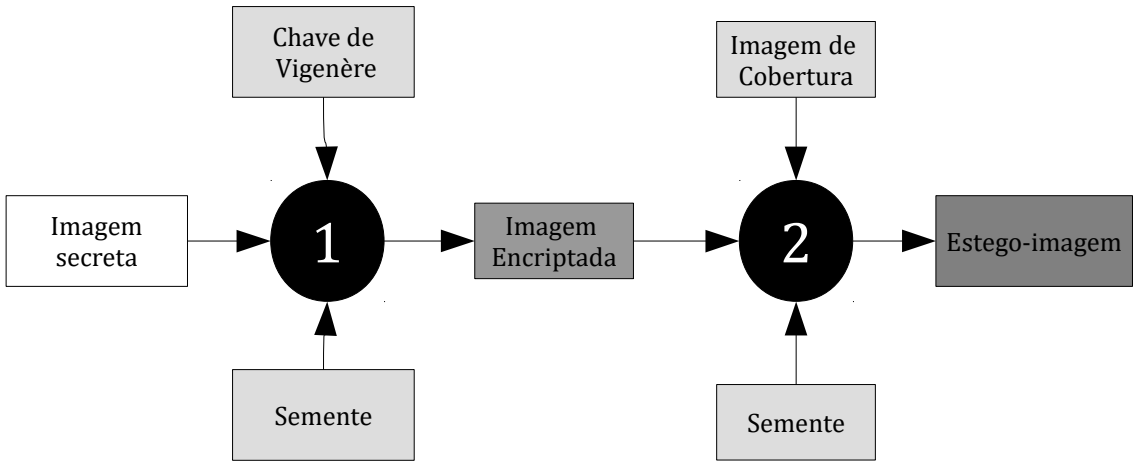
Fonte: autoria própria (2017).

Após o procedimento de descoberta realizado para cada pixel da imagem secreta, ela estará recuperada.

3.3 VISÃO GLOBAL

O método LSBR é baseado na junção de criptografia e esteganografia, possuindo um procedimento de global de ocultação de imagens e outro de extração. O procedimento global para a ocultação de imagens pelo LSBR é ilustrado na Figura 28,

Figura 28 – Procedimento global para ocultação de imagens pelo LSBR.

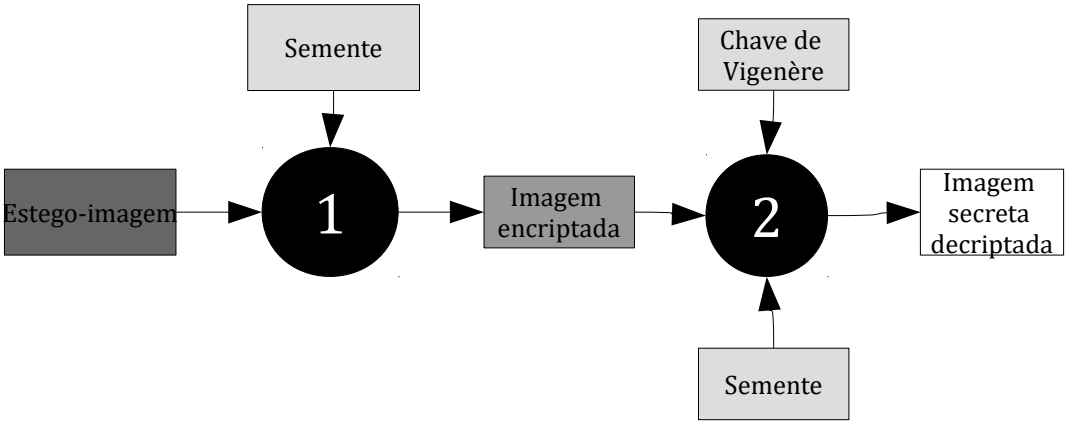


Fonte: autoria própria (2017).

em que 1 é o processo de criptografia mostrado na Figura 15 e 2 é o processo de esteganografia mostrado na Figura 26.

No procedimento global de ocultação, a etapa de criptografia antecede a etapa de esteganografia. Dessa forma, a etapa de esteganografia atuará sobre uma imagem encriptada, produto da etapa de criptografia. O procedimento global para extração de imagens secretas pelo LSBR é ilustrado na Figura 29,

Figura 29 – Procedimento global para extração de imagens pelo LSBR.

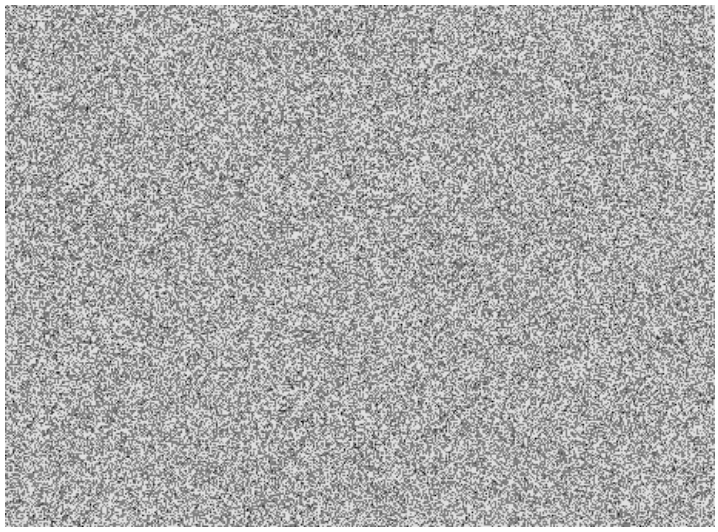


Fonte: autoria própria (2017).

em que 1 é o processo reverso de esteganografia mostrado na Figura 27 e 2 é o processo reverso de criptografia mostrado na Figura 21.

No procedimento global de extração, após essa ação é realizada a decriptação da imagem extraída. Caso a decriptação não ocorra, a imagem extraída será como a imagem da Figura 30, formada por ruído.

Figura 30 – Imagem extraída sem ser decriptada.



Fonte: autoria própria (2017).

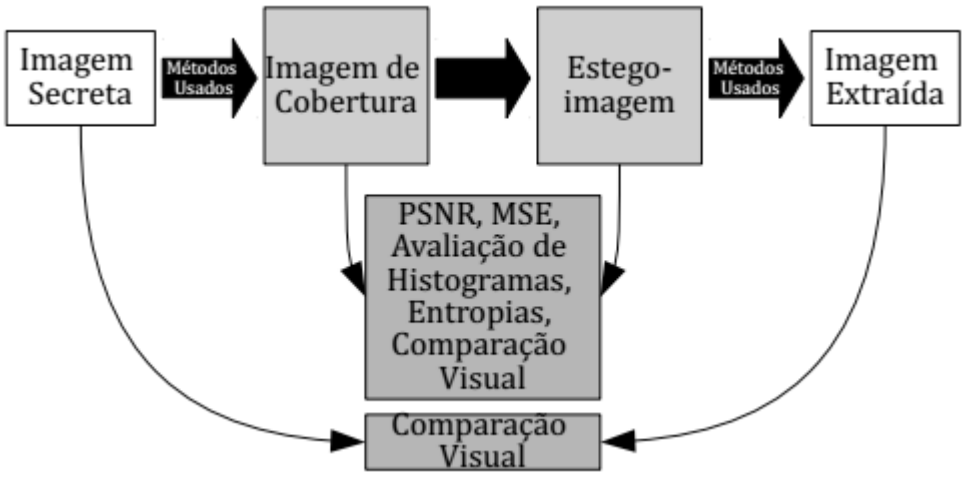
Isso justifica-se pelo fato de que a imagem secreta que é incorporada a uma imagem de cobertura está encriptada, sendo necessário que reverta essa criptografia para ela ser visualizada em sua forma original.

4 METODOLOGIA

Neste capítulo é apresentada a metodologia adotada para a realização dos testes de criptografia e esteganografia com os métodos LSBR, LSB *Replacement* e LSB *Matching*. Para a realização dos testes, foram escolhidos dois conjuntos de imagens, sendo um constituído por seis imagens de cobertura e outro constituído por seis imagens secretas. Todas as imagens usadas nesses testes foram obtidas do banco de imagens Caltec 101 (FEI-FEI; FERGUS; PERONA, 2004). Esse banco é composto por 9144 imagens distribuídas em várias categorias. A resolução média dessas imagens é 300 x 200 *pixels*.

A metodologia dos testes consiste em criar cinco conjuntos de testes com duas imagens cada, de forma que a imagem secreta deve ser incorporada à imagem de cobertura para gerar uma estego-imagem. Nesse momento a estego-imagem gerada é comparada à imagem de cobertura para que as métricas de avaliação sejam obtidas. Essas métricas são o PSNR e o MSE. Além disso, as entropias da imagem gerada e da imagem original são calculadas, além de suas diferenças. Os histogramas da imagem original e da estego-imagem também são gerados, para que uma avaliação perceptual possa ser realizada. A imagem secreta é extraída pelo processo de extração dos métodos e comparada visualmente com a imagem secreta original. Um esquema da metodologia de testes é apresentado na Figura 31.

Figura 31 – Metodologia de testes.



Fonte: autoria própria (2017).

As imagens usadas no conjunto de imagens de cobertura foram ampliadas, pois o método LSBR necessita que cada *pixel* da imagem secreta tenha liberdade para visitar n

pixels da imagem de cobertura até que seja incorporado. Além disso, as imagens usadas nos testes estão em sua versão escala de cinza. A relação desejável entre os tamanhos das imagens de cobertura e secreta no LSBR é dada pela Equação 5,

$$Nc = n \times Ns \tag{5}$$

em que n representa o número médio de *pixels* visitados na imagem de cobertura por cada *pixel* secreto no momento da incorporação. Para os métodos LSB *Matching* e LSB *Replacement*, a relação entre os tamanhos das imagens pode ser expressa pela Equação 5, em que n é o número de *bits* secretos por *pixel* secreto que se deseja ocultar na imagem de cobertura. Ainda na Equação 5, *Nc* representa o número de *pixels* da imagem de cobertura e *Ns* o número de *pixels* da imagem secreta. As imagens do grupo de imagens de cobertura estão representadas na Figura 32.

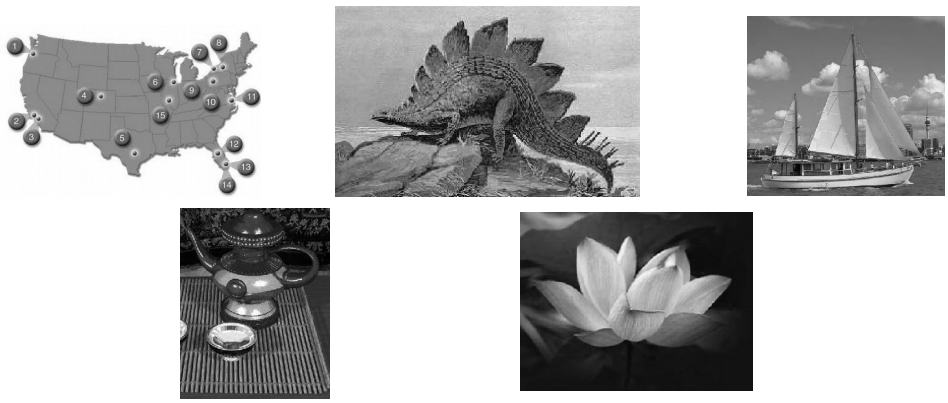
Figura 32 – Conjunto de imagens de Cobertura.



Fonte: Fei-Fei, Fergus e Perona (2004)

As imagens utilizadas como imagens secretas estão representadas na Figura 33.

Figura 33 – Conjunto de imagens secretas.



Fonte: Fei-Fei, Fergus e Perona (2004)

Cada uma das imagens dos dois conjuntos foi convertida para o formato PNG para que fossem utilizadas nos testes, embora outros formatos possam ser utilizados. Além disso, as imagens do conjunto de imagens de cobertura receberam um *zoom* de 5 vezes nas suas dimensões normais para que o LSBR tivesse liberdade para visitar os *pixels* da imagem de cobertura a cada passo de sua execução. Os testes dos métodos foram realizados utilizando o IDE NetBeans 8.2, onde as aplicações foram desenvolvidas utilizando-se Java.

4.1 MÉTRICAS DE AVALIAÇÃO

Os testes realizados foram avaliados e comparados com base em medidas numéricas e visualmente. Com relação às medidas numéricas, foram usadas a Entropia, o MSE e o PSNR.

4.1.1 Entropia (Entropia de Shannon)

A entropia pode medir a informação contida em uma mensagem (PINEDA, 2006). A Entropia de Shannon é definida pela Equação 6,

$$H = -K \sum_{i=1}^{n} p_i \log(p_i) \tag{6}$$

em que K é uma constante arbitrária e p_i é a probabilidade de ocorrência de um evento. Em uma imagem, a probabilidade de ocorrer um *pixel* com valor 10 é igual à quantidade de *pixels* com valor 10 dividida pela quantidade de *pixels* totais.

De acordo com o crescimento da probabilidade de ocorrência de um grupo de símbolos em detrimento de outros em um conjunto, a entropia decresce. A máxima entropia em um conjunto de símbolos é alcançada quando todos os símbolos do conjunto possuem a mesma probabilidade de ocorrência. No momento em que um símbolo de um conjunto possui probabilidade de ocorrência de 100%, a entropia tende a zero (ASSIRATI, 2014).

Em relação à imagens, os símbolos envolvidos na análise de Entropia de Shannon são as intensidades dos *pixels*, isto é, símbolos pertencentes ao conjunto C = [0, 255]. Quanto menos variação de intensidades houver em uma imagem, menor será sua entropia, pois como definido anteriormente, a entropia tende a zero sempre que a probabilidade de ocorrência de um símbolo tende a 100%.

4.1.2 *Mean squared error* (MSE)

O MSE é o *Mean Squared Error* ou Erro Médio Quadrático. Para Al-najjar e Soong (2012), o MSE está entre as medidas de qualidade de imagens mais comumente usadas. O MSE calcula o erro médio quadrático existente entre os *pixels* de uma imagem original e sua versão modificada (como com acréscimo de ruído ou incorporação de dados por esteganografia, por exemplo), podendo ser calculado pela Equação 7,

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (7)$$

em que I(i, j) e K(i, j) são respectivamente os valores dos *pixels* da posição (i, j) das imagens I e K, sendo que m e n são as dimensões da imagem.

4.1.3 *Peak Signal-to-Noise Ratio* (PSNR)

Segundo Begazo (2012), o PSNR é uma métrica utilizada de forma ampla pela comunidade científica. Essa métrica define a relação entre a máxima energia possível em um sinal e o ruído que afeta esse sinal. Bhattacharya, Dey e Chaudhuri (2012) definem o *Peak Signal-to-Noise Ratio* (PSNR) como uma métrica de desempenho usada para determinar a transparência perceptual de uma imagem portadora de dados secretos em relação à imagem de cobertura. O PSNR é calculado por meio da Equação 8,

$$PSNR = 10 \cdot \log_{10}\left(\frac{S^2}{MSE}\right) \quad (8)$$

em que S é o valor máximo que pode ser alcançado pelos elementos da amostra. Considerando-se imagens com 256 níveis de cinza, o valor de S é 255, pois esse é o maior valor pertencente ao intervalo *I = [0, 255]* (ALBUQUERQUE, 2008).

Segundo Veldhuizen (1998), o PSNR é medido em decibels (dB). Para Begazo (2012), o PSNR possui uma faixa de valores que varia de 0 a 100, de forma que quanto maior o valor, melhor a qualidade medida. Segundo Valenzuela (2011), a métrica Média de Opinião (MOS)

avalia a qualidade de vídeos atribuindo pontuações que variam de 1 a 5. Quanto maior a pontuação, maior a qualidade do vídeo e de sua imagem. O Quadro 4 ilustra a métrica MOS.

Quadro 4: Métrica MOS.

Pontuação	Qualidade Atribuída	Prejuízo de Imagem
5	Excelente	Imperceptível
4	Ótimo	Perceptível, com pouca distorção
3	Bom	Ligeira Distorção
2	Regular	Distorção Irritante
1	Ruim	Grave Distorção

Fonte: Adaptado de Valenzuela (2011).

Há uma relação entre a métrica MOS e o PSNR. Essa relação é ilustrada pelo Quadro 5.

Quadro 5: Relação entre o PSNR e a métrica MOS.

PSNR (dB)	MOS
>37	5 (Excelente)
31 - 37	4 (Ótimo)
25 - 31	3 (Bom)
20 - 25	2 (Regular)
< 20	1 (Ruim)

Fonte: Adaptado de Valenzuela (2011).

Assim, como a qualidade da métrica MOS está relacionada com a qualidade das imagens de vídeo, a partir do Quadro 5 uma imagem pode ser classificada com boa qualidade visual para valores de PSNR acima de 37dB.

4.2 AVALIAÇÃO PERCEPTUAL

A avaliação perceptual consiste na verificação das características visuais e de distribuição de frequências de intensidades entre imagens. A avaliação perceptual realizada nos testes baseia-se na comparação visual entre imagem de cobertura e estego-imagem, assim como na comparação entre imagens secretas extraídas em cada método.

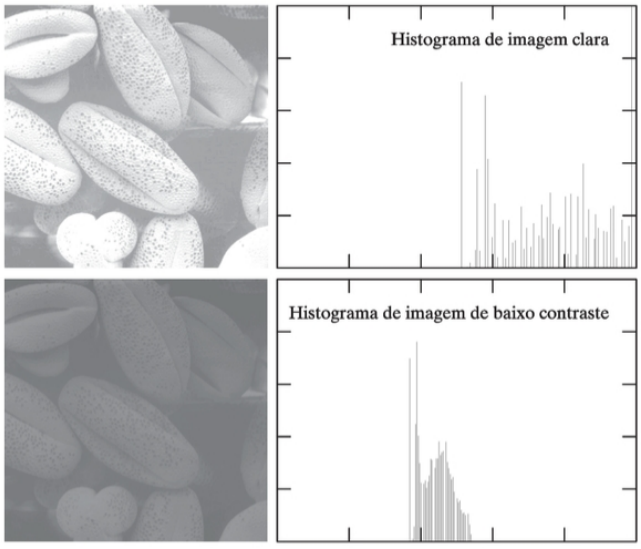
A avaliação perceptual dos histogramas das imagens envolvidas foi escolhida como uma das formas de análise dos resultados obtidos. Segundo Gonzalez e Woods (2010), o

histograma de uma imagem digital cujos níveis de intensidade pertencem ao intervalo *I = [0, 255]* pode ser definido como uma função discreta $h(r_k) = n_k$. Nessa definição, r_k é o k-ésimo valor de intensidade e n_k é o número de *pixels* presentes na imagem com intensidade igual a r_k.

Os histogramas são tidos como base para inúmeras técnicas para processamento de imagens no domínio espacial. Os histogramas podem ser manipulados para a realização de realce nas imagens, para o fornecimento de estatísticas da imagem, além de serem úteis em aplicações como compressão e segmentação de imagens (GONZALEZ; WOODS, 2010).

Algumas imagens com seus respectivos histogramas de intensidade são ilustradas na Figura 34.

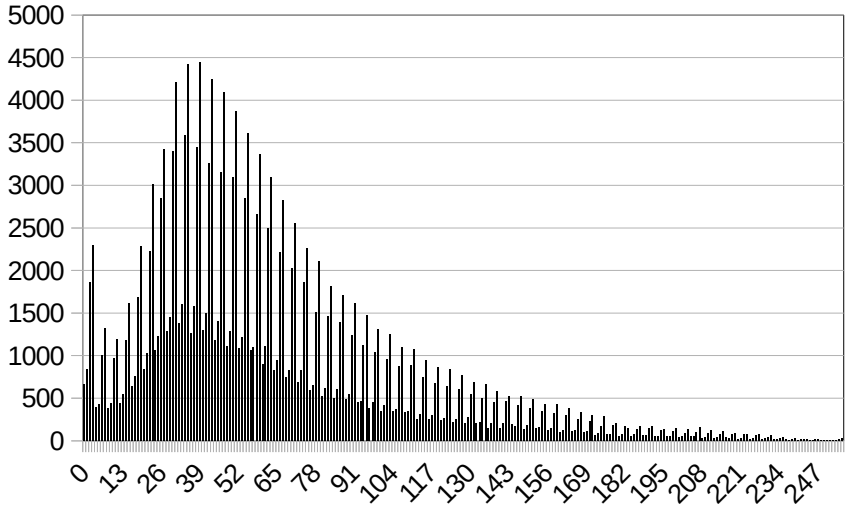
Figura 34 – Imagens e seus histogramas.



Fonte: Gonzalez e Woods (2010)

A avaliação realizada por meio do uso de histogramas será verificar imagens de cobertura e estego-imagens em conjunto com seus respectivos histogramas, buscando-se encontrar similaridades ou diferenças entre eles. Quanto mais fiel ao histograma original for o histograma da estego-imagem, melhor é o resultado da incorporação de *bits*, pois perturbações como a da Figura 35 serão evitadas.

Figura 35 – Anomalias na distribuição de frequências.



Fonte: autoria própria (2017)

Essas perturbações consistem em valores discrepantes entre intensidades vizinhas, de uma forma intermitente. Quanto maiores forem essas perturbações, maior será a diferença entre os histogramas das imagens. Além disso, elas podem indicar que houve alguma modificação na imagem, sendo desejável evitá-las.

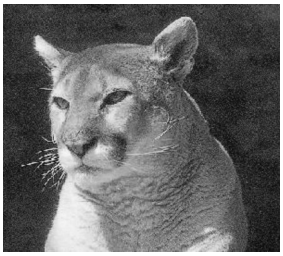
5 RESULTADOS

Neste capítulo são apresentados os resultados obtidos dos testes aplicados aos conjuntos de imagens adotados. São apresentados os resultados de cinco testes e, ao final, é feita uma discussão dos resultados obtidos.

5.1 CONFIGURAÇÃO DE TESTE 1

A Configuração de Teste 1 foi realizado utilizando-se uma imagem do conjunto de imagens de cobertura e uma do conjunto de imagens secretas. Foram realizadas três incorporações da imagem secreta à imagem de cobertura e três extrações, sendo uma operação para cada método. As imagens utilizadas no teste 1 estão representadas na Figura 36. O método de realização das análises foi o mesmo para cada teste realizado.

Figura 36 – Imagens usadas no teste 1.



(a) Imagem de cobertura



(b) Imagem secreta

Fonte: Fei-Fei, Fergus e Perona (2004)

No processo de incorporação, foi aplicado o algoritmo de criptografia e logo após o algoritmo de esteganografia. Após esse processo, foram geradas três estego-imagens, uma por cada método. Essas imagens estão representadas na Figura 37.

Figura 37 – Estego-imagens geradas.

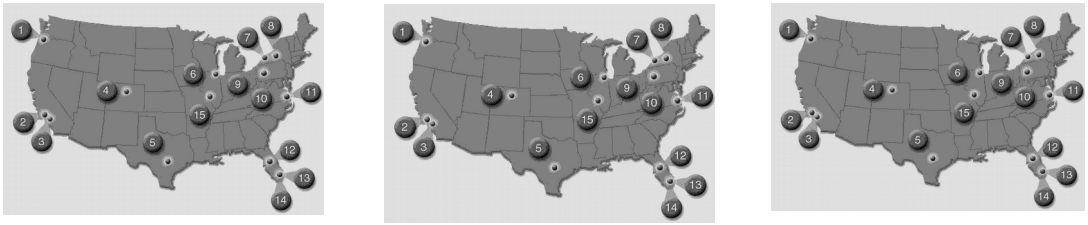


(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

Com a análise visual da Figura 37 é possível perceber a semelhança existente entre a imagem original e as estego-imagens. Visualmente, nada há nessas imagens que indique que elas passaram por uma modificação e escondem dados. Na continuação do teste, essas estego-imagens foram submetidas ao processo de extração. Cada uma dessas imagens secretas foi extraída pelo processo reverso ao que incorporou os dados. O resultado dessas operações de extração é apresentado na Figura 38.

Figura 38 – Imagens secretas extraídas.



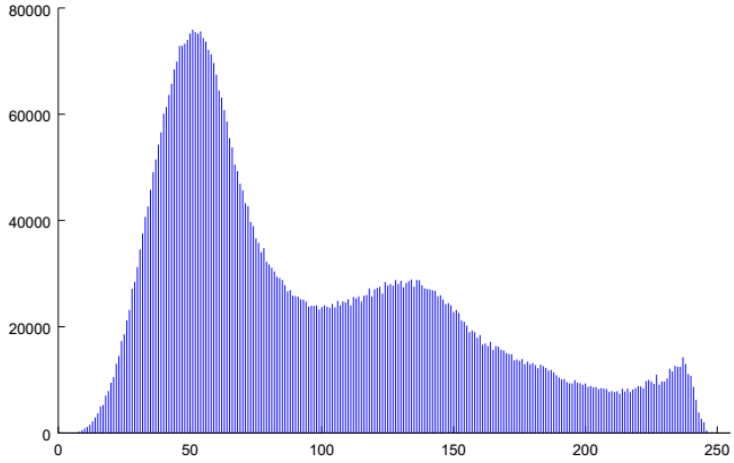
(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

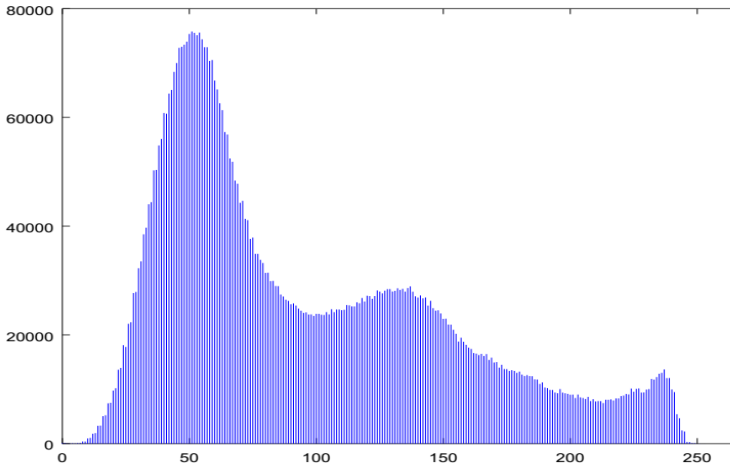
Essas imagens possuem similaridade visual entre si, uma vez que são formadas pelos mesmos *bits* em cada *pixel*. Em relação à sua similaridade com a imagem secreta original, elas perderam qualidade, uma vez que para todos os testes, apenas os três *bits* mais significativos de cada imagem secreta foram ocultados. Isso faz com que no processo de extração, cada um de seus *pixels* perca cinco *bits* de informação, uma vez que apenas três serão recuperados. Considerando que as características gerais da imagem secreta sejam o essencial em uma comunicação secreta, os três métodos obtiveram um bom resultado, uma vez que a imagem recuperada pelos três possui semelhança com a imagem secreta original.

Com relação à avaliação perceptual do histograma de frequências, percebe-se que o LSBR obteve um desempenho superior aos outros métodos, uma vez que o histograma da estego-imagem gerada por ele foi o que mais se aproximou da distribuição de frequências da imagem de cobertura original. Esse resultado pode ser visto na Figura 39. O padrão de espaçamento entre as barras de frequências existente nos histogramas dos métodos LSB *Matching* e LSB *Replacement* pode causar desconfiança, por parte de quem está analisando essa imagem, sobre o conteúdo da mesma.

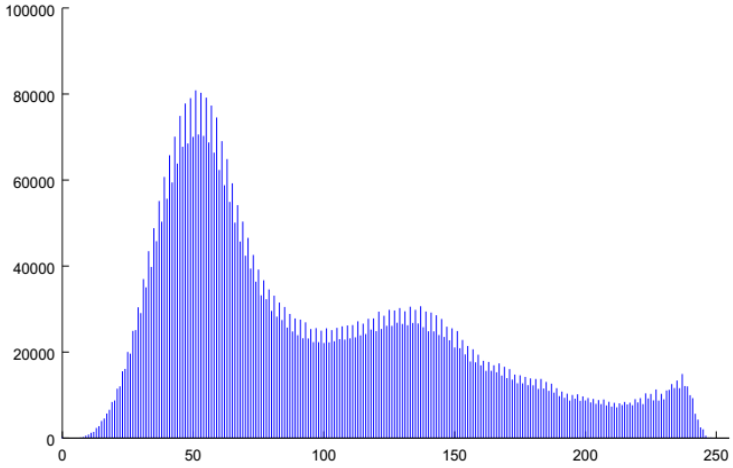
Figura 39 – Histograma da imagem original X Histograma das estego-imagens.



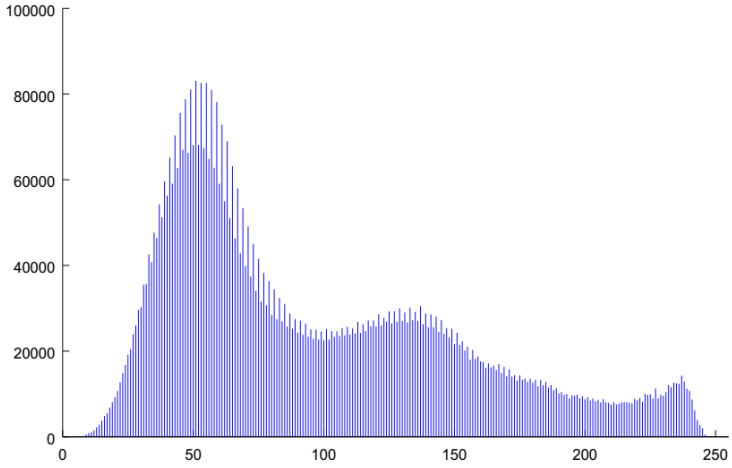
(a) Histograma da imagem de cobertura.



(b) Histograma da estego-imagem gerada pelo LSBR.



(c) Histograma da estego-imagem gerada pelo LSB *Matching.*



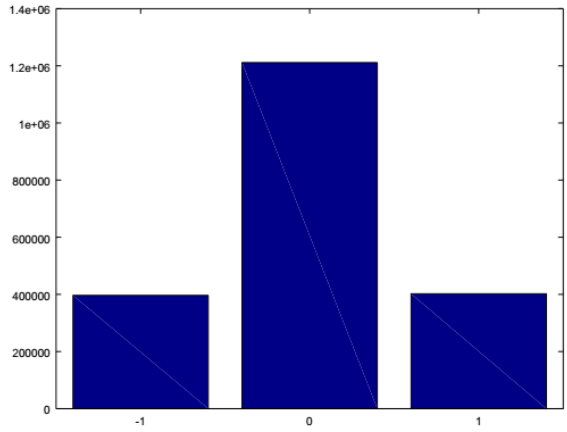
(d) Histograma da estego-imagem gerada pelo LSB *Replacement*

Fonte: autoria própria (2017).

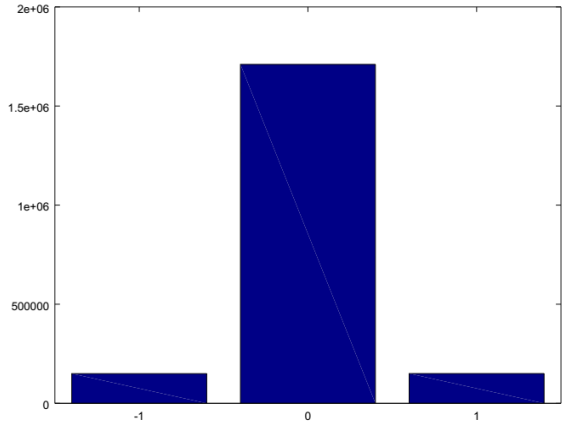
Avaliando graficamente a diferença entre estego-imagens e imagens de cobertura originais, percebe-se que o LSB *Replacement* e o LSB *Matching* geraram imagens que possuem mais semelhança com a imagem de cobertura. Os gráficos apresentados na Figura 40 são os histogramas de frequências dos valores resultantes da operação de subtração entre a estego-imagem e a imagem de cobertura. Nesse gráfico, os valores presentes na categoria -1 indicam a quantidade de *pixels* da estego-imagem que sofreram redução na sua intensidade original. Os valores presentes na categoria +1 referem-se à quantidade de *pixels* da estego-imagem que tiveram sua intensidade aumentada em relação ao valor original. Os valores 0 indicam a quantidade de *pixels* que não sofreram alteração em suas intensidades. A situação ótima nessa análise é que se encontre um cenário onde o número de zeros no gráfico seja

maximizado, indicando que a imagem de cobertura foi pouco modificada para se obter a estego-imagem.

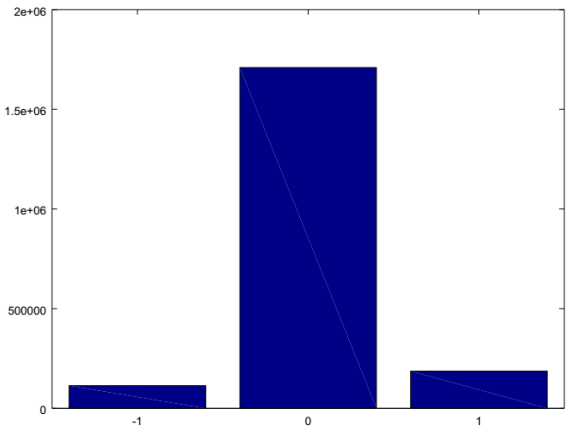
Figura 40 – Valor da diferença entre imagens originais e estego-imagens.



(a) Diferença entre a imagem de cobertura e a estego-imagem do LSBR



(b) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Matching.*



(c) Diferença entre a imagem original e a estego-imagem do LSB *Replacement.*

Fonte: autoria própria (2017).

No caso em análise, os valores dos zeros para o LSB *Replacement* e LSB *Matching* são mais elevados pois a quantidade de *pixels* de cobertura que permaneceram iguais após a incorporação de uma imagem foi elevada. Nesse ponto de avaliação, o LSB *Replacement* e o LSB *Matching* foram melhores, pois mantiveram mais *pixels* idênticos aos da imagem de cobertura original.

As medidas de desempenho encontradas para esse teste estão representadas na Tabela 1.

Tabela 1 – Métricas obtidas (Teste 1).

	MSE	**PSNR (dB)**	**Entropia da imagem original**	**Entropia da estego-imagem**	**Diferença de Entropia**
LSB com Rejeição	0,3974	52,139	7,5317	7,5322	0,0005
LSB *Matching*	0,14921	56,393	7,5317	7,529	-0,0027
LSB *Replacement*	0,1495	56,384	7,5317	7,528	-0,0037

Fonte: autoria própria (2017).

Para as medidas do MSE, o LSBR teve um desempenho pior. O valor mais elevado de MSE encontrado para esse método explica o fato de ele ter gerado uma menor quantidade de *pixels* iguais aos da imagem de cobertura após o processo de esteganografia. Com relação ao PSNR, o LSBR obteve valores mais baixos, devido ao seu MSE mais elevado. No entanto, esses valores não trazem diferença para o visualizador, pois pelo Quadro 5 essa faixa de valores está em uma região de boa qualidade de imagem.

Com relação à entropia, o LSBR fez com que sua estego-imagem aumentasse a sua entropia em relação à imagem de cobertura, enquanto que os outros métodos fizeram a entropia diminuir. Uma conclusão que pode ser tirada para essa situação é que o LSB *Replacement* e o LSB *Matching* tornaram a distribuição de frequências da nova imagem mais previsível, de forma que alguns elementos da imagem podem possuir uma probabilidade de ocorrência maior em detrimento de outros. Isso pode contribuir para a suposição de que há algo escondido nessa imagem, pois elementos com probabilidade de ocorrência em destaque podem levantar suspeita, ao contrário de um conjunto de elementos que possuem probabilidades de ocorrência próximas entre si.

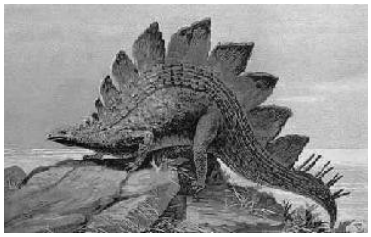
5.2 CONFIGURAÇÃO DE TESTE 2

Para a Configuração de Teste 2, foram utilizadas as imagens ilustradas na Figura 41.

Figura 41 – Imagens usadas no teste 2.



(a) Imagem de cobertura



(b)Imagem secreta

Fonte: Fei-Fei, Fergus e Perona (2004)

Após o processo de incorporação foram geradas três estego-imagens, uma por cada método. Essas imagens estão representadas na Figura 42.

Figura 42 – Estego-imagens geradas.



(a) LSBR



(b) LSB *Matching*

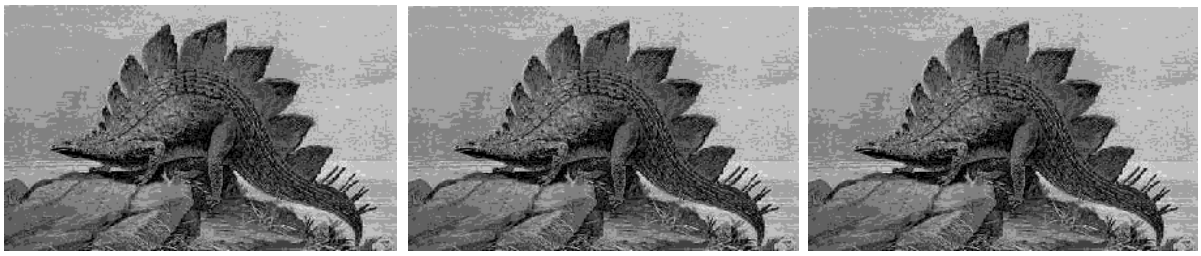


(c) LSB *Replacement*

Fonte: autoria própria (2017).

É possível perceber a semelhança existente entre a imagem original e as estego-imagens. Essa constatação atesta que os três métodos podem ser equiparados nesse caso. Na continuação do teste, essas estego-imagens foram submetidas ao processo de extração. O resultado dessas operações de extração é apresentado na Figura 43.

Figura 43 – Imagens secretas extraídas.



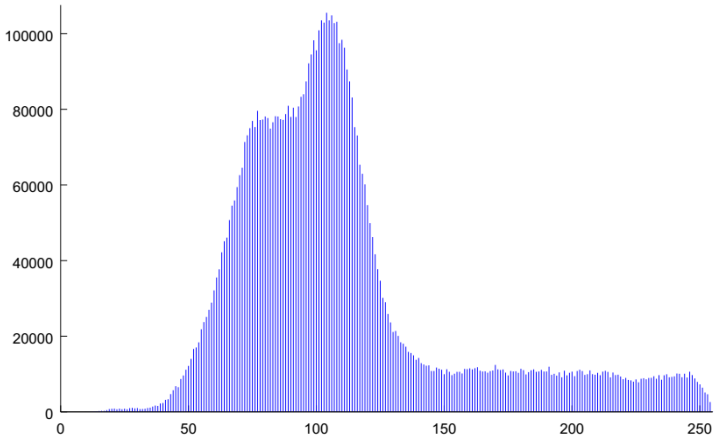
(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

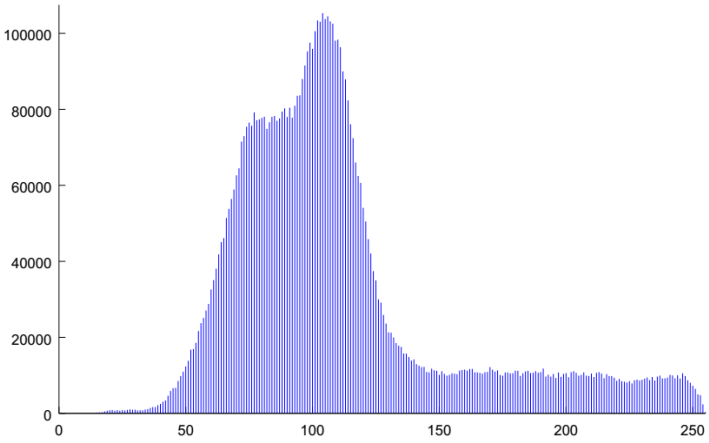
Essas imagens possuem similaridade visual entre si, uma vez que são formadas pelos mesmos *bits* em cada *pixel*. Em relação à sua similaridade com a imagem secreta original, elas também perderam qualidade, devido ao fato de que apenas os três *bits* mais significativos de cada imagem secreta foram ocultados nesse teste. Considerando que as características gerais da imagem secreta foram mantidas após a extração, os três métodos obtiveram um bom resultado, uma vez que a imagem recuperada pelos três possui semelhança com a imagem secreta original.

Com relação à avaliação perceptual do histograma de frequências das estego-imagens geradas pelos três métodos, percebe-se que o LSBR obteve um desempenho próximo ao dos outros métodos, uma vez que o histograma da estego-imagem gerada por este método está visualmente semelhante ao histograma da imagem de cobertura, em conjunto com os outros métodos. Esse resultado pode ser visto na Figura 44. Neste teste não ocorreu o padrão de espaçamento entre as barras de frequências existente nos histogramas dos métodos LSB *Matching* e LSB *Replacement*, como no teste anterior.

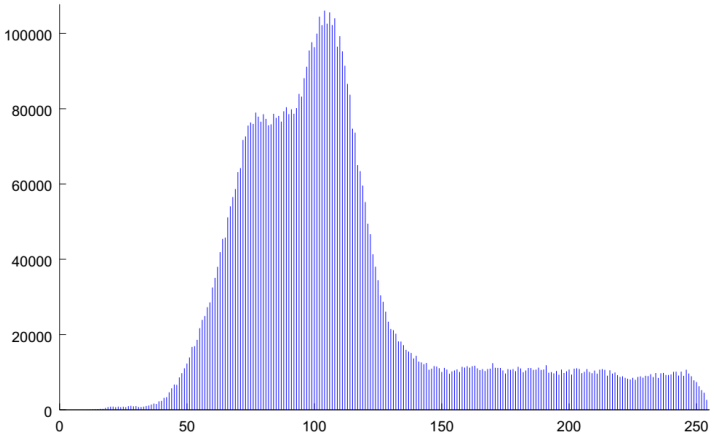
Figura 44 – Histograma da imagem original X Histograma das estego-imagens.



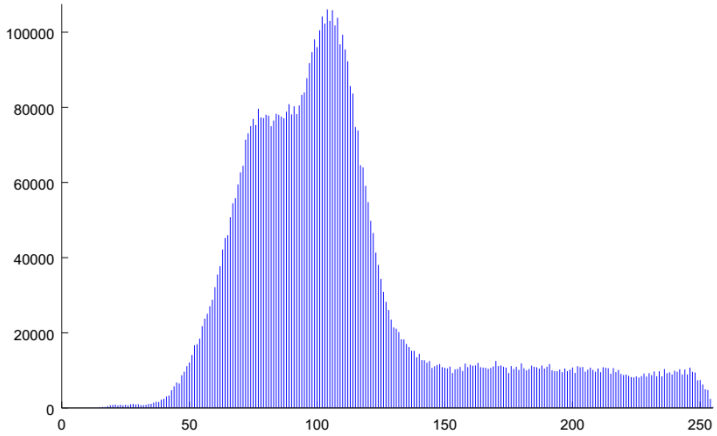
(a) Histograma da imagem de cobertura



(b) Histograma da estego-imagem gerada pelo LSBR



(c) Histograma da estego-imagem gerada pelo LSB *Matching*

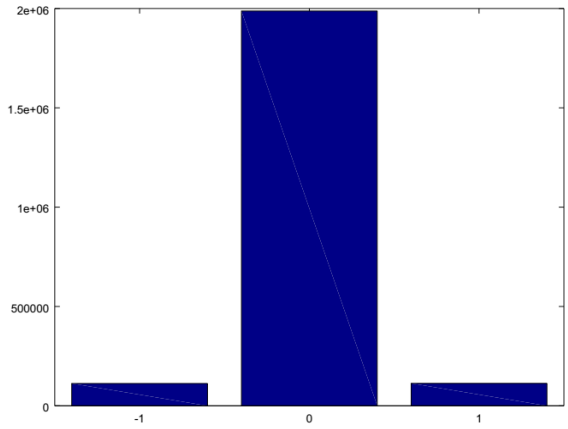


(d) Histograma da estego-imagem gerada pelo LSB *Replacement.*

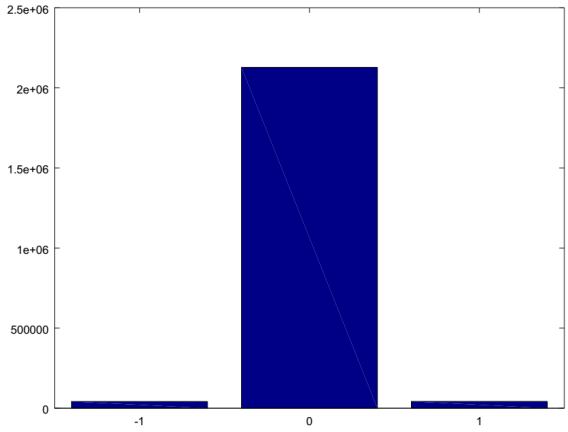
Fonte: autoria própria (2017).

Avaliando graficamente a diferença entre estego-imagens e imagem de cobertura original por meio da Figura 45, percebe-se que o LSBR gerou um número de modificações de *pixels* maior que o dos outros métodos.

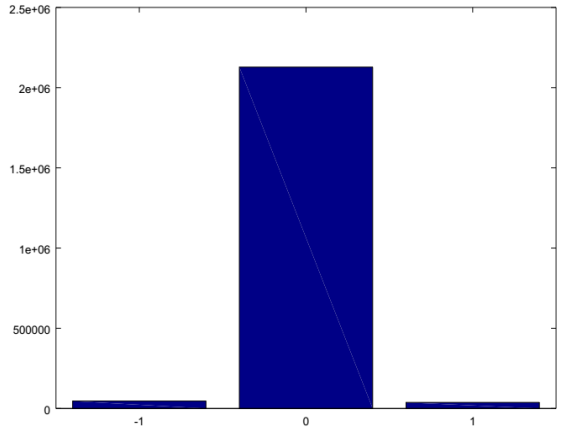
Figura 45 - Valor da diferença entre imagens originais e estego-imagens.



(a) Diferença entre a imagem de cobertura e a estego-imagem do LSBR



(b) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Matching*



(c) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Replacement*

Fonte: autoria própria (2017).

Nesse ponto de avaliação, o LSB *Replacement* e o LSB *Matching* foram melhores, pois modificaram menos *bits* na imagem de cobertura durante o processo de incorporação. As medidas de desempenho encontradas para esse teste estão representadas na Tabela 2.

Tabela 2 – Métricas obtidas (Teste 2).

	MSE	**PSNR (dB)**	**Entropia da imagem original**	**Entropia da estego-imagem**	**Diferença de Entropia**
LSB com Rejeição	0,1017	58,054	7,1275	7,1279	0,0004
LSB *Matching*	0,0382	62,305	7,1275	7,1276	1E-04
LSB *Replacement*	0,0381	62,317	7,1275	7,1274	-0,0001

Fonte: autoria própria (2017).

Em relação ao MSE, o LSBR obteve a pior medida, ficando atrás dos outros métodos. A explicação para o fato de o LSBR possuir um MSE maior que os outros métodos é que ele altera mais *bits* da imagem de cobertura. No entanto, devido à proximidade de zero dos valores gerados pelo MSE, nenhum dos métodos alterou a imagem de cobertura de forma contundente. Com relação ao PSNR, o LSB *Replacemen*t e o LSB *Matching* obtiveram o maior valor de desempenho. Entretanto, o valor alcançado pelo LSBR permite que a estego-imagem gerada por esse método se enquadre no conjunto de imagens com boa qualidade visual, de acordo com Quadro 5. Com relação à entropia, o LSBR fez com que sua estego-imagem aumentasse a sua entropia em relação à imagem de cobertura, enquanto que para os outros métodos houve uma diminuição e um aumento em menor proporção.

5.3 CONFIGURAÇÃO DE TESTE 3

Para a Configuração de Teste 3, foram utilizadas as imagens ilustradas na Figura 46.

Figura 46 – Imagens utilizadas no teste 3.



(a) Imagem de cobertura



(b) Imagem secreta

Fonte: Fei-Fei, Fergus e Perona (2004)

Após o processo de incorporação foram geradas três estego-imagens, uma por cada método. Essas imagens estão na Figura 47.

Figura 47 – Estego-imagens geradas.



(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

Há semelhança visual entre a imagem original e as estego-imagens para os métodos testados. Essa constatação atesta que os três métodos atingiram resultados semelhantes nesse caso. Na continuação do teste, essas estego-imagens foram submetidas ao processo de extração. O resultado dessas operações de extração é apresentado na Figura 48.

Figura 48 – Imagens secretas extraídas.



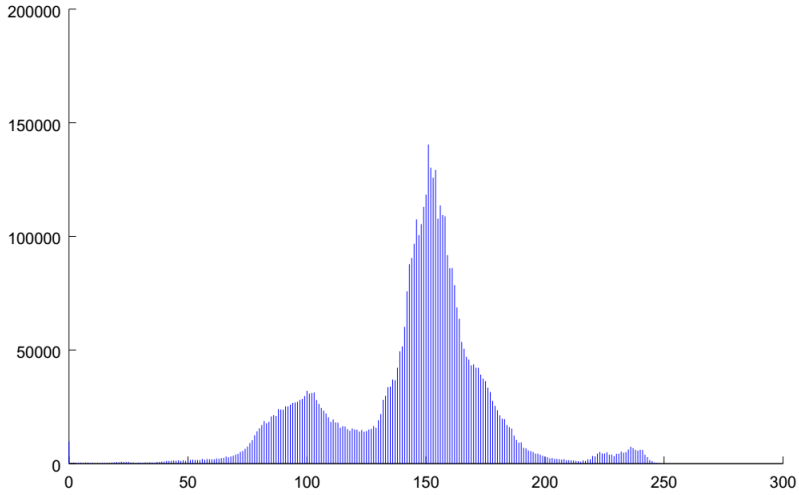
(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

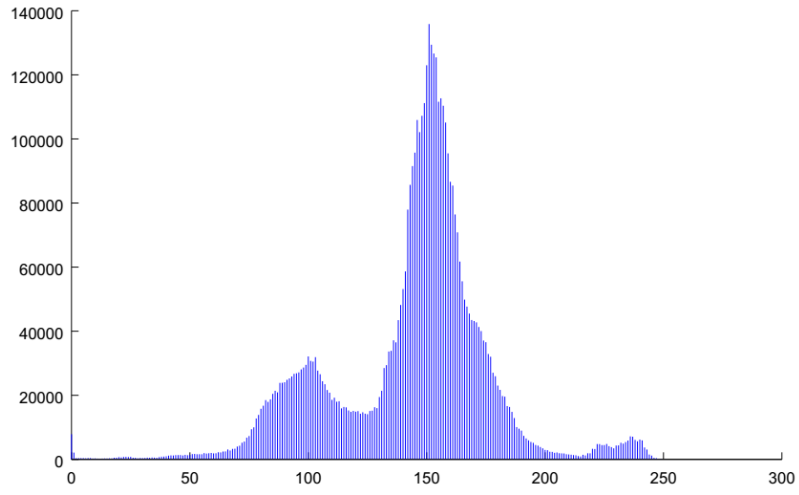
As imagens extraídas por cada um dos métodos mantiveram as características básicas de suas respectivas imagens secretas originais. Houve uma perda de qualidade em razão do uso de apenas três dos *bits* mais significativos de cada *pixel* original no processo de incorporação. Por meio da comparação de características visuais para esse teste, nota-se que os métodos analisados possuem o mesmo poder para extração de dados ocultados em imagens.

Com relação à avaliação perceptual do histograma de frequências das estego-imagens geradas, percebe-se que o LSBR também obteve um desempenho próximo ao dos outros métodos. O histograma de sua estego-imagem está visualmente próximo aos histogramas da imagem de cobertura, da mesma forma para os outros métodos. Esse resultado pode ser visto na Figura 49. Neste teste também não ocorreu o padrão de espaçamento entre as barras de frequências existentes.

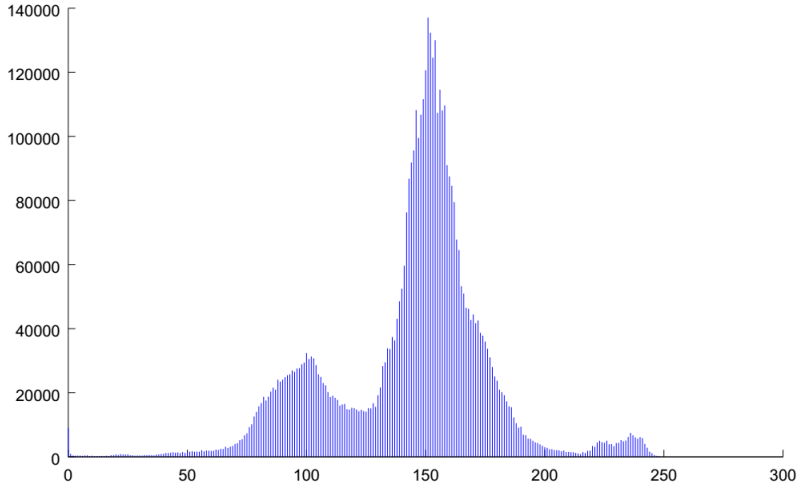
Figura 49 – Histograma da imagem original X Histograma das estego-imagens.



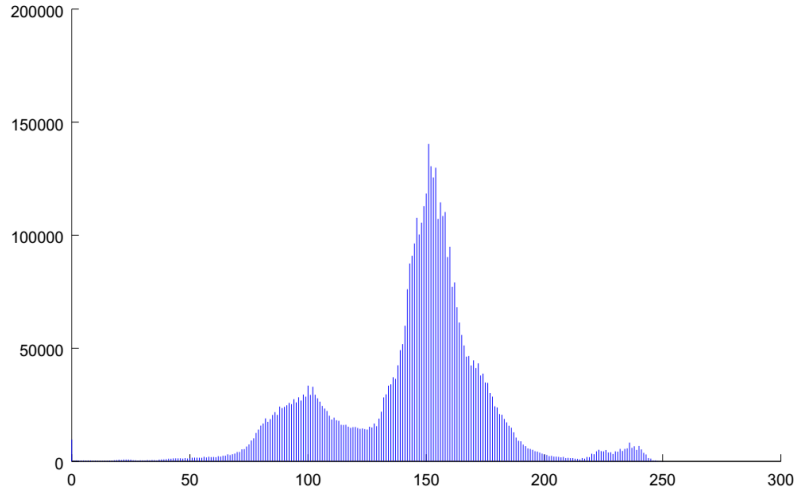
(a) Histograma da imagem de cobertura



(b) Histograma da estego-imagem gerada pelo LSBR



(c) Histograma da estego-imagem gerada pelo LSB *Matching*

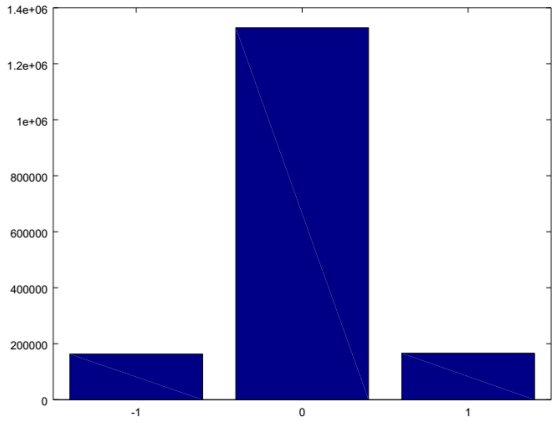


(d) Histograma da estego-imagem gerada pelo LSB *Replacement.*

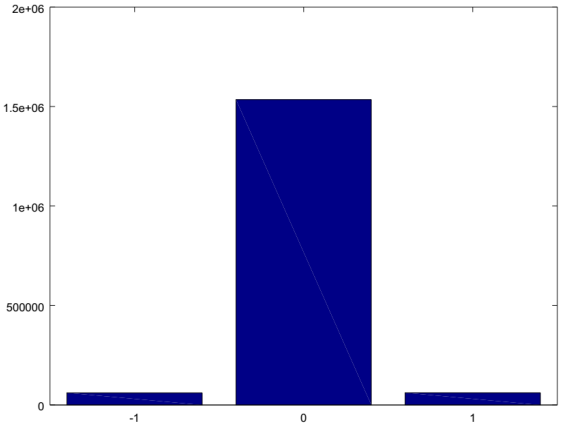
Fonte: autoria própria (2017).

Com relação à diferença gráfica entre estego-imagens e imagem de cobertura original ilustrada na Figura 50, percebe-se que o método que gerou um maior número de modificações de *pixels* foi o LSBR.

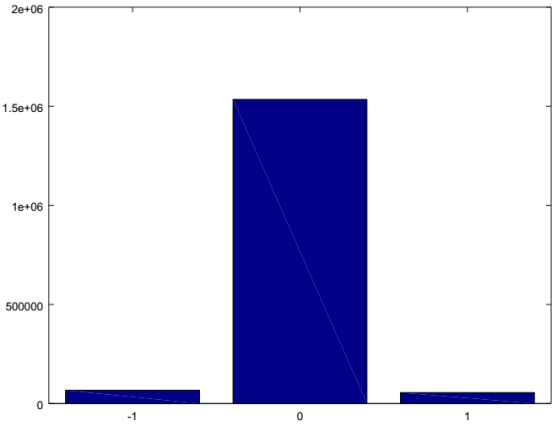
Figura 50 - Valor da diferença entre imagens originais e estego-imagens.



(a) Diferença entre a imagem de cobertura e a estego-imagem do LSBR



(b) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Matching*



(c) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Replacement*.

Fonte: autoria própria (2017)

Nesse ponto de avaliação, o LSB *Replacement* e o LSB *Matching* foram melhores, pois modificaram menos *bits* na imagem de cobertura durante o processo de incorporação.

Esse resultado pode ser visualizado por meio da observação da frequência dos valores diferentes de zero, após a subtração das imagens. Esse valor é maior, para o LSBR, implicando que houve mais modificações nos *pixels* durante a incorporação.

As medidas de desempenho encontradas para esse teste estão representadas na Tabela 3.

Tabela 3 – Métricas obtidas (Teste 3).

	MSE	**PSNR (dB)**	**Entropia da imagem original**	**Entropia da estego-imagem**	**Diferença de Entropia**
LSB com Rejeição	0,1984	55,154	6,7903	6,7926	0,0023
LSB *Matching*	0,0739	59,442	6,7903	6,7911	0,0008
LSB *Replacement*	0,0739	59,439	6,7903	6,7897	-0,0006

Fonte: autoria própria (2017).

Em relação ao MSE, o LSBR obteve a pior medida, ficando atrás dos outros métodos. A explicação para o fato de o LSBR possuir um MSE maior que os outros métodos é que ele altera mais *bits* da imagem de cobertura. Com relação ao PSNR, o LSB *Replacement* e o LSB *Matching* obtiveram o maior valor de desempenho. Entretanto, o valor alcançado pelo LSBR permite que a estego-imagem gerada por esse método se enquadre no conjunto de imagens com boa qualidade visual, de acordo com o Quadro 5. Com relação à entropia, o LSBR fez com que sua estego-imagem aumentasse a sua entropia em relação à imagem de cobertura, enquanto que para os outros métodos houve uma diminuição e um aumento em menor proporção.

5.4 CONFIGURAÇÃO DE TESTE 4

Para a Configuração de Teste 4, foram utilizadas as imagens ilustradas na Figura 51.

Figura 51 – Imagens utilizadas no teste 4.



(a) Imagem de cobertura (b) Imagem secreta

Fonte: Fei-Fei, Fergus e Perona (2004)

Após o processo de incorporação foram geradas três estego-imagens, uma por cada método. Essas imagens estão representadas na Figura 52.

Figura 52 – Estego-imagens geradas.



(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

A semelhança visual entre a estego-imagem gerada por cada método e sua imagem original é notável. Essa constatação atesta que os três métodos atingiram resultados semelhantes nesse caso. Na continuação do teste, essas estego-imagens foram submetidas ao processo de extração. O resultado dessas operações de extração é apresentado na Figura 53.

Figura 53 – Imagens secretas extraídas.



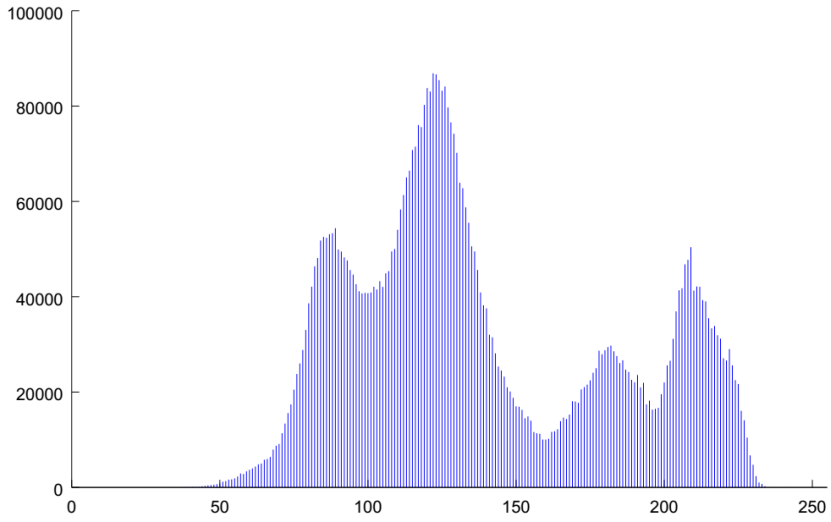
(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

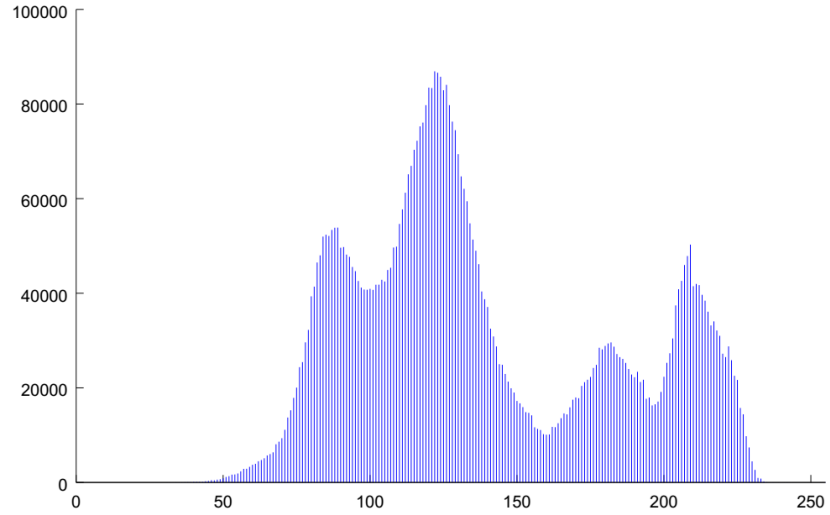
As imagens extraídas por cada um dos métodos mantiveram as características básicas de suas respectivas imagens secretas originais. A perda de qualidade ocorreu em decorrência do uso de apenas três dos *bits* mais significativos de cada *pixel* original no processo de incorporação. Por meio da comparação de características visuais para esse teste, nota-se que os métodos analisados possuem o mesmo poder para extração de dados ocultados em imagens.

Com relação à avaliação perceptual do histograma de frequências das estego-imagens geradas, percebe-se que o LSBR também obteve um desempenho próximo ao dos outros métodos. No entanto, o LSBR evitou o surgimento de padrões de anomalia no histograma, como os apresentados na Figura 35. O LSB *Replacement*, principalmente, apresentou esses padrões em seu histograma. Esse resultado pode ser visto na Figura 54.

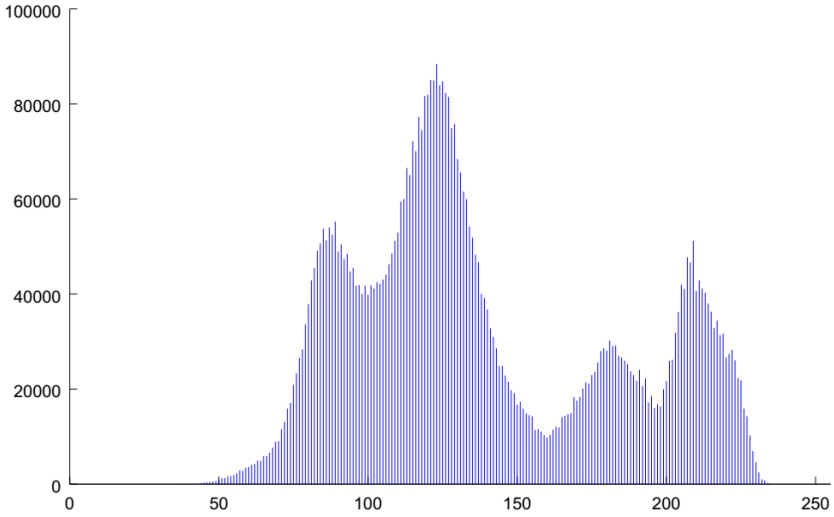
Figura 54 – Histograma da imagem original X Histograma das estego-imagens.



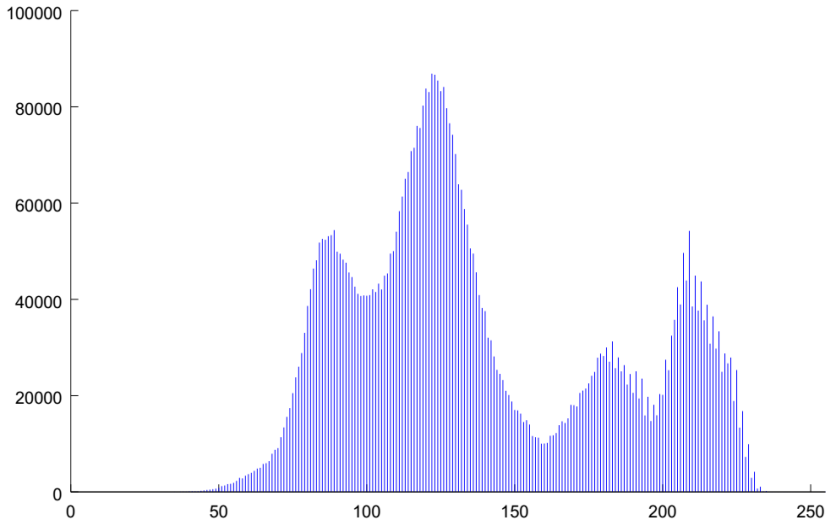
(a) Histograma da imagem de cobertura



(b) Histograma da estego-imagem gerada pelo LSBR.



(c) Histograma da estego-imagem gerada pelo LSB *Matching*

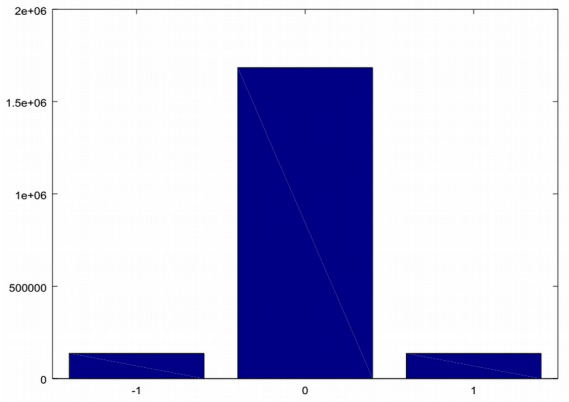


(d) Histograma da estego-imagem gerada pelo LSB *Replacement*.

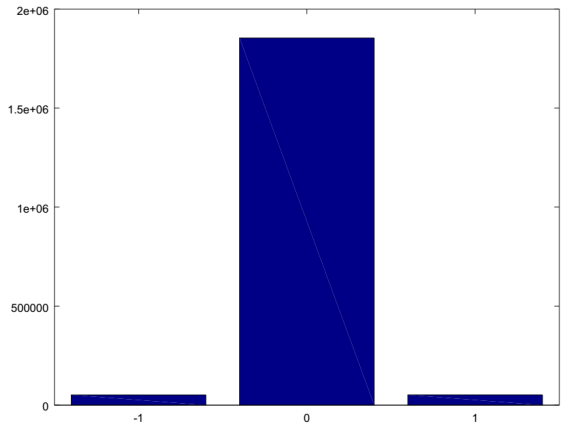
Fonte: autoria própria (2017).

Com relação à diferença gráfica entre estego-imagens e imagem de cobertura original ilustrada na Figura 55, percebe-se que o método que gerou um maior número de modificações de *pixels* foi o LSBR.

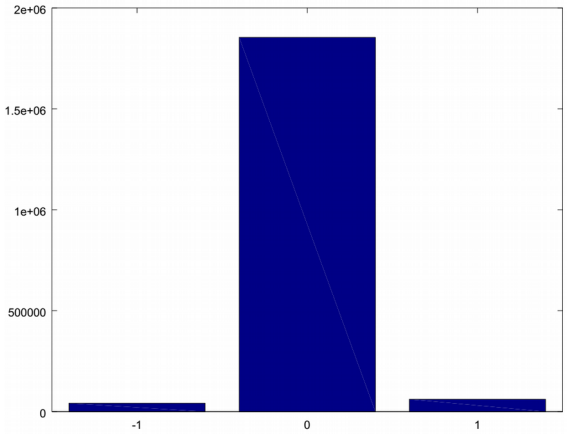
Figura 55 – Valor da diferença entre imagens originais e estego-imagens.



(a) Diferença entre a imagem de cobertura e a estego-imagem do LSBR.



(b) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Matching*



(c) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Replacement*

Fonte: autoria própria (2017).

Nesse ponto de avaliação, o LSB *Replacement* e o LSB *Matching* foram melhores, pois modificaram menos *bits* na imagem de cobertura durante o processo de incorporação. Esse resultado pode ser visualizado por meio da observação da frequência dos valores diferentes de zero, após a subtração das imagens. Esse valor é maior, para o LSBR, implicando que houve mais modificações nos *pixels* durante a incorporação.

As medidas de desempenho encontradas para esse teste estão representadas na Tabela 4.

Tabela 4 – Métricas obtidas (Teste 4).

	MSE	**PSNR (dB)**	**Entropia da imagem original**	**Entropia da estego-imagem**	**Diferença de Entropia**
LSB com Rejeição	0,1395	56,683	7,1817	7,1823	0,0006
LSB *Matching*	0,0527	60,905	7,1817	7,1817	0
LSB *Replacement*	0,0527	60,908	7,1817	7,1808	-0,0009

Fonte: autoria própria (2017)

Em relação ao MSE, o LSBR obteve a pior medida, ficando atrás dos outros métodos. A explicação para o fato de o LSBR possuir um MSE maior que os outros métodos é que ele altera mais *bits* da imagem de cobertura. Com relação ao PSNR, o LSB *Replacement* e o LSB *Matching* obtiveram o maior valor de desempenho. Entretanto, o valor alcançado pelo LSBR permite que a estego-imagem gerada por esse método se enquadre no conjunto de imagens com boa qualidade visual, de acordo com Quadro 5. Com relação à entropia, o LSBR fez com que sua estego-imagem aumentasse a sua entropia em relação à imagem de cobertura, enquanto que para os outros métodos houve uma diminuição e uma estagnação.

5.5 CONFIGURAÇÃO DE TESTE 5

Para a Configuração de Teste 5, foram utilizadas as imagens ilustradas na Figura 56.

Figura 56 – Imagens utilizadas no teste 5.



(a) Imagem de cobertura



(b)Imagem secreta

Fonte: Fei-Fei, Fergus e Perona (2004)

Após o processo de incorporação foram geradas três estego-imagens, uma por cada método. Essas imagens estão representadas ao lado da imagem de cobertura na Figura 57.

Figura 57 – Estego-imagens geradas.



(a) LSBR



(b) LSB *Matching*



(c) LSB *Replacement*

Fonte: autoria própria (2017).

A semelhança visual entre a estego-imagem gerada por cada método e sua imagem original é um fato observável. Os métodos atingiram resultados semelhantes nesse avaliação. Na continuação do teste, essas estego-imagens foram submetidas ao processo de extração. O resultado dessas operações de extração é apresentado na Figura 58.

Figura 58 – Imagens secretas extraídas.



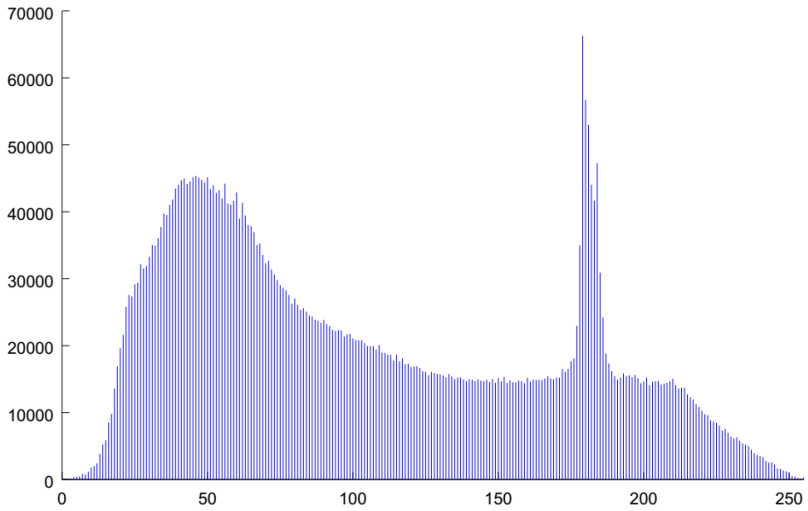
(a) LSBR (b) LSB *Matching* (c) LSB *Replacement*

Fonte: autoria própria (2017).

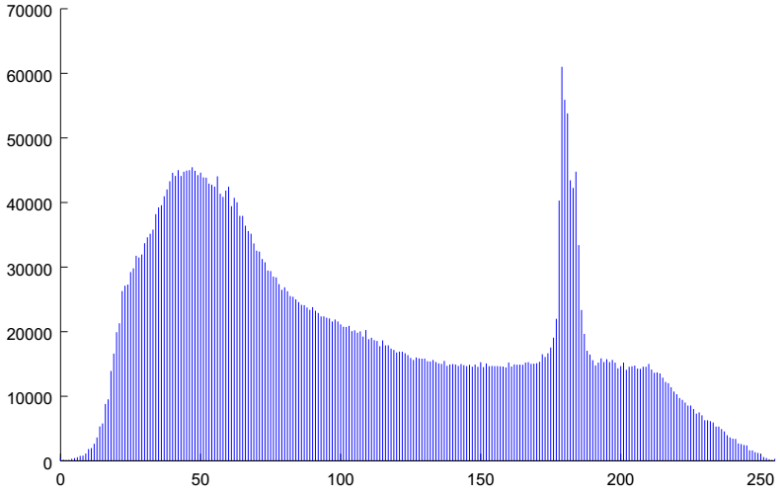
As imagens extraídas por cada um dos métodos mantiveram as características básicas de suas respectivas imagens secretas originais. Assim como em todos os outros testes, a perda de qualidade nas estego-imagens ocorreu em decorrência do uso de apenas três dos *bits* mais significativos de cada *pixel* original no processo de incorporação. Por meio da comparação de características visuais para esse teste, nota-se que os métodos analisados também possuem o mesmo poder para extração de dados ocultados em imagens.

Com relação à avaliação perceptual do histograma de frequências das estego-imagens geradas, percebe-se que o LSBR obteve um melhor desempenho do que os outros métodos. Ele evitou o surgimento de anomalias no histograma, como as apresentadas na Figura 35. O LSB *Replacement* e o LSB *Matching* apresentaram esses padrões em maior grau em seus histogramas. Esse resultado pode ser visto na Figura 59.

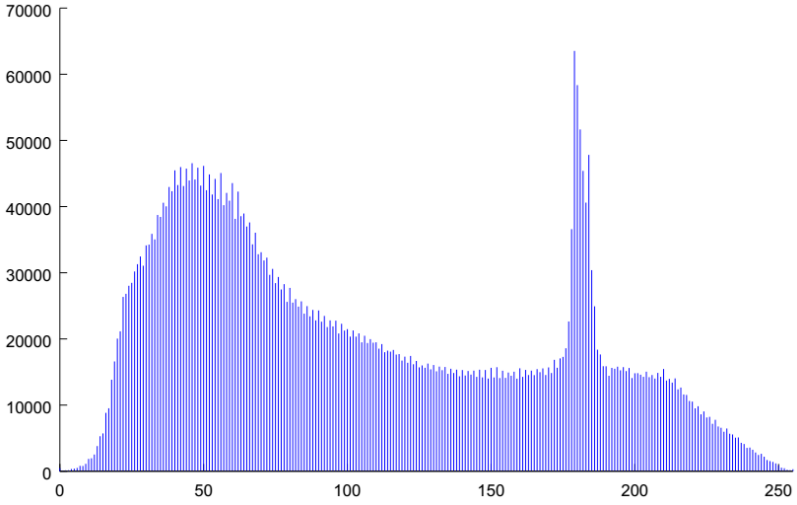
Figura 59 – Histograma da imagem original X Histograma das estego-imagens.



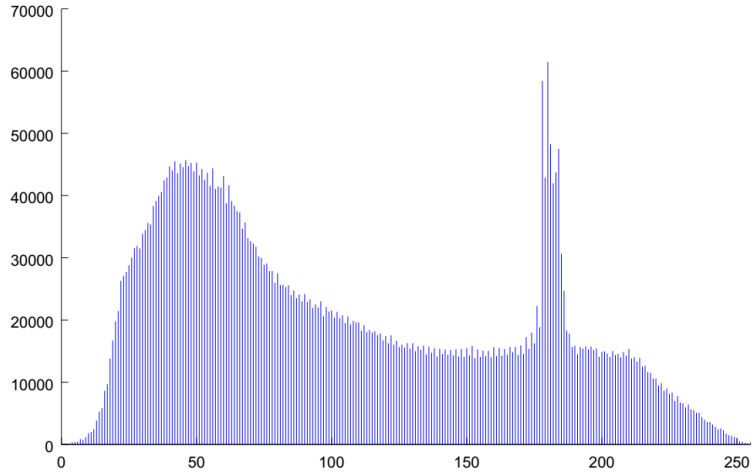
(a) Histograma da imagem de cobertura



(b) Histograma da estego-imagem gerada pelo LSBR



(c) Histograma da estego-imagem gerada pelo LSB *Matching*.

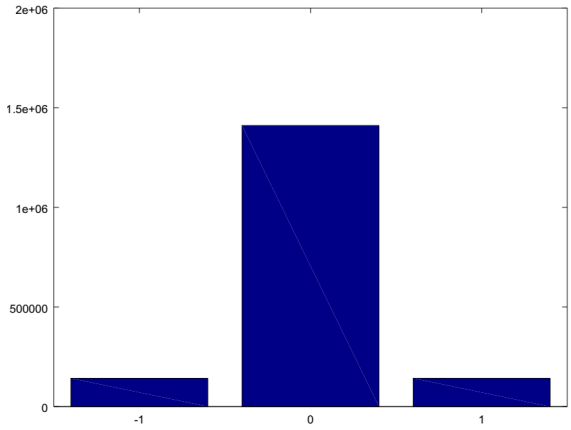


(d) Histograma da estego-imagem gerada pelo LSB *Replacement.*

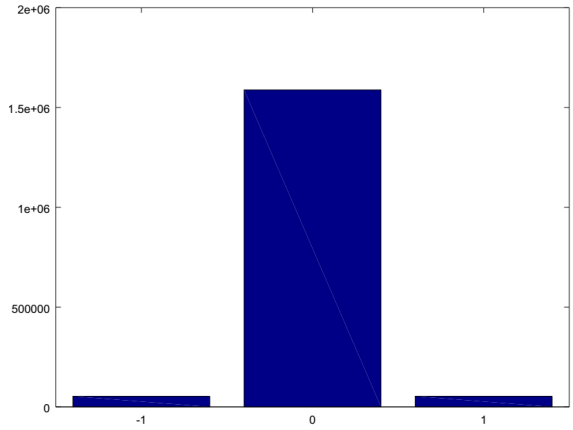
Fonte: autoria própria (2017).

Com relação à diferença gráfica entre estego-imagens e imagem de cobertura original ilustrada na Figura 60, percebe-se que o método que gerou um maior número de modificações de *pixels* foi o LSBR.

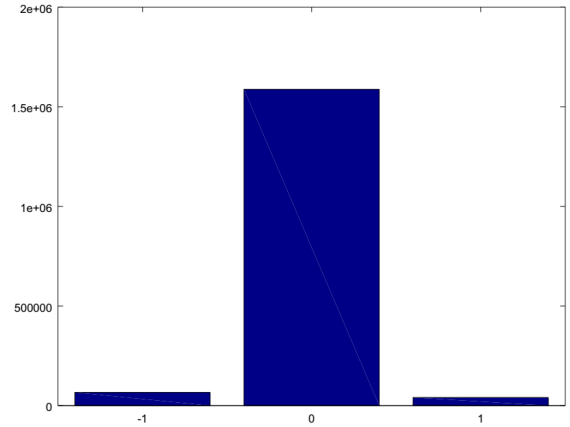
Figura 60 – Valor da diferença entre imagens originais e estego-imagens.



(a) Diferença entre a imagem de cobertura e a estego-imagem do LSBR.



(b) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Matching*.



(c) Diferença entre a imagem de cobertura e a estego-imagem do LSB *Replacement*

Fonte: autoria própria (2017)

Nesse ponto de avaliação, o LSB *Replacement* e o LSB *Matching* foram melhores, devido ao fato de modificarem menos *bits* na imagem de cobertura durante o processo de incorporação. Esse resultado pode ser visualizado por meio da observação da frequência dos valores diferentes de zero, após a subtração das imagens. O LSBR possui maiores valores para essa frequência, implicando que houve mais modificações nos *pixels* durante a incorporação.

As medidas de desempenho encontradas para esse teste estão representadas na Tabela 5.

Tabela 5 – Métricas obtidas (Teste 5).

	MSE	**PSNR (dB)**	**Entropia da imagem original**	**Entropia da estego-imagem**	**Diferença de Entropia**
LSB com Rejeição	0,1677	55,884	7,6665	7,6679	0,0014
LSB *Matching*	0,0628	60,148	7,6665	7,6665	0
LSB *Replacement*	0,0633	60,116	7,6665	7,667	0,0005

Fonte: autoria própria (2017).

Em relação ao MSE, o LSBR obteve a pior medida, ficando atrás dos outros métodos. Devido ao fato de que ele altera mais *bits* da imagem de cobertura. Com relação ao PSNR, o LSB *Replacement* e o LSB *Matching* obtiveram o maior valor de desempenho. Entretanto, o valor alcançado pelo LSBR permite que a estego-imagem gerada por este método possa se enquadrar no conjunto de imagens com boa qualidade visual, de acordo com Quadro 5. Com relação à entropia, o LSBR fez com que sua estego-imagem aumentasse a sua entropia em relação à imagem de cobertura, enquanto que para os outros métodos houve uma aumento em menor grau e uma estagnação.

5.6 DISCUSSÃO DOS RESULTADOS

Nos testes realizados, as avaliações foram feitas tendo como base as imagens de cobertura utilizadas e as estego-imagens geradas a partir da aplicação de cada um dos métodos avaliados. Um dos métodos propostos, algoritmo de criptografia, foi utilizado em conjunto com três métodos de esteganografia: o LSB *Replacement*, o LSB *Matching* e o método proposto, o LSB com Rejeição. A avaliação perceptual por meio das características visuais das imagens, a avaliação com base na análise gráfica, por meio de histogramas de frequências e a avaliação com base em métricas qualidade de imagem foram os meios utilizados para realizar a comparação ente os três métodos.

Com relação a avaliação perceptual por meio das características visuais das imagens, os três métodos avaliados mostraram ter um desempenho equivalente. A qualidade das estego-imagens geradas e das imagens secretas extraídas manteve-se satisfatória. As estego-imagens geradas pelos três métodos de esteganografia estudados mantiveram sua fidelidade às imagens de cobertura que as geraram, não apresentando nenhuma característica visual que as diferenciassem de sua imagem originária. As imagens secretas extraídas também mantiveram fidelidade às características principais das imagens originárias quando foram extraídas pelos três métodos abordados. As mesmas informações que foram inseridas, foram também extraídas, e de forma inteligível. Um ponto a ser destacado no processo de extração de imagens secretas nos testes realizados foi a perda de qualidade quanto à quantidade de níveis de cor representada na imagem extraída. Nos testes realizados, foi feita a inserção de apenas três *bits* mais significativos de cada *pixel* das imagens secretas na imagem de cobertura. Como a informação que foi colocada em uma imagem é mesma que é retirada no processo, quando a imagem secreta é remontada ela perde seus cinco *bits* menos significativos em cada *pixel*,

ocasionando um *pixel* com apenas oito intensidades de cor possíveis, para escala de cinza, e 512 para imagens coloridas. A perda ocorre apenas no campo de definição fiel de cores, as formas das imagens são mantidas. No geral, os três métodos avaliados obtiveram um bom resultado.

Em relação à avaliação gráfica, duas situações puderam ser vistas. No momento em que se analisou graficamente a quantidade de modificações geradas na imagem de cobertura pela aplicação dos métodos, o LSB *Replacement* e o LSB *Matching* mostram-se superiores ao LSBR, pois em todos os testes realizados aqueles métodos modificaram menos *pixels* na imagem de cobertura do que o LSBR. Consequentemente, alteraram menos *pixels* também. No entanto, na análise da distribuição de frequências, o LSBR mostrou um desempenho superior aos outros dois métodos, apesar de seu processo de esteganografia modificar mais *pixels*. Os histogramas das estego-imagens geradas por todos os métodos se aproximaram da curvatura do histograma da imagem de cobertura original. Entretanto, os métodos LSB *Replacement* e LSB *Matching* introduziram perturbações nas curvaturas dos histogramas de estego-imagens na maioria dos testes, ocasionando uma diferença visual perceptível entre o original e o da estego-imagem. O método LSBR não introduziu essas perturbações aos histogramas das estego-imagens que gerou, de forma que esses histogramas adquiriram um alto nível de semelhança visual quando comparados aos histogramas de imagens de cobertura originais.

Em relação às medidas de desempenho, o LSB *Replacement* e o LSB *Matching* obtiveram melhores resultados na medição do MSE em todos os testes. O valor mais baixo de MSE encontrado para esses métodos é explicado pelo fato de eles modificarem a imagem de cobertura menos que o LSBR. Para o PSNR, os métodos LSB *Replacement* e LSB *Matching* obtiveram resultados por volta de 5dB acima do LSBR em todos os testes, o que pode indicar que produziram uma estego-imagem de qualidade, quando comparada com a imagem real. Entretanto, os valores para o PSNR encontrados na análise do LSBR indicam que as imagens geradas por esse método também possuem qualidade em relação à imagem original. Essa constatação foi feita com base nos intervalos de qualidade definidos no Quadro 5. As entropias encontradas para as imagens de cobertura originais e estego-imagens geradas por cada método em todos os testes mostraram que, em geral, a esteganografia realizada com o LSBR eleva a entropia da imagem original. Também de um modo geral, as entropias calculadas para os métodos LSB *Replacement* e LSB *Matching* mostraram redução ou estagnação na entropia da estego-imagem em relação à original. Nos testes em que esses valores foram aumentados em relação à imagem de cobertura, esse fato se deu em menor grau

quando comparado com o LSBR. O ideal é que a entropia de um sistema de imagem possa aumentar, pois segundo Assirati (2014), à medida que um elemento de um sistema passa a ter probabilidade de ocorrência próxima de 100%, a entropia do sistema cai para próximo de 0. Dessa forma, a redução da entropia mostra que alguns símbolos de um sistema estão ocorrendo com mais frequência no conjunto. Isso pode acarretar suspeitas quanto à esteganografia quando, em alguma imagem, determinadas sequências de *bits* surgem com mais frequência que as demais.

De forma geral, o LSBR mostrou-se melhor que os outros métodos analisados no que diz respeito à analise perceptual de histogramas, quando comparados aos histogramas das imagens originais. Esse resultado vem do fato de que os histogramas de estego-imagens geradas pelo LSBR foram mais similares aos originais que os das estego-imagens geradas pelos outros métodos. Em relação à modificação de *pixels* da imagem de cobertura, o LSB *Replacement* e o LSB *Matching* obtiveram um melhor desempenho, conforme foi comprovado pela análise gráfica das diferenças entre imagens geradas e originais e pela comparação das medidas MSE. Em relação ao PSNR, o LSBR obteve menores valores nos testes, no entanto, as imagens geradas por esse método podem ser consideradas com bom nível de qualidade, baseando-se nos intervalos de qualidade definidos no Quadro 5. Em relação à entropia das imagens, considerando Assirati (2014), o método LSBR mostrou um desempenho melhor que os outros métodos, uma vez que aumentou os níveis de entropia da estego-imagem gerada em relação à imagem de cobertura original.

6 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho propôs um método para a realização de criptografia e esteganografia em imagens digitais. O método proposto foi o do *bit* menos menos significativo com rejeição (LSBR). O método LSB tradicional permite, de forma geral, que seja feita a incorporação de um *bit* por *pixel* de cobertura. Essa incorporação é feita alterando-se o *bit* menos significativo de cada *pixel* de cobertura, de forma que cada *pixel* seja responsável por ocultar um *bit* da mensagem secreta. Isto faz com que a quantidade de *bits* da mensagem secreta seja limitada à quantidade de *pixels* de uma imagem multiplicada por três, que é o número de canais de cor de uma imagem.

O método do LSBR possui uma importante vantagem em relação ao LSB tradicional: cada *pixel* da imagem de cobertura pode incorporar de um a sete *bits* secretos. Dessa maneira, a quantidade de *bits* possível de ser incorporada é igual a até sete vezes o número de *pixels* existente na imagem de cobertura, multiplicada por três, que é o número de canais de cor em uma imagem digital. De fato, esta forma de incorporar *bits* permite que os *bits* mais significativos de cada *pixel* de uma imagem secreta possam ser incorporados a uma imagem de cobertura modificando apenas um *bit* em tal imagem – o *bit* de sinalização.

O processo adotado de reservar um *bit* para sinalização, podendo esse ser modificado, e outros *bits* – que não sofrem alteração – para a incorporação, permite que mais dados sejam ocultados que em métodos LSB convencionais.

Considerando três canais de cores, um *pixel* de cobertura poderia então ocultar até 21 *bits* secretos. À medida que o tamanho da sequência secreta aumenta, a quantidade de sequências equivalentes nos *pixels* de cobertura tende a diminuir, pois como mais *bits* mais significativos são empregados na composição das sequências, a variação em todos os *bits* das sequências ocorre de forma menos acentuada.

A aleatoriedade introduzida no processo de escolha do *bit* sinalizador é também uma vantagem do método proposto. Com os *bits* de sinalização assumindo os valores 0 ou 1 de forma aleatória, é possível que longas sequências de *bits* iguais a zero ou um sejam formadas, em caso de muitas rejeições de ocultação de *bits* ou não. Esse resultado beneficia a entropia da imagem, pois uma vez que a quantidade de *bits* 1 e 0 variam de forma aleatória, não haverá crescimento de probabilidades de se encontrar determinada sequência de *bits* nos planos da imagem. Essa imprevisibilidade dificulta a busca por padrões, inclusive na análise de histogramas, o que pode ser feito na tentativa de se descobrir informações secretas em imagens.

O método proposto também proporciona à estego-imagem uma qualidade visual muito próxima da imagem original, de forma que essas duas imagens possuem uma grande semelhança entre si. Além disso, as imagens secretas extraídas preservam as informações nelas contidas, a não ser pela perda visual decorrente da supressão de *bits* no processo de esteganografia. Dessa forma, por meio da aplicação do LSBR é possível guardar imagens digitais de forma confidencial, de forma que indivíduos não autorizados não tenham acesso simples à informação oculta.

O trabalho propôs a avaliação do LSBR em conjunto com dois métodos de esteganografia, o LSB *Replacement* e o LSB *Matching*. Essa avaliação mostrou pontos fortes e fracos de um método em relação ao outro, com relação à medidas de avaliação de qualidade de imagens e avaliações perceptuais. O LSBR mostrou-se superior aos outros dois no que diz respeito à avaliação de histogramas de variação entropia. Com relação a medidas de qualidade como o PSNR, o LSBR mostrou um desempenho próximo aos demais métodos. Em relação ao MSE, mostrou um desempenho abaixo dos outros métodos.

Como trabalhos futuros, propõe-se verificar a possibilidade de aplicação do método LSBR em um contexto de transmissão de vídeos digitais, com a finalidade de diminuição da banda de transmissão desses conteúdos em uma rede. Dessa forma, seria possível transmitir vários conteúdos simultaneamente por meio de um mesmo canal de comunicação.

Um desdobramento dessa proposta seria a possibilidade de transmissão de outros conteúdos de mídia em imagens digitais, tais como som e textos. Como exemplo, uma imagem ou áudio poderia ser transmitido com o seu próprio programa de manipulação incorporado em seus *bits*.

Um outro tópico de extrema relevância sugerido é a medição de segurança. Sugere-se testar o quanto o método proposto resiste a algum ataque que envolva esteganálise, quebra de criptografia, ou ambos.

REFERÊNCIAS

ALBUQUERQUE, Rafael Bezerra. **Esteganografia:** Análise de Algoritmos Baseada em Comparação entre Imagens. 2008. 54 f. TCC (Graduação) - Curso de Engenharia da Computação, Escola Politécnica de Pernambuco – Universidade de Pernambuco., Recife, 2008.

AL-NAJJAR, Yusra A. Y.; SOONG, Der Chen. Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI**. International Journal Of Scientific & Engineering Research**, v. 3, n. 8, p.1-5, ago. 2012.

ALVES, Dorirley Rodrigo. **Avaliação dos Modelos de Cores RGB e HSV na segmentação de Curvas de Nível em Cartas Topográficas Coloridas.** 2010. 65 f. Dissertação (Mestrado) - Curso de Pós-graduação em Engenharia Elétrica, Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2010.

ASSIRATI, Lucas. **Entropia aplicada ao reconhecimento de padrões em imagens.** 2014. 120 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação em Física Aplicada Computacional, Universidade de São Paulo, São Carlos, 2014.

ATEE, Hayfaa Abdulzahra *et al*. Extreme Learning Machine Based Optimal Embedding Location Finder for Image Steganography. **Plos One**, p.1-23, fev. 2017.

BEGAZO, Dante Coaquira. **Avaliação Objetiva e Subjetiva de Qualidade de Vídeo Via Rede IP com Variação de Atraso.** 2012. 62 f. Dissertação (Mestrado) - Curso de Mestrado em Ciências, Escola Politécnica da Universidade de São Paulo, São Paulo, 2012.

BHATTACHARYA, Tanmay; DEY, Nilanjan; CHAUDHURI, S. R. Bhadra. A Session based Multiple Image Hiding Technique using DWT and DCT. **International Journal Of Computer Applications**, v. 38, n. 5, p.18-21, jan. 2012.

BONFIM, Daniele Helena. **Criptografia RSA.** 2017. 91 f. Dissertação (Mestrado) - Curso de Programa de Mestrado Profissional em Matemática, Universidade de São Paulo, São Carlos, 2017.

BRAZIL, André Luiz. **Path Relinking and AES Cryptography in Color Image Steganography.** 2008. 106 f. Dissertação (Mestrado) - Curso de Mestrado em Computação, Universidade Federal Fluminense, Niterói, 2008.

CAHÚ, Carlos Bruno Gomes. **Uma Abordagem BSP Tree na Esteganografia.** 2009. 63 f. TCC (Graduação) - Curso de Engenharia da Computação, Escola Politécnica de Pernambuco – Universidade de Pernambuco, Recife, 2009.

CANTANHEDE, Hugo Silva. **Esteganografia em Áudio e Imagem utilizando a técnica LSB.** 2009. 62 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal de Goiás, Catalão, 2009.

CARVALHO, Diego Fiori de. **Esteganografia em vídeos comprimidos MPEG-4.** 2008. 69 f. Dissertação (Mestrado) - Curso de Mestrado em Ciência da Computação e Matemática Computacional, USP, São Carlos, 2008.

CERT.br (Org.). **Estatísticas dos Incidentes Reportados ao CERT.br.** 2017. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 15 jan. 2017.

CHAN, Chi-kwong; CHENG, L.m. Hiding data in images by simple LSB substitution. Pattern Recognition: **The Journal of the Pattern Recognition Society**, p.469-474, ago. 2003.

CHEDDAD, Abbas *et al*. **Enhancing Steganography In Digital Images.** 2008. Canadian Conference on Computer and Robot Vision. Disponível em: <http://ieeexplore.ieee.org/document/4562128/>. Acesso em: 04 maio 2017.

CRUZ, Edilson Fernandes da. **A Criptografia e Seu Papel na Segurança da Informação e das Comunicações (SIC):** Retrospectiva, Atualidade e Perspectiva. 2009. 84 f. Monografia (Especialização) - Curso de Especialização em Gestão de Segurança da Informação e Comunicações, Universidade de Brasília, Brasília, 2009.

DARABKH, Khalid *et al*. **An improved image least significant bit replacement method.** 2014. 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Disponível em: <https://www.researchgate.net/publication/269291454_An_improved_image_least_significant_bit_replacement_method>. Acesso em: 28 mar. 2017.

FEI-FEI, L.; FERGUS, R.; PERONA, P. **Learning generative visual models from few training examples:** an incremental Bayesian approach tested on101 object categories. IEEE. CVPR 2004, Workshop on Generative-ModelBased Vision. 2004

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática.** 2010. 144 f. Dissertação (Mestrado) - Curso de Mestrado em Matemática Para Professores, Universidade de Lisboa, Lisboa, 2010.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de Computadores**: uma abordagem top-down. Porto Alegre: AMGH Editora Ltda., 2013. 896 p.

FRANÇA, A. E. A. G.; MADEIRO, F. **Esteganografia LSB em Imagens Digitais Baseada em Sequências VDH.** Revista de Engenharia e Pesquisa Aplicada, v. 2, n. 1, p.369-373, jan./dez. 2016.

GIL, Fernando de O. *et al*. **SEA – Sistema Esteganográfico de Arquivos.** 2008. VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Disponível em: <http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_04_wticg.pdf>. Acesso em: 10 maio 2017.

GONZALEZ, Rafael C.; WOODS, Richard E.. **Processamento de imagens digitais.** São Paulo: Blucher, 2000. Tradução: Roberto Marcondes Cesar Junior, Luciano da Fontoura Costa.

GONZALEZ, Rafael C.; WOODS, Richard E.. **Processamento Digital de Imagens.** 3. ed. São Paulo: Pearson Prentice Hall, 2010. ISBN: 978-85-7605-401-6.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores.** Porto Alegre: Bookman, 2013. 568 p. ISBN: 978-85-407-0192-2.

GUTTE, R. S.; CHINCHOLKAR, Y. D. Comparison of Steganography at One LSB and Two LSB Positions. **International Journal Of Computer Applications**, v. 49, n. 11, p.1-7, jul. 2012.

GUTUB, Adnan Abdul-aziz. Pixel Indicator Technique for RGB Image Steganography. **Journal Of Emerging Technologies In Web Intelligence**, v. 2, n. 1, p.56-64, fev. 2010.

HOSPODAR, Gabriel Mayrink da Rocha. **Algoritmos de Esteganografia via Restauração Estatística em Imagens Digitais.** 2009. 73 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2009.

IBGE. **Introdução ao Processamento Digital de Imagens. Rio de Janeiro:** IBGE, 2001. 94 p. ISBN: 85-240-0762-1.

JINDAL, Sakshi; KAUR, Navdeep. Digital Image Steganography Survey And Analysis Of Current Methods. Iracst **- International Journal Of Computer Science And Information Technology & Security (IJCSITS)**, v. 6, n. 3, p.10-13, jun. 2016. ISSN: 2249-9555.

JULIO, Eduardo Pagani; BRAZIL, Wagner Gaspar; ALBUQUERQUE, Célio Vinicius Neves. **Esteganografia e suas Aplicações.** 2007. VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Disponível em: <http://ceseg.inf.ufpr.br/anais/2007/minicursos/cap2-esteganografia.pdf>. Acesso em: 21 jan. 2017.

KAUR, Amandeep; KAUR, Rupinder; KUMAR, Navdeep. A Review on Image Steganography Techniques. **International Journal Of Computer Applications**, v. 123, n. 4, p.20-24, ago. 2015.

KAUR, Ravpreet; MAHAJAN, Manish. Random Pattern based sequential bit (RaP-SeB) Steganography with Cryptography for Video Embedding. I.j. **Modern Education And Computer Science**, p.51-59, set. 2016.

KUMAR, Anil; SHARMA, Rohini. A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. **International Journal Of Advanced Research In Computer Science And Software Engineering**, v. 3, n. 7, p.363-372, jul. 2013. ISSN: 2277 128X.

LI, Bin *et al*. A Survey on Image Steganography and Steganalysis. **Journal Of Information Hiding And Multimedia Signal Processing**, v. 2, n. 2, p.142-172, abr. 2011.

LI, Ze-nian; DREW, Mark S.; LIU, Jiangchuan. **Fundamentals of Multimedia.** 2. ed. : Springer, 2014. 727 p.

LUO, Weiqi; HUANG, Fangjun; HUANG, Jiwu. Edge Adaptive Image Steganography Based on LSB Matching Revisited. **IEEE Transactions On Information Forensics And Security**, v. 5, n. 2, p.201-214, jun. 2010.

MANDAL, J. K.; DAS, Debashis. Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain. **International Journal Of Information Sciences And Techniques (IJIST)**, v. 2, n. 4, p.83-93, jul. 2012.

MARQUES, Thiago Valentim. **Criptografia:** abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula. 2013. 62 f. Dissertação (Mestrado) - Curso de Matemática, Universidade Federal da Paraíba, João Pessoa, 2013.

MIELIKAINEN, Jarno. **LSB Matching Revisited.** 2006. Disponível em: <https://www.researchgate.net/publication/3343443_LSB_matching_revisited>. Acesso em: 21 jan. 2017.

MORKEL, T.; ELOFF, J.H.P.; OLIVIER, M.S. **An Overview of Image Steganography.** 2005. Proceedings of the Fifth Annual Information Security South Africa Conference - June/July 2005. Disponível em: <http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/098_Article.pdf>. Acesso em: 29 mar. 2017.

OLIVEIRA, Fábio Borges de. **Análise da segurança de criptografia e esteganografia em sequências de imagens.** 2007. 101 f. Dissertação (Mestrado) - Curso de Modelagem Computacional, Laboratório Nacional de Computação Científica, Petrópolis - RJ, 2007.

OLIVEIRA, Nícholas André Pinho de. **Aplicação de Zoom em Imagens Digitais Utilizando Regressão Linear**. 2016. 58 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal Rural do Semi-Árido, Mossoró - RN, 2016.

PETRI, Marcelo. **Esteganografia.** 2004. 57 f. TCC (Graduação) - Curso de Sistemas de Informação, Instituto Superior Tupy, Joinville, 2004.

PINEDA, José Octávio de Carvalho. **A entropia segundo Claude Shannon: o desenvolvimento do conceito fundamental da teoria da informação.** 2006. 124 f. Dissertação (Mestrado) - Curso de Mestrado em História da Ciência, Pontifícia Universidade Católica de São Paulo, São Paulo, 2006.

QUEIROZ, Corina Jara de**. Analise de Transformações Geométricas para o Georreferenciamento de Imagens do Satélite CBERS-I.** 2003. 79 f. Dissertação (Mestrado) - Curso de Mestrado em Sensoriamento Remoto, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2003.

RENZA, Diego; L., Dora M. Ballesteros; RINCÓN, Ramiro. Método de Ocultamiento de Píxeles Para Esteganografía de Imágenes en Escala de Gris Sobre Imágenes a Color. **Ingeniería y Ciencia**, v. 12, n. 23, p.145-162, jun. 2016. ISSN: 1794-9165.

ROCHA, Anderson de Rezende. **Camaleão:** um Software para Segurança Digital Utilizando Esteganografia. 2003. 108 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal de Lavras, Lavras - MG, 2003.

ROCHA, Anderson *et al*. **Segurança e privacidade na internet por esteganografia em imagens.** 2004. Disponível em: <https://pdfs.semanticscholar.org/b37b/884e9e2b7436137b3fc75d6a378e278be95f.pdf>. Acesso em: 28 mar. 2017.

SEIVI, G.karthigai; MARIADHASAN, Leon; SHUNMUGANATHAN, K. L.. **Steganography Using Edge Adaptive Image.** 2012. International Conference on Computing, Electronics and Electrical Technologies [ICCEET]. Disponível em: <https://www.researchgate.net/publication/254034959_Steganography_using_edge_adaptive_image>. Acesso em: 08 mar. 2017.

STALLINGS, William. **Criptografia e Segurança de Redes.** 4. ed. São Paulo: Pearson Prentice Hall, 2008. 512 p. ISBN: 978-85-7605-119-0.

TAVARES, João Rafael C.; LIMA, J. Bandeira; MADEIRO, F. **LSB Word-Hunt:** Um Método de Esteganografia para Imagens Digitais Utilizando Chave Simétrica. 2012. Anais do Congresso de Matemática Aplicada e Computacional 2012. Disponível em: <http://www.sbmac.org.br/cmacs/cmac-ne/2012/trabalhos/PDF/190.pdf>. Acesso em: 21 jan. 2017.

TAVARES, R.; MADEIRO, F. **Word-Hunt:** A LSB Steganography Method with Low Expected Number of Modifications per Pixel. Ieee Latin America Transactions, v. 14, n. 2, p.1058-1064, fev. 2016.

THYAGARAJAN, K. S. **Still Image and Video Compression with MATLAB.** Wiley, 2011. Disponível em: <https://books.google.com.br/books?id=adv71MkRIWYC&pg=RA1-PR3&hl=pt-BR&source=gbs_selected_pages&cad=2#v=onepage&q&f;=false>. Acesso em: 10 maio 2017.

UMBAUGH, Scott E. **Digital Image Processing and Analysis: Human and Computer Vision Applications with CVIPtools.** 2. ed. Crc Press - Taylor & Francis Group, 2010. 955 p.

VALENZUELA, Gracieth Mendes. **Mecanismo de Seleção de Rede em Ambientes Heterogêneos Baseado em Qualidade de Experiência (QoE).** 2011. 109 f. Dissertação (Mestrado) - Curso de Mestrado em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011.

VASHISHTHA, Lalit Kumar; DUTTA, Tanima; SUR, Arijit**. Least Significant Bit Matching Steganalysis Based on Feature Analysis.** 2013. Disponível em: <https://www.researchgate.net/publication/261247056_Least_significant_bit_matching_steganalysis_based_on_feature_analysis>. Acesso em: 29 mar. 2017.

VELDHUIZEN, Todd. **Measures of image quality.** 1998. Disponível em: <http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/VELDHUIZEN/node18.html>. Acesso em: 13 maio 2017.