ESCOLA POLITÉCNICA
DE PERNAMBUCO

d.s.c. UPE
Departamento de Sistemas e Computação

Esteganografia: Análise de Algoritmos Baseada em Comparação entre Imagens

Trabalho de Conclusão de Curso

Engenharia da Computação

Rafael Bezerra Albuquerque
Orientador: Prof. Dr. Carlos Alexandre Barros de Mello

UNIVERSIDADE
DE PERNAMBUCO

Rafael Bezerra Albuquerque

Esteganografia: Análise de Algoritmos Baseada em Comparação entre Imagens

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia da Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, Novembro de 2008.

À Jesus Cristo, que se deu por mim.

Resumo

O avanço tecnológico e a crescente necessidade de prover segurança nos mais diversos tipos de transações têm proporcionado, nos últimos anos, estudos visando não só aperfeiçoar as técnicas existentes, como criar novas. Técnicas de ocultação de informação têm sido utilizadas desde os tempos mais remotos, mas, com o surgimento de meios digitais como imagem, áudio e vídeo, sua aplicação se tornou mais viável nos dias atuais. Esteganografia é a arte de esconder informação em um meio digital de maneira que não se perceba nem mesmo a existência da mensagem. Este trabalho compreende um estudo sobre esteganografia aplicada a imagens digitais a partir da implementação de algoritmos clássicos com variações e sua aplicação a um banco de imagens. Por fim, também são apresentados resultados da análise de similaridade entre a imagem original e a imagem com a mensagem escondida, chamada estego-imagem.

Abstract

The technological advance and the growing need to provide security in several different kind of transactions in recent years have drawn great attention to the subject, providing studies that aim at not only improving existing techniques, but also at developing new ones. Information hiding techniques have been used for a long time, but with the advent of digital media such as images, video and audio, its implementation has become more feasible. Steganography is the art of hiding information in a digital media so that the occluded message is imperceptible. In this work, classical steganography algorithms and some variations of them are applied to a digital image data base through the use of some classical algorithms. Finally, image similarity is evaluated between the original image and the image with the hidden message, also called stego-image.

Sumário

Índice de Figuras

Índice de Tabelas

Tabela de Símbolos e Siglas

(Dispostos por ordem de aparição no texto)

IHW – *Information Hiding Workshop* (Simpósio de Ocultação da Informação)

IEEE – *Institute of Eletrical and Eletronics Engineers* (Instituto de Engenheiros Eletricistas e Eletrônicos)

P2P – *Peer to Peer* (Ponto a Ponto)

LSB – *Least Significant Bit* (Bit Menos Significativo)

DES – *Data Encryption Standard* (Padrão de Cifragem de Dados)

AES – *Advanced Encryption Standard* (Padrão de Cifragem Avançado)

MSE – *Mean Square Error* (Erro Médio Quadrático)

PSNR – *Peak Signal-to-Noise Ratio* (Razão Sinal-Ruído de Pico)

Q – *Universal Quality Index* (Índice Universal de Qualidade)

SSIM – *Structural Similarity* (Índice de Similaridade Estrutural)

Agradecimentos

“Os teus olhos me viram substância ainda informe, e no teu livro foram escritos todos os meus dias, cada um deles escrito e determinado, quando nem um deles havia ainda.” Salmo 139,16

Inicialmente a Deus, meu Senhor e Salvador, por me conhecer melhor até do que eu mesmo e ainda assim me amar ao ponto de pregar Seu Filho em uma cruz por mim. À Ele que tornou tudo isso possível.

À minha família que me tornou o que sou hoje, não apenas dando força e incentivo aos estudos, mas atuando diretamente na formação do meu caráter. Ao meu pai por sempre ter lutado, não medindo esforços, para que eu pudesse fazer bons cursos e ter uma boa formação. À minha, doce, mãe por me ensinar o que é o amor e o perdão desde os meus primeiros passos.

À minha amada esposa, Cláudia, por me fazer sentir mais completo, dando-me carinho, amor e cuidando de mim. À ela, que me é exemplo de garra e persistência e que tanto me influencia a continuar lutando, por mais dura que a batalha seja.

Aos meus amigos, de todas as épocas. Na faculdade posso citar alguns que representam tantos que me foram verdadeiros companheiros: Victor Braz, Júlio Taveira, Adriano Marques, Péricles Sales, Ricardo Ulisses e Leopoldo Teixeira. Aos amigos do trabalho por criarem um ambiente tão legal e entenderem minhas ausências em alguns momentos, represento-os por: Arlington (meu irmão por escolha), Fagner e Gugu.

Aos meus irmãos em Cristo pelo constante desejo de sermos um só e nos ajudarmos, suportarmos e nos edificarmos mutuamente.

Ao meu orientador, Prof. Dr. Carlos Alexandre, que não obstante orientar-me de forma brilhante, foi responsável direto e indireto pela mudança na minha forma de encarar o curso. A todos os professores do DSC pela dedicação, criando um alento de esperança de que é possível termos uma educação de qualidade no nosso país.

Capítulo 1

Introdução

O acréscimo na quantidade de serviços e o surgimento de novos modelos de negócios e novos mercados vêm sendo proporcionado por: 1) o aumento do uso de computadores nos mais diversos setores produtivos, para fins de otimização de processos, e 2) uma constante redução de preço do hardware, o que viabiliza a inclusão digital por grande parte da sociedade. Esse aumento dos negócios através da Internet demanda segurança nas transações. Não basta apenas funcionar, mas tem de haver confiabilidade no serviço para que seus usuários tenham credibilidade no mesmo.

Inicialmente, o que se viu foram técnicas de criptografia [15], cada vez mais avançadas a fim de proteger o conteúdo dos dados transmitidos. Isso ocorreu de tal forma que, mesmo havendo interceptação da mensagem, o conteúdo capturado não seria inteligível, estaria cifrado e dependente, por exemplo, de uma chave que apenas o destinatário possuiria para decifragem da mensagem.

Posteriormente, a comunidade científica passou a pensar em técnicas de ocultação da informação (*information hiding* ou *data hiding*). Tais técnicas têm por objetivo principal embutir uma mensagem em um determinado conteúdo (imagem, áudio, vídeo, etc.) [4][14] deixando a mensagem imperceptível [8] ou secreta [5]. Elas diferem de criptografia ao objetivar ocultar a mensagem e não cifrá-la. Em criptografia, a mensagem está, na maioria das vezes, disponível ao criptoanalista que sabe da existência da mensagem, mas precisa utilizar-se de técnicas de criptoanálise para tentar descobrir o seu significado (decifrar).

No tocante a ocultação de informação, este trabalho fará uso de esteganografia [3][6][12][18][21][24]. Esteganografia é a arte de esconder informação de maneira que não se perceba nem mesmo a existência da mensagem escondida [11].

Em se tratando de esteganografia em imagens, têm sido propostos vários algoritmos. O objetivo da maioria dos trabalhos têm sido dificultar a descoberta da mensagem por técnicas de estegoanálise [9][13][16][17] em situações em que não se dispõe da imagem original. Esse trabalho diferencia-se dos demais ao buscar uma comparação do desempenho dos algoritmos tomando como base a imagem gerada (com a mensagem escondida), chamada de estego-imagem, em comparação com a imagem original sem qualquer mensagem.

1.1 Objetivos

O objetivo deste trabalho é analisar o desempenho de algumas técnicas clássicas de esteganografia aplicadas a imagens digitais. Essa análise é feita comparando o resultado final das técnicas, ou seja, a estego-imagem. Para alcançar esse objetivo foram necessários alguns pontos chaves:

- Maior entendimento dos conceitos de esteganografia.
- Análise e implementação de algoritmos clássicos de esteganografia.
- Estudo e análise das medidas de comparação entre imagens.

1.2 Organização do trabalho

Este trabalho encontra-se dividido em 5 capítulos:

- Capítulo 1 – provê uma introdução ao trabalho, incluindo uma motivação inicial e os objetivos principais.
- Capítulo 2 – provê uma explicação geral da área de ocultação da informação, diferenciando *watermarking* e esteganografia. São explicados o cerne do funcionamento de alguns algoritmos clássicos que foram desenvolvidos e o resultado da aplicação destes como forma de exemplificar o funcionamento.
- Capítulo 3 – provê uma introdução sobre como classificar a similaridade entre imagens, apresenta alguns dos índices de fidelidade mais utilizados pela

comunidade científica e apresenta exemplos de imagens e seus respectivos valores comparativos.

- Capítulo 4 – provê explicação e análise de uma série de experimentos desenvolvidos com base na fundamentação teórica encontrada nos dois Capítulos anteriores.

- Capítulo 5 – provê uma conclusão final sobre o trabalho, definindo possíveis trabalhos futuros para os autores e também aos leitores deste trabalho que se interessarem pelo tema.

Capítulo 2

Information Hiding

Em *Information Hiding* temos duas grandes áreas de pesquisa que têm sido tendência: *watermarking* (marca d'água) e esteganografia. Este Capítulo diferencia as duas áreas, destacando esteganografia, foco deste trabalho.

2.1 Watermarking

O primeiro indício do uso de *watermarking* só se tem registro por volta do século XIII, na Itália. Entretanto, não se tem certeza do objetivo das marcas no papel, podendo ser desde uma forma de identificação de seu fabricante até uma simples forma de decoração ou elemento místico [5].

Atualmente, a razão do uso de *watermarking* encontra-se bem definido como sendo uma forma de identificar um objeto de maneira que qualquer tentativa de retirar essa marcação torne seu conteúdo inutilizável [8]. O objeto em questão deixou de ser apenas o papel, como era na antiguidade, para atingir as mídias digitais e ser utilizada em imagens, áudio e vídeo.

O crescimento do interesse em *watermarking* digital como área de pesquisa se inicia com a necessidade de criação de técnicas de proteção de conteúdo. Após o primeiro IHW (*Information Hiding Workshop*) em 1996, aumentou bastante o número de artigos publicados sobre o assunto. A Figura 1 [5] apresenta o gráfico de quantidade de artigos relacionados a *watermarking* publicados no IEEE entre 1991 e 2006. Podemos ver o grande crescimento a partir de 1996 associado ao primeiro IHW. Essa busca crescente por técnicas de proteção de conteúdo acontece, principalmente, devido ao aumento da capacidade de transmissão de dados (*bandwidth*) na Internet associado à criação de mídias de alta capacidade de armazenamento o que permitiu o compartilhamento não apenas de músicas, mas filmes inteiros por meio das redes P2P [27].

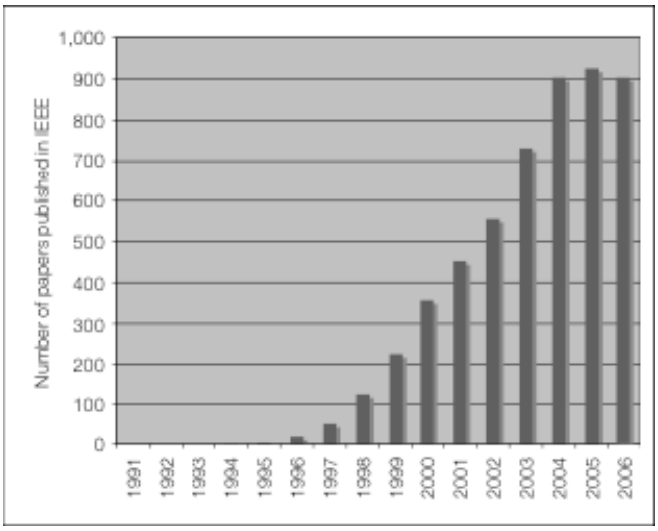


Figura 1. Gráfico em barras do aumento do número de artigos sobre watermarking e esteganografia publicados na IEEE.

Nas pesquisas mais recentes, tem sido uma constante a criação de novos métodos de implementação de proteção de conteúdo, mas que, logo em seguida, têm sua segurança quebrada. Logo, surgem novos algoritmos e, embora existam avanços nas pesquisas, ainda não se pode apontar uma técnica que seja eficiente, pelo menos por um espaço de tempo razoável. Para mais informações sobre *watermarking* recomendamos a leitura de [5] e [8].

2.2 Esteganografia

O primeiro relato que se tem notícia do uso de Esteganografia chega pelas histórias de Heródoto. Conta-se que Histiæus desejava enviar uma mensagem para o seu chefe, Aristogaras de Mileto, então escolheu um escravo de sua confiança, raspou-lhe a cabeça e tatuou a mensagem incentivando Aristogaras a iniciar uma revolta contra o rei da Pérsia. Deixou então o cabelo do escravo crescer novamente e o enviou à Mileto. Lá chegando, bastou a Aristagaras raspar a cabeça do escravo e ler a mensagem.

Mais recentemente, outro exemplo clássico que se tem conhecimento ocorreu na Segunda Guerra Mundial. Refere-se à mensagem enviada por um espião alemão à seu comandante contendo o seguinte texto: *“Apparently neutral's protest is*

thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils". Sem aparentar conter qualquer conteúdo malicioso, ao juntarmos a segunda letra de cada palavra teremos a informação que verdadeiramente fora transmitida: "*Pershing sails from NY June 1*".

Com o advento da utilização dos computadores, assim como ocorreu com *watermarking*, ocorre também com esteganografia o aumento por seu interesse. O que antes se restringia a textos e tintas invisíveis ganha, agora, novas possibilidades com a esteganografia digital. Pode-se usar desde os meios mais comuns como imagem, vídeo e áudio até os mais surpreendentes como, por exemplo, descritores de arquivos e superbloco de sistemas de arquivos [1].

2.2.1 Esteganografia em imagens

A estrutura de uma imagem pode ser vista, matematicamente, como 3 matrizes onde cada célula possui valores variando de 0 a 255, a chamada matriz RGB. No caso, o R refere-se à componente *Red* (vermelho), G a *Green* (verde) e B a *Blue* (azul). A estrutura do olho humano não nos permite perceber alterações mínimas nos tons das cores, como por exemplo, uma variação de valor absoluto 1 (um) na tonalidade de azul como mostra a Figura 2.

(a) (b)

Figura 2. (a) imagem com cor R=0,G=0 e B=254 e (b) cor R=0,G=0 e B=255.

Diante do exposto, têm sido propostos vários algoritmos para a utilização de esteganografia em imagens. Os métodos mais comuns são variações de técnicas de modificação do bit menos significativo (LSB) devido ao baixo custo computacional requerido. As próximas seções deste trabalho comprovam a funcionalidade ao comparar as imagens com sua respectiva estego-imagem através de índices de fidelidade.

2.2.2 Algoritmos de Esteganografia em imagens

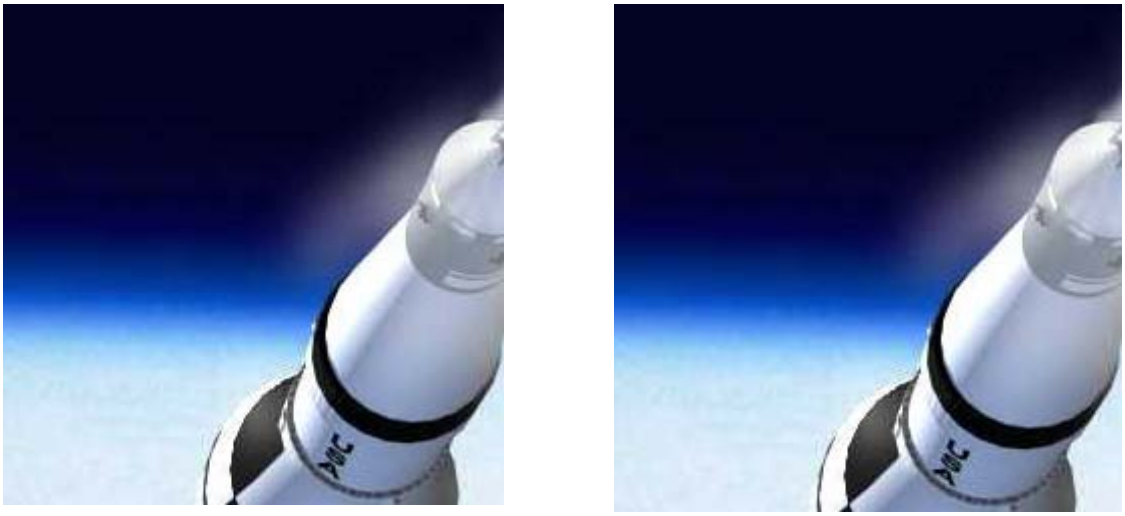
Com base nas características inerentes do olho humano e das imagens, nesta Seção são apresentados alguns dos algoritmos clássicos mais utilizados em esteganografia, elucidando o funcionamento e as vantagens e desvantagens de cada um.

LSB 1 bit

Esse é o primeiro algoritmo e também o mais simples. Consiste, basicamente, em modificar o bit menos significativo de uma das bandas de cor (R, G ou B) de uma célula da matriz imagem com a finalidade de inserir a mensagem, utilizando esse espaço de um bit por pixel para armazenar a mensagem. Existem implementações que utilizam as três bandas e não apenas uma com objetivo de aumentar a capacidade de armazenamento da mensagem na estego-imagem.

Além do já citado baixo custo computacional que é característica dos algoritmos LSBs, especificamente nesse caso podemos citar a alta fidelidade entre a imagem original e a estego-imagem. A modificação de apenas um bit garante uma dificuldade muito grande para se notar à “olho nu” a diferença entre elas, como podemos ver na Figura 3. Nela, temos a imagem original sua estego-imagem com uma mensagem de 7.811 bytes armazenada de acordo com o método descrito nesta Seção.

As desvantagens são: 1) a baixa capacidade de armazenamento por usar apenas 1 bit por pixel (um caractere armazenado em 8 bits precisaria de 8 pixels para ser armazenado), ou, em uma versão modificada, 3 bits por pixel, e 2) por ser uma técnica bastante simples e pioneira já existem diversos algoritmos para detecção de seu uso e obtenção da mensagem oculta, utilizando técnicas estatísticas de estegoanálise.



(a) (b)

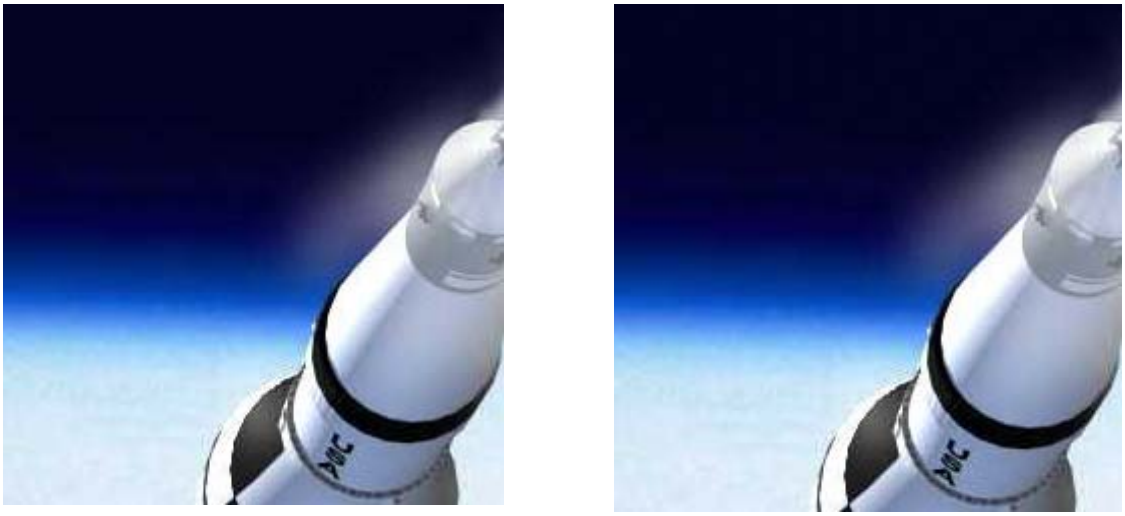
Figura 3. (a) Imagem original colorida e com 250x250 pixels e (b) estego-imagem utilizando LSB 1 bit e mensagem de 7.811 bytes.

LSB 2 bit

Uma pequena variação do LSB de 1 bit, a única diferença, como o próprio nome sugere, é a utilização dos 2 bits menos significativos na imagem, podendo ser apenas uma das bandas da cor (R,G ou B) do pixel ou as três.

Da mesma forma que compartilha a idéia e o projeto, herda também as mesmas vantagens e desvantagens. A diferença sutil está na capacidade de armazenamento da mensagem oculta que é o dobro, e a mudança na figura também é um pouco mais acentuada, mas ainda, em geral, imperceptível à “olho nu”, como podemos ver na Figura 4, onde apresentamos uma estego-imagem com uma mensagem de 15.622 bytes armazenada nela.

Em diversos momentos deste trabalho, repetiremos a imagem original sem mensagens escondidas apenas para facilitar uma comparação visual com a imagem com a mensagem. Também armazenaremos as imagens no formato BMP para impedir qualquer tipo de codificação provocada por formatos que usem compressão de dados (como JPG).

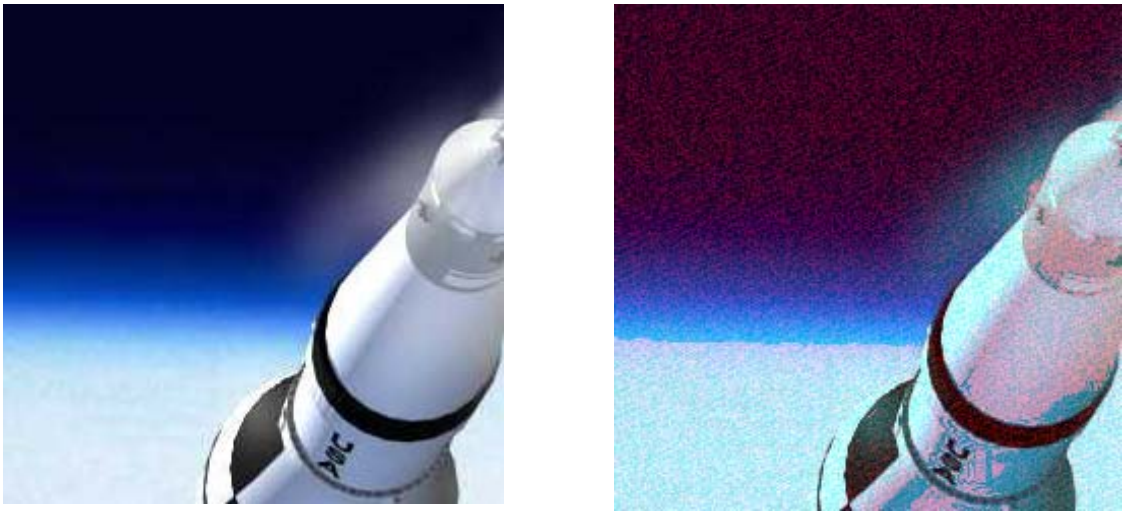


(a) (b)

Figura 4. (a) Imagem original colorida e com 250 x 250 pixels e (b) estego-imagem utilizando LSB 2 bit e mensagem de 15.622 bytes.

LSB *n* bit

De maneira geral, o LSB n bit aumenta a quantidade de bits a serem utilizados. Isso provoca um aumento na capacidade de armazenamento em detrimento de uma estego-imagem bastante modificada em relação à original. Para exemplificar, a Figura 5 mostra a imagem original e a estego-imagem, utilizando o algoritmo LSB 7 bits, a discrepância entre as imagens é alta e patente aos nossos olhos.

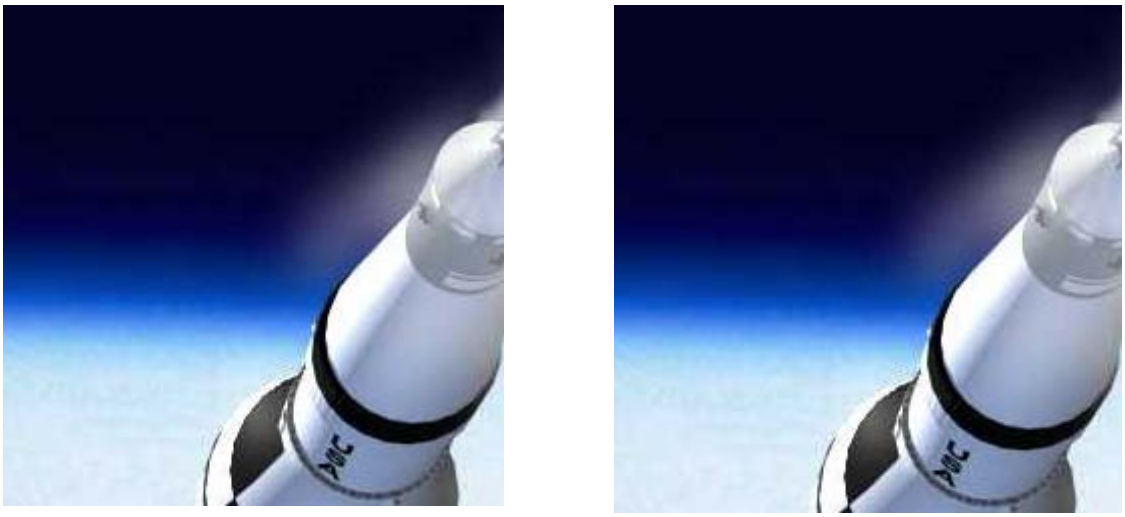


(a) (b)

Figura 5. (a) Imagem original colorida e com 250x250 pixels e (b) estego-imagem utilizando LSB 7 bit e mensagem de 54.685 bytes.

LSB cíclico

Ainda bastante semelhante aos algoritmos anteriores, com uma modificação apenas: o bit menos significativo a ser modificado é alternado entre as bandas de maneira cíclica. Por exemplo, para armazenar uma mensagem de apenas 4 bits na imagem o algoritmo gravaria o primeiro bit na banda R, o segundo bit na banda G, o terceiro na B e quarto voltaria para a banda R. Dessa forma, é produzida uma alternância na ordem pixels a serem modificados conseguindo, assim, impor uma dificuldade a mais para o estegoanalista detectar e obter a mensagem corretamente. A Figura 6 mostra a imagem original e a estego-imagem, utilizando o algoritmo LSB cíclico. É possível perceber claramente a semelhança entre elas.



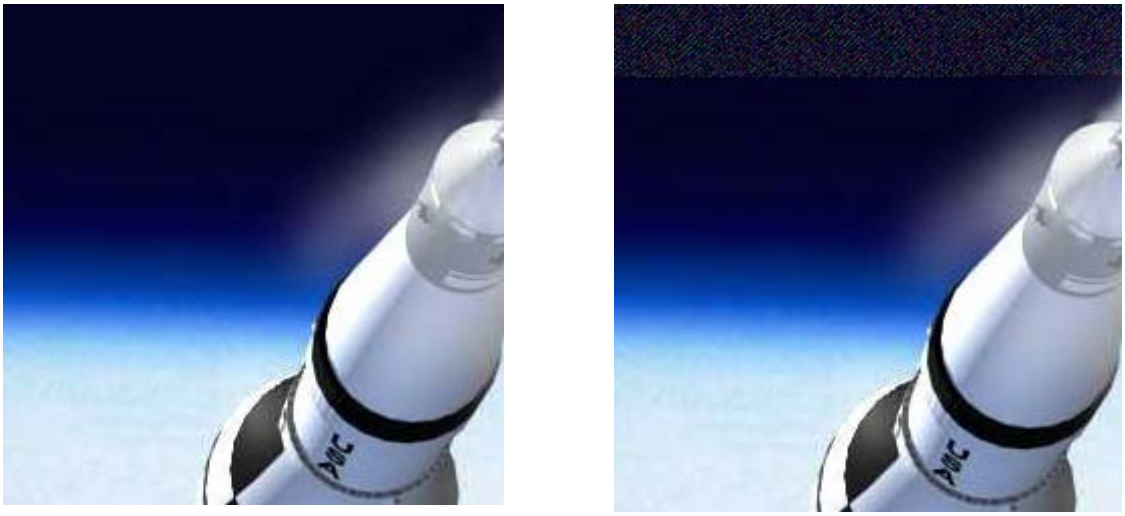
(a) (b)

Figura 6. (a) Imagem original colorida e com 250 x 250 pixels e (b) estego-imagem utilizando LSB cíclico e mensagem de 7.811 bytes.

LSB com salto

Em todos os algoritmos anteriores o que se apresentou foi a modificação de pixels em seqüência. Mesmo no LSB cíclico a seqüência é patente o que não apenas facilita a detecção através de métodos estatísticos de estegoanálise como também nos apresenta outro problema peculiar. No caso da mensagem a ser escondida na imagem ser bastante menor que a capacidade de armazenamento da mesma, o que se vê é apenas o início da figura modificado. Podemos perceber isso facilmente na Figura 7, pois o seu início (canto extremo superior esquerdo) apresenta uma grande

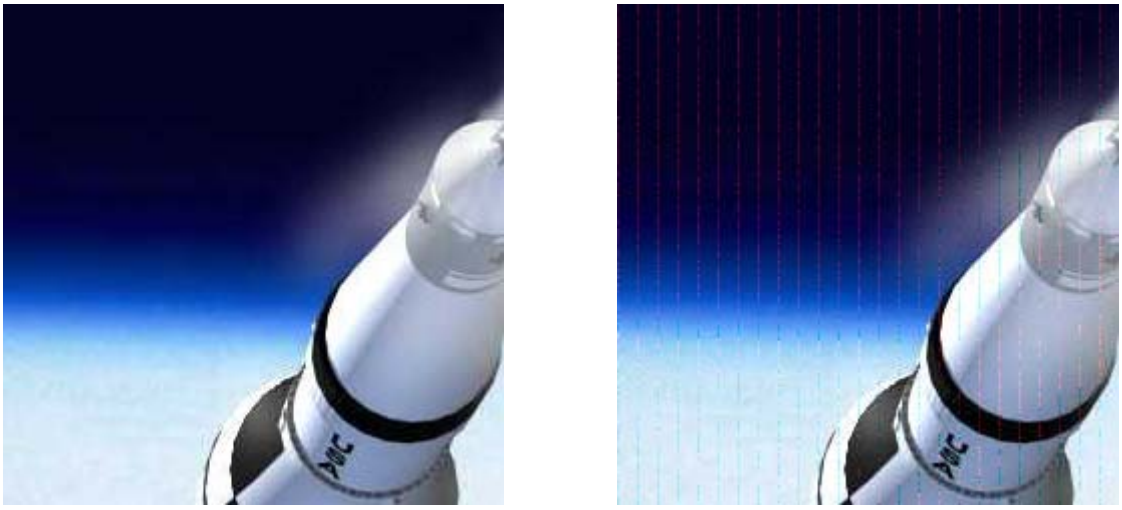
quantidade de *pixels* de uma mesma tonalidade, que interpretamos como sendo o espaço. A aplicação de um algoritmo de seleção de pixels em seqüência produz modificação apenas nesse trecho inicial o que facilita também a percepção visual.



(a) (b)

Figura 7. (a) Imagem original colorida e com 250 x 250 e (b) estego-imagem utilizando LSB 7 bits e mensagem de 7.811 bytes, demonstrando a fácil percepção à “olho nu”.

Para resolver o problema foi proposto um método de LSB com salto. Dessa forma, é possível informar um valor referente a quantidade de pixels entre cada bloco de *n* bits inseridos, sendo *n* a quantidade dos bits LSB escolhido no algoritmo. Também é possível o desenvolvimento de uma técnica semelhante baseada em chave, onde baseado na chave informada é calculado um vetor de seleção de pixels e seguindo esse vetor cada bloco de *n* bits é inserido na imagem. Essa técnica dificulta a detecção do uso de esteganografia na imagem e também aumenta ainda mais a semelhança entre as figuras por dividir de maneira mais equalitária o ruído adicionado no processo de embutir a informação. A Figura 8 nos dá um exemplo.



(a) (b)

Figura 8. (a) Imagem original colorida e com 250 x 250 e (b) estego-imagem utilizando LSB com valor de salto fixo = 10.

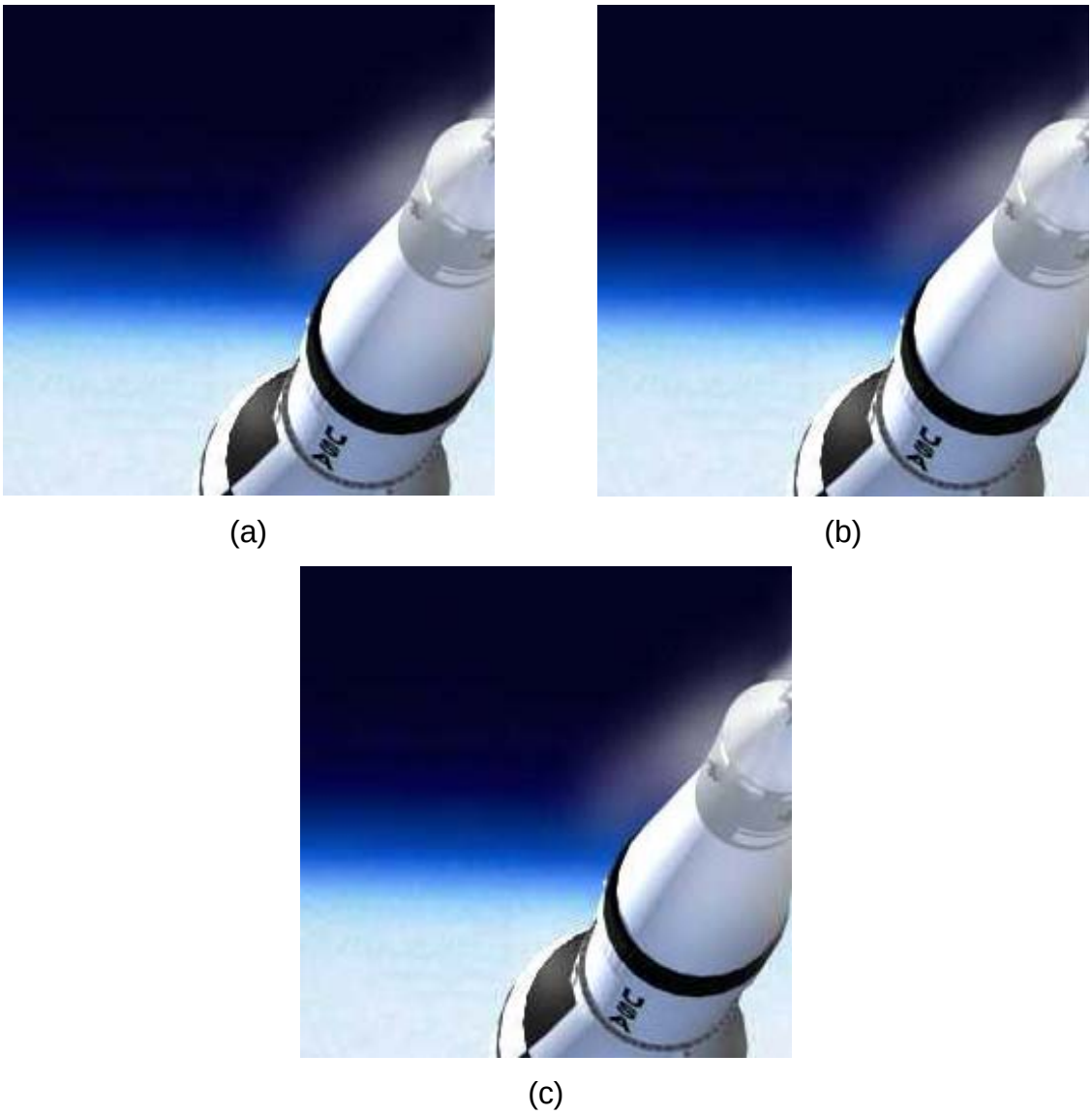
LSB com criptografia

Consiste em adicionar uma camada a mais de segurança, utilizando criptossistemas. Quaisquer dos algoritmos anteriores podem ser utilizados, a diferença é que a mensagem, antes de ser embutida no meio digital, é cifrada com algum algoritmo de criptografia como, por exemplo, DES ou AES [15].

Na prática, os efeitos em termos de esteganografia são os mesmos do algoritmo base utilizado, seja ele o LSB 1 bit ou o LSB com chave para seleção de pixels. A única diferença é que, caso a mensagem embutida seja retirada da imagem por algum método ou por um estegoanalista, se encontrará cifrada e será preciso ainda quebrar a técnica de criptografia. É importante ressaltar que não se espera com esse método conseguir a solução perfeita, mas, ao adicionarmos mais uma camada de segurança, estamos aumentando a dificuldade e o tempo necessário para alguém quebrar a proteção. Se conseguirmos garantir que o tempo para quebrar é maior que a validade útil da informação oculta na imagem, a eficiência terá sido alcançada.

Na Figura 9, apresentamos a mesma imagem utilizada no exemplo do LSB 1 bit (Figura 3), utilizando o mesmo algoritmo, porém com a prévia cifragem da

mensagem utilizando AES. É fácil perceber a semelhança na imagem gerada por essa técnica e a anterior.



(a) (b)

(c)

Figura 9. (a) Imagem original colorida e com 250 x 250, (b) estego-imagem utilizando LSB 1 bit e (c) a estego-imagem, utilizando o LSB 1 bit com cifragem AES.

Capítulo 3

Avaliação de Fidelidade entre Imagens

Avaliar fidelidade entre imagens consiste em analisar o grau de semelhança entre duas imagens. Inicialmente, a forma de comparar as imagens, original e modificada, era feita através da avaliação de um grupo de pessoas que atribuiriam notas, indicando o grau de semelhança entre elas. O resultado final seria uma média das notas dadas por cada avaliador. Esse método foi chamado de *mean opinion score* (MOS) e rapidamente se mostrou inviável dado o grau de subjetividade e o alto tempo para obtenção dos resultados.

Métodos automáticos de avaliação de imagens vêm sendo criados ao longo dos anos. Nesse sentido, podemos dividir esses métodos em termos da presença da imagem original, sendo uma referência completa (quando temos acesso à imagem original), sem referência (quando não temos acesso) e referência parcial (quando temos acesso a apenas alguns fragmentos da imagem original). Quando a análise não possui qualquer elemento da imagem original para prover um resultado comparativo, diz-se que é feita uma avaliação da qualidade da imagem [10]. Quando a referência ou parte dela existe, diz-se que é feita uma avaliação de fidelidade de imagem [20]. Notadamente, há relação entre os dois conceitos já que uma imagem fiel à imagem original é uma imagem de boa qualidade.

Assim como grande parte das abordagens existentes nessa área, este trabalho usa técnicas de referência completa. Ou seja, temos acesso completo a imagem original, que neste caso consiste na imagem sem a inserção da mensagem por esteganografia. Então, usamos elementos relacionados com fidelidade de imagens.

Podemos, ainda, dividir os métodos quanto à forma de análise das matrizes correspondentes às imagens. De um lado, os métodos de análise pixel-a-pixel como

por exemplo, o erro médio quadrático. De outro, uma nova abordagem que consiste na tentativa de usar elementos de percepção visual para a análise. São algoritmos que tentam “imitar” o sistema visual humano a fim de se obter melhores resultados.

A seguir, definimos brevemente alguns desses índices de fidelidade que são utilizados nos experimentos do Capítulo 4 deste trabalho.

3.1 Métodos de Análise Pixel-a-Pixel

Essa classe é composta por métodos que se utilizam essencialmente da análise matemática sobre os valores das matrizes de cores das imagens. Tais métodos são comumente chamados de distâncias. A baixa complexidade e custo computacional as tornam ainda bastante utilizadas, embora exista um número significativo de estudos [23] que demonstram a sua ineficiência para análise de qualidade visual. Nas medidas apresentadas, consideramos que *x* é a imagem original (ou de referência) e *y* é a imagem de teste. Apresentamos resumidamente aqui o Erro Médio Quadrático, Razão Sinal-Ruído de Pico, e as distâncias euclidiana, *City-Block*, *Minkowski*, *Canberra* (medidas de dissimilaridade) e a separação angular (medida de similaridade) [25] .

3.1.1 Erro Médio Quadrático (*MSE – Mean Square Error*)

Apesar de amplamente conhecida e bastante utilizada para análise de fidelidade, essa métrica não apresenta bons resultados em diversos casos. É possível analisar imagens modificadas por diferentes filtros de distorção e com o mesmo valor de MSE. Segundo *Zhou Wang et al* [22], isso se deve ao fato de que o MSE é sensível apenas a alterações de energia e não à perda de informação real.

O cálculo do MSE é dado pela Eq.1 e, quanto menor o seu valor absoluto, menor o erro.

$$MSE = \frac{1}{m * n} \sum_{y=1}^{m} \sum_{x=1}^{n} \left[I(x,y) - I'(x,y) \right] \qquad \text{(Eq.1)}$$

Onde *m* e *n* são as dimensões da matriz, *I* é a imagem alvo e *I'* é a imagem de referência.

3.1.2 PSNR (Peak Signal-to-Noise Ratio)

Corresponde apenas a um ajuste de escala (agora logarítmica) do MSE. O seu cálculo é dado pela Eq.2 e, quanto maior o seu valor absoluto, menor o erro.

$$PSNR = 10 \log_{10} \left(\frac{S^2}{MSE} \right) \qquad \text{(Eq.2)}$$

onde *S* é o valor máximo dos elementos na amostra. No caso, por exemplo, de imagens com 256 tons de cinza, *S* é 255, pois esse é o valor máximo que cada componente de cor pode alcançar (0 a 255).

3.1.3 Distância euclidiana

O cálculo da distância euclidiana é dado pela Eq.3 e representa em valor absoluto a diferença entre o valor original e o valor de teste.

$$D_{euclidiana} = \sqrt{\sum_{i=1}^{p} \left(x_i - y_i \right)^2} \qquad \text{(Eq.3)}$$

3.1.4 Distância *City-block*

Também conhecida como *Manhattan* ou distância de valor absoluto, tem esse nome porque seu cálculo é indicado para o cálculo de distância entre pontos de uma cidade. O cálculo da distância *city-block* é dado pela Eq.4.

$$D_{city-block} = \sum_{i=1}^{p} \left| x_i - y_i \right| \qquad \text{(Eq.4)}$$

3.1.5 Distância de Minkowski

É apenas uma generalização das distancias euclidiana e *City-block*, o cálculo da distância de *Minkowski* de ordem *m* é dada pela Eq.5.

$$D_{Minkowski} = \sqrt[m]{\sum_{i=1}^{p} \left| x_i - y_i \right|^m} \qquad \text{(Eq.5)}$$

3.1.6 Distância de Canberra

O cálculo da distância *Canberra* é dada pela Eq.6 e é uma soma de uma série de frações, sendo útil para variáveis que podem assumir valores negativos.

$$D_{canberra} = \sum_{i=1}^{p} \frac{\left| x_i - y_i \right|}{x_i + y_i} \qquad \text{(Eq.6)}$$

3.1.7 Separação angular

O cálculo da separação angular é dado pela Eq.7 e representa uma medida do ângulo entre vetores unitários na direção de dois vetores padrão de interesse.

$$S_{angular} = \frac{\sum_{i=1}^{p} x_i y_i}{\sqrt{\sum_{i=1}^{p} x_i^2 \sum_{i=1}^{p} y_i^2}} \qquad \text{(Eq.7)}$$

3.1.8 Índice Q

O índice universal de qualidade de imagem, ou simplesmente índice Q, foi proposto por *Zhou Wang et al* em [22], com o intuito de resolver os problemas inerentes às outras métricas no tocante aos resultados não satisfatórios para alguns tipos de distorções. Para tanto, essa abordagem não depende das imagens que são testadas, nem nas condições visuais e, tampouco, da análise subjetiva de um observador. Na verdade, apesar de proposto como índice de qualidade, o índice Q avalia a fidelidade entre imagens.

Esse índice utiliza três componentes para calcular a diferença entre as imagens: perda de correlação, distorção de luminância e distorção de contraste. A expressão que resulta no valor de Q é definida pela Eq.8, tendo seus valores variando entre -1 e 1, onde 1 indica duas imagens iguais.

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{\left(\sigma_x^2 + \sigma_y^2\right)\left[\left(\bar{x}\right)^2 + \left(\bar{y}\right)^2\right]} \qquad \text{(Eq.8)}$$

onde:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i,$$

$$\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \bar{x}\right)^2, \quad \sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}\left(y_i - \bar{y}\right)^2$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right)$$

Sendo *N* é a quantidade total de pixels da imagem, *x* e *y* são a matriz de pixels da imagem original e de teste, respectivamente. Enquanto *xi* e *yi* são os pixels na posição *i* da imagem *x* e da imagem *y*, respectivamente.

3.2 Métricas baseadas no sistema visual humano

São métricas que se utilizam da capacidade do sistema visual humano de ser altamente adaptado à extração de informação estrutural a partir do campo visual. Dessa forma, medir as alterações provocadas na estrutura da imagem podem garantir um bom resultado na comparação entre imagens.

O índice SSIM (*Structural Similarity*), desenvolvido por *Zhou Wang et al* e apresentado em [23] pode ser calculado com a Eq 9.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \qquad \text{(Eq.9)}$$

O índice SSIM equivale ao Q quando C_1=C_2=0, o que produz resultados bastante instáveis quando $\mu_x^2 + \mu_y^2$ ou $\sigma_x^2 + \sigma_y^2$ são muito próximos de zero. A Figura 10 mostra um conjunto de imagens para exemplificar a análise de fidelidade, utilizando os índices apresentados nesta Seção. Nessa Figura, apresentamos uma imagem de teste (Figura 10a) e diversas modificações implementadas nela: b) aplicação de um filtro Gaussiano, c) aplicação de um filtro *blur*, d) alteração no brilho e (e) alteração no contraste. Na Tabela 1 apresentamos o valor de cada um dos índices calculados.

Percebe-se que enquanto mudanças na estrutura (aplicação do filtro *Blur*) afetam diretamente o resultado do SSIM, a variação do brilho influencia mais fortemente o índice Q.

(a)

(b)

(c)

(d)

(e)

Figura 10. Análise de fidelidade de imagens, (a) imagem original, (b) imagem original após aplicação de filtro gaussiano, (c) imagem original após aplicação do filtro *blur*, (d) alteração no brilho e (e) no contraste da imagem original.

Tabela 1. Valores dos índices de fidelidade calculados.

Índice	Figura 10 (b)	Figura 10 (c)	Figura 10 (d)	Figura 10 (e)
MSE	71,6581	559,1279	2500	2486,0535
PSNR	29,5782	20,6557	14,1514	14,1757
Euclidiana	2167,0681	6053,3468	12800	12764,247
City-Block	278340	1087998	3276800	2973816
Minkowski	502,9253	1197,9315	2015,8737	2139,3434
Canberra	2639,1302	8079,9999	17136,4086	13182,9279
Sep. Angular	0,0023508	0,0017831	0,0034481	0,0034224
Q	0,99931	0,96606	0,77062	0,84676
SSIM	0,93553	0,65358	0,86939	0,88601

Capítulo 4

Experimentos

Neste Capítulo, apresentamos uma série de experimentos realizados com o objetivo de avaliar o funcionamento dos algoritmos desenvolvidos durante a realização deste trabalho. Para isso, preparamos um banco de imagens composto por 10 figuras de tamanho, forma e complexidade variados.

Os algoritmos foram desenvolvidos utilizando o Matlab e cada um deles permite a variação de parâmetros como quantidade de bits ou a componente de cor a ser modificada. As técnicas foram desenvolvidas, inicialmente, na forma de *scripts*, onde cada um implementava um método (LSB 1 bit, etc.). Posteriormente, visando facilitar a experimentação e obtenção dos resultados, foi criada uma interface gráfica (GUI), utilizando o *guide* do Matlab, chamado *Stego Suite*. Essa interface proporciona uma facilidade na escolha dos parâmetros de cada experimento, e também apresenta o resultado final, ou seja, a estego-imagem gerada e os índices de similaridade entre ela e a imagem original.

Na Figura 11 pode-se observar a interface gráfica. Podemos perceber a facilidade de variação dos parâmetros e da obtenção do resultado final da aplicação do algoritmo de esteganografia LSB *n* bit cíclico com n=8 e mensagem de 7.060 bytes.

No tocante aos parâmetros de cada algoritmo, variamos a utilização de cada um deles em termos da quantidade de bits LSB a serem modificados na imagem com a finalidade de tornar possível a análise do impacto dessa alteração não apenas através da utilização dos índices de similaridade, mas também através do nosso sistema visual. Já na escolha de qual componente de cor modificar (R,G ou B) optamos por, sempre que possível, modificar a banda de cor B, devido a dificuldade inerente ao ser humano de visualizar esse componente [7]. Dessa forma, buscamos tornar as alterações nas imagens o menos perceptível possível aos nossos olhos.

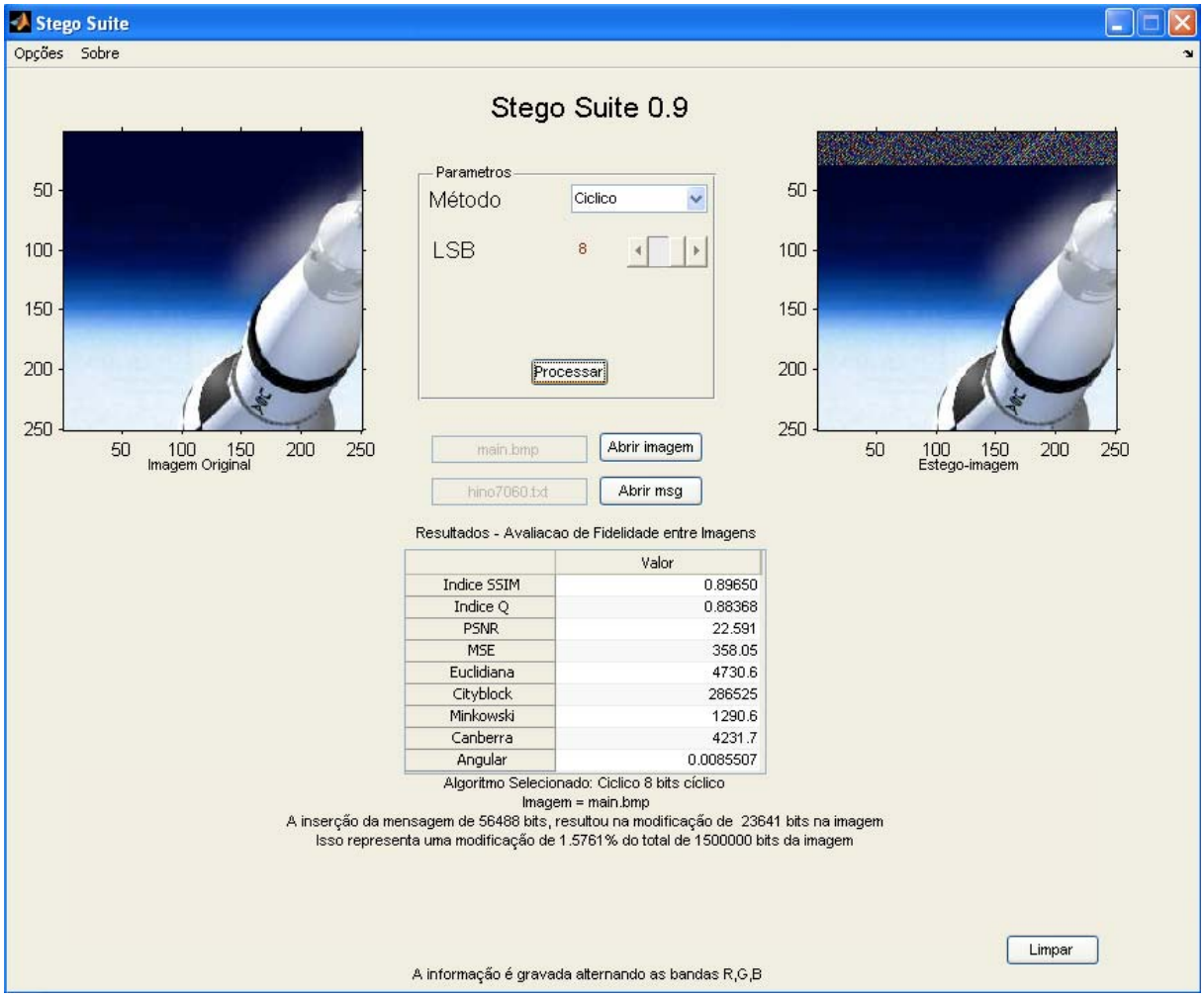


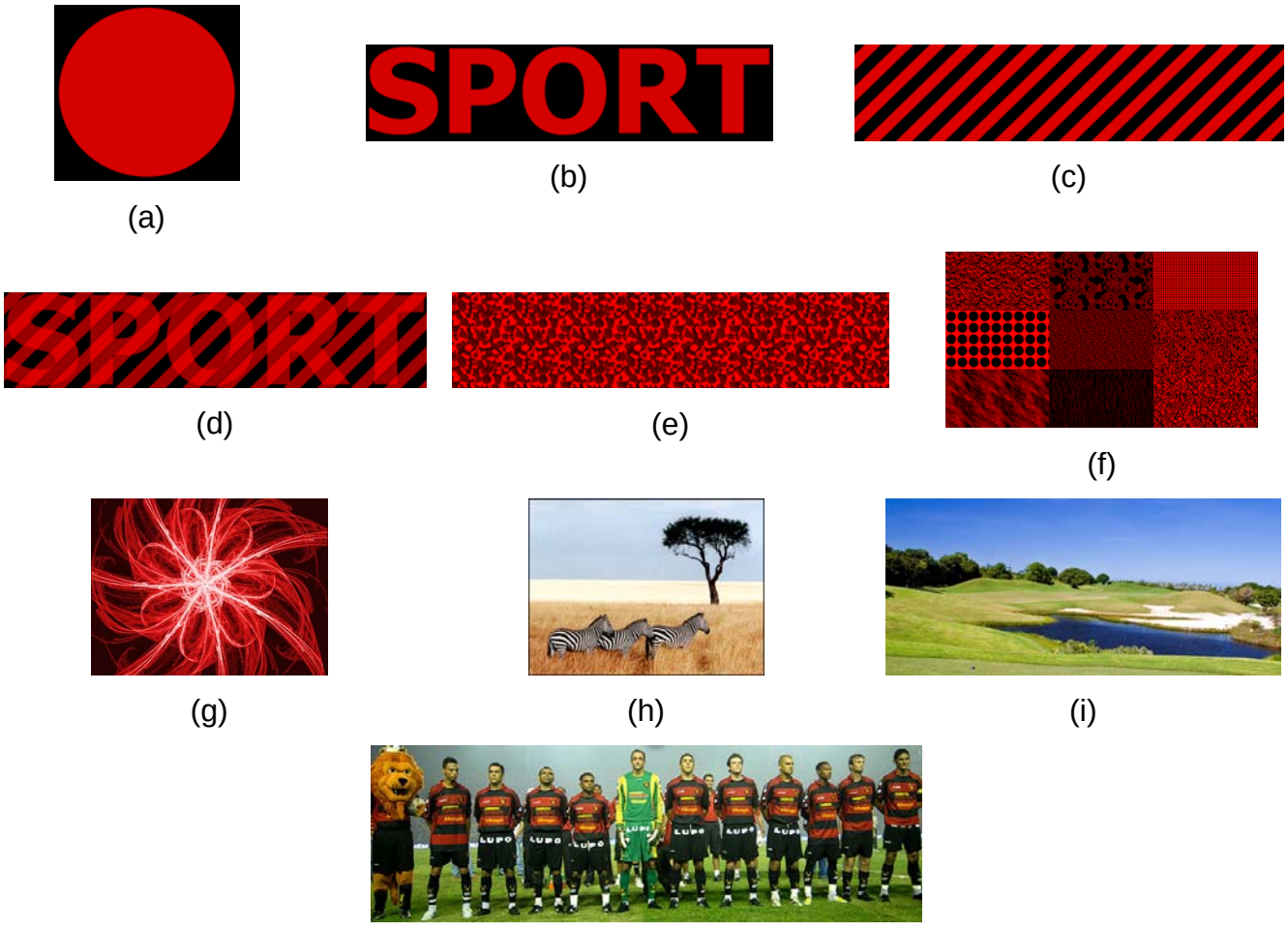
Figura 11. *Screenshot* da interface gráfica para os algoritmos desenvolvidos

Devido às diferenças entre as imagens (tamanho, forma, complexidade) e também entre os algoritmos, optamos por utilizar como informação a ser oculta na imagem o Hino Nacional Brasileiro, repetido *n* vezes de modo que o tamanho da mensagem seja aproximadamente a capacidade máxima para o conjunto de parâmetros do algoritmo e imagem escolhidos.

Observamos ainda que as imagens em vermelho e preto, Figura 12(a), (b), (c), (d), (e) e (f), por não possuírem valor diferente de zero nas componentes G e B causavam o mau funcionamento de alguns dos índices de similaridade (Q, *cityblock*, *canberra* e separação angular). Para mitigar esse problema optamos por modificar o componente de cor a ser modificado. Nesses casos específicos, utilizamos o componente de cor R.

4.1 Banco de Imagens

Como já citado, o banco de imagens é composto por 10 figuras em grau crescente de complexidade. Isso é patente ao observar a Figura 12. Como imagem mais simples, Figura 12 (a), temos o círculo vermelho inscrito em um quadrado preto enquanto que a imagem mais complexa, Figura 12 (j), é a fotografia do time do Sport Club do Recife, por conter um maior número de objetos e detalhes. O tamanho da figura também é um fator variável.



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

Figura 12. Banco de imagens utilizado para os experimentos e a dimensão das imagens: (a) círculo inscrito no quadrado (357x354 pixels), (b) letras (713x172 pixels), (c) listras inclinadas (746x172 pixels), (d) letras com listras inclinadas (710x162 pixels), (e) textura (746x164 pixels), (f) várias texturas (373x206 pixels), (g) fractal (281x206 pixels), (h) zebras (533x400 pixels), (i) paisagem (746x332 pixels) e (j) time do Sport Club do Recife (745x234 pixels).

4.2 Aplicação dos Algoritmos

Nesta Seção, apresentamos os resultados da comparação das imagens originais com as estego-imagens após a aplicação de cada um dos algoritmos. O valor utilizado para os parâmetros C1 e C2 do índice SSIM foram, respectivamente, 0,01 e 0,05.

4.2.1 LSB Simples

1 Bit

A Tabela 2 apresenta os resultados da análise comparativa entre a imagem original e sua versão esteganografada contendo uma mensagem escondida. O tamanho dessa mensagem varia de acordo com o tamanho da imagem para testarmos os algoritmos em sua máxima capacidade.

Tabela 2. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 1 bit

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	0,52	50,99	255,51	65286	40,27	15883,12	7,5e-91	0,08	0,992	R	15665
12b	0,48	51,29	243,51	59297	38,99	27023,47	9e-108	0,26	0,987	R	14922
12c	0,50	51,13	253,58	64303	40,06	27487,47	0,00573	0,54	0,989	R	16014
12d	0,47	51,41	232,38	54002	37,80	11737,40	0,00327	0,66	0,995	R	14177
12e	0,49	51,18	246,07	60553	39,27	247,55	0,00585	0,99	0,999	R	14922
12f	0,48	51,28	192,83	37185	33,38	2955,56	0,00321	0,99	0,999	R	9340
12g	0,49	51,18	169,32	28672	30,60	2164,54	0,00058	0,94	0,997	B	7060
12h	0,49	51,19	324,47	10581	47,22	7037,60	6,72e-9	0,99	0,998	B	26455
12i	0,49	51,16	351,09	123264	49,77	3884,87	0,00095	0,92	0,998	B	30880
12j	0,50	51,17	294,25	86584	44,24	7145,72	0,00066	0,99	0,998	B	21627

Quanto à análise do Erro Médio Quadrático (MSE) e o PSNR, seus valores devem ser o mais baixo e o mais alto possível, respectivamente. Com apenas um experimento, não podemos concluir o comportamento do algoritmo baseado nessas medidas.

Para as distâncias, o valor esperado deve ser baixo, onde uma distância com valor zero corresponderia a uma comparação entre imagens iguais. Esse conceito é válido para as distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra*. No caso da Separação Angular, seu valor deve ser elevado para indicar imagens semelhantes.

Os valores de Q e de SSIM, como já mencionado, devem tender a 1 para indicar alta similaridade entre as imagens.

4 Bits

A Tabela 3 apresenta os resultados para o algoritmo LSB usando 4 bits para armazenar a mensagem.

Tabela 3. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 4 bits

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	35,64	32,61	2122,42	586516	350,20	31995,53	6,7e-91	0,08	0,732	R	62660
12b	44,50	31,60	2349,06	645956	385,24	53862,55	8e-108	0,25	0,607	R	59688
12c	45,27	31,57	2410,22	686396	390,82	54888,47	0,00571	0,49	0,680	R	64056
12d	40,38	32,07	2155,24	599320	353,55	24101,00	0,00328	0,61	0,836	R	56708
12e	47,86	31,33	2419,87	689022	389,29	2686,87	0,00595	0,98	0,981	R	59688
12f	43,81	31,71	1834,67	409240	321,49	8442,82	0,00323	0,98	0,974	R	37360
12g	38,49	32,28	1492,61	288034	275,17	15466,98	0,00058	0,60	0,878	B	28240
12h	42,11	31,89	2996,55	112778	442,49	18243,77	6,7e-9	0,82	0,913	B	105820
12i	43,13	31,78	3268,31	1326813	469,466	15445,03	0,00095	0,56	0,901	B	123520
12j	41,24	31,98	2681,23	907290	409,78	30005,65	0,00066	0,78	0,907	B	86508

Ao comparar os resultados obtidos na aplicação dos algoritmos LSB 1 bit e LSB 4 bits (Tabela 2 e Tabela 3, respectivamente) podemos perceber que a alocação de mais bits para ocultação da mensagem afeta diretamente os índices de similaridade entre as imagens.

Embora as figuras geradas pela aplicação dos algoritmos sejam bem semelhantes a ponto de não ser uma tarefa trivial a análise de similaridade pelo nosso sistema visual, os índices de fidelidade ilustram essa avaliação. De uma forma geral, todos os índices avaliados demonstram um impacto maior na diminuição de qualidade das images geradas pelo LSB 4 bits. Podemos perceber o aumento do Erro Médio Quadrático e a conseqüente diminuição do PSNR. As distâncias Euclidiana, *CityBlock*, *Minkowski* e *Canberra* também tiveram seus respectivos valores acrescidos. Os índices Q e SSIM apresentam redução.

8 Bits

Na tabela 4, podemos ver os resultados da comparação da imagem original com a estego-imagem, usando 8 bits para armazenar a mensagem.

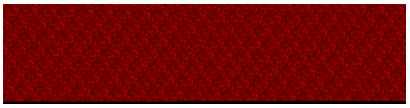
Tabela 4. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 8 bits

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	16026	6,08	45004,45	13267958	7079,54	69438,66	6,1e-90	0,00	0,018	R	125320
12b	16515	5,95	45003,88	12951346	7122,44	82614,06	1,5e-107	0,00	0,012	R	119376
12c	16759	5,89	46372,36	13821005	7256,88	86786,39	0,00417	0,00	0,014	R	128112
12d	12095	7,30	37298,92	10166206	6087,18	56486,88	0,00368	0,00	0,020	R	113416
12e	11645	7,47	37746,22	10712267	6174,93	46093,30	0,00694	0,00	0,022	R	119376
12f	10742	7,82	28729,68	6423125	5041,99	34687,81	0,00295	0,00	0,017	R	74720
12g	14974	6,38	29441,34	5745135	5314,65	38348,55	0,00024	0,00	0,009	B	56480
12h	14701	6,46	55985,37	21290160	8167,94	94971,40	8,8e-9	0,00	0,023	B	211640
12i	13642	6,70	50120,71	20002090	8293,56	109383,96	0,0012	0,00	0,026	B	247040
12j	12995	6,99	47596,84	16189860	7183,98	99699,25	0,0044	0,00	0,017	B	173016

Nesse caso, fica clara a queda na qualidade da imagem em comparação com os métodos anteriores. Os valores calculados para as distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra* cresceram bastante. O índice Q, reduziu para valores de ordem de grandeza 10^{-4}, tornando-se zero em uma aproximação de duas casas decimais. O SSIM também se aproximou de zero, seguindo a tendência. O MSE cresceu bastante, reduzindo o PSNR.

O comportamento dos índices se deu conforme o esperado e observado nas imagens geradas. Uma modificação de 8 bits tende a tornar a imagem inutilizável, como podemos ver na Figura 13, ainda que todo o processo seja dependente da mensagem. Ou seja, mensagens distintas podem implicar resultados diferentes embora a tendência natural é de se obter valores muitos próximos para mensagens distintas. É muito pouco provável que uma determinada mensagem, ao ser convertida caractere a caractere para bits, possa gerar uma sequência de bits exatamente igual à presente na imagem original. Para esse caso hipotético a mensagem seria inserida corretamente, sua posterior extração seria possível, mas devido a não haver mudança nos valores dos pixels as imagens seriam idênticas.

(a)



(b)

Figura 13. (a) Imagem original e (b) estego-imagem gerada a partir da aplicação do algoritmo LSB 8 bits com uma mensagem de 119.376 bytes.

4.2.2 LSB cíclico

1 Bit

Pode-se observar, na Tabela 5, os resultados da comparação das imagens originais com as imagens geradas pela aplicação do algoritmo LSB 1 bit cíclico.

Tabela 5. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 1 bit cíclico

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	0,15	56,38	137,47	18899	26,64	5347,93	1,6e-83	0,08	0,998	R,G,B	15665
12b	0,15	56,40	135,09	18249	26,33	9024,16	9,1e-99	0,26	0,997	R,G,B	14922
12c	0,15	56,29	140,06	19616	26,97	9210,43	0,00572	0,54	0,998	R,G,B	16014
12d	0,23	54,55	161,98	26236	29,71	4053,75	0,00325	0,66	0,998	R,G,B	14177
12e	0,20	54,99	158,62	25161	29,30	268,54	0,00584	0,99	0,999	R,G,B	14922
12f	0,20	55,05	124,86	15589	24,98	1208,16	0,00320	0,99	0,999	R,G,B	9340
12g	0,18	55,63	101,40	10282	21,745	133,31	0,00174	0,99	0,999	R,G,B	7060
12h	0,15	56,34	179,52	32228	31,82	1879,35	4,4e-10	0,99	0,999	R,G,B	26455
12i	0,18	55,63	209,838	44032	35,31	773,08	0,00365	0,98	0,999	R,G,B	30880
12j	0,17	55,77	173,21	30002	31,07	601,98	0,00426	0,99	0,999	R,G,B	21627

Ao compararmos os resultados obtidos pela aplicação do LSB 1 bit normal e cíclico (Tabela 2 e Tabela 5, respectivamente), podemos perceber que a estratégia de alternar os componentes de cor (R,G e B) para cada bit inserido proporcionou uma imagem de melhor qualidade, mais próxima da original.

Embora não seja possível perceber à “olho nu”, os índices de similaridade demonstram uma maior similaridade para as imagens geradas pelo LSB 1 bit cíclico. O MSE teve seu valor, percentualmente, bastante reduzido e como conseqüência elevou o PSNR. As distâncias Euclidiana, *CityBlock*, *Minkowski* e *Canberra* apresentaram seus valores bastante reduzidos. Os índices Q e SSIM, tiveram seus valores acrescidos, indicando uma similaridade maior.

4 Bits

Na Tabela 6, apresentamos os resultados da comparação usando o algoritmo LSB 4 bits Cíclico.

Tabela 6. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 4 bits cíclico

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	10,09	38,09	1128,99	280538	195,25	29779,17	1,3e-83	0,08	0,863	R,G,B	62660
12b	10,33	37,99	1125,53	278740	194,42	49636,87	7,2e-99	0,25	0,782	R,G,B	59688
12c	10,54	37,90	1163,09	298130	198,68	50526,33	0,00568	0,49	0,816	R,G,B	64056
12d	10,35	37,98	1090,89	268251	190,00	22407,43	0,00318	0,59	0,906	R,G,B	56708
12e	10,27	38,01	1120,96	281284	193,42	2848,16	0,00575	0,98	0,986	R,G,B	59688
12f	10,27	38,01	888,407	176035	165,86	7881,98	0,00312	0,97	0,979	R,G,B	37360
12g	6,56	39,96	616,49	103800	122,56	1153,14	0,00174	0,95	0,990	R,G,B	28240
12h	6,43	40,04	1171,36	355031	190,59	10084,97	4,4e-10	0,92	0,981	R,G,B	105820
12i	7,01	39,67	1317,69	458226	204,93	4629,44	0,00365	0,78	0,974	R,G,B	123520
12j	7,03	39,66	1107,50	323966	182,65	5195,84	0,00427	0,94	0,987	R,G,B	86508

Os resultados demonstram uma maior perda de qualidade das imagens geradas pelo algoritmo LSB 4 bits cíclico em comparação com o LSB 1 bit cíclico (Tabela 6 e Tabela 5, respectivamente). Esse comportamento já era esperado porque desde o início do trabalho foi percebido, empíricamente, que o aumento da quantidade de bits a ser modificada por pixel implica numa maior alteração da imagem.

Assim como o LSB 1 bit cíclico apresentou resultados melhores que o LSB 1 bit simples, suas respectivas versões com alocação de 4 bits para mensagem, seguiram a mesma tendência.

As distâncias Euclidiana, *CityBlock*, *Minkowski* e *Canberra* resultam em valores menores para a versão cíclica do algoritmo LSB 4 bits, o que indica imagens mais próximas da original. O MSE, segue a tendência, também valores bem menores que na versão simples do algoritmo, e como conseqüência, o PSNR nos retorna valores maiores. A avaliação dos resultados SSIM, mais uma vez segue as demais, valores mais próximos de 1, que significa imagens mais fidedignas. Os valores obtidos no índice Q apresentam uma discrepância. Em algumas imagens

(Fig 12(d) e Figura 12(f)), apontando pra um melhor desempenho do LSB 4 bits simples, enquanto que as demais imagens tem valores de Q mais próximos de 1 para o algoritmo LSB 4 bits cíclico.

4.2.3 LSB com Salto Fixo

1 Bit

Na Tabela 7, apresentamos os resultados da comparação usando o algoritmo LSB 1 bit com salto fixo definido com valor 3 pixels.

Tabela 7. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 1 bit com salto de 3 pixels.

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	0,17	55,80	146,93	21588	27,84	5170,82	7,4e-91	0,08	0,998	R	5200
12b	0,16	56,08	140,14	19640	26,98	8762,51	9e-108	0,27	0,997	R	4900
12c	0,17	55,86	147,04	21621	27,85	9242,35	0,00573	0,55	0,998	R	5300
12d	0,15	56,20	133,91	17931	26,17	3872,43	0,00328	0,67	0,999	R	4700
12e	0,16	55,99	141,53	20031	27,16	82,66	0,00585	0,99	0,999	R	4900
12f	0,16	56,10	110,71	12256	23,06	1012,94	0,00320	0,99	0,999	R	3100
12g	0,16	56,05	96,64	9340	21,06	695,73	0,00058	0,96	0,999	B	2300
12h	0,16	55,98	186,97	34957	32,70	2401,97	6,7e-9	0,99	0,999	B	8750
12i	0,16	55,98	201,37	40552	34,36	1285,87	0,0094	0,97	0,999	B	10150
12j	0,16	56,02	168,41	28363	30,50	2402,36	0,00066	0,99	0,999	B	7100

Na comparação entre o LSB 1 bit simples e o LSB 1 bit com salto (Tabela 2 e Tabela 7, respectivamente), podemos perceber que a inclusão do salto entre bits na inserção da mensagem proporcionou a geração de estego-imagens mais semelhantes as suas respectivas imagens originais. Embora nosso sistema visual não consiga perceber, ao analisarmos os valores podemos perceber uma diminuição do MSE e um aumento do PSNR. As distâncias Euclidiana, *Cityblock*, *Minkowski* e Canberra, por sua vez, também apresentam valores menores, o que também corrobora com a análise. Os índices Q e SSIM, embora apresentem valores próximos para os dois algoritmos, podemos perceber uma pequena vantagem para o LSB 1 bit com salto.

Interessante notar que os valores obtidos para os índices de similaridade na aplicação dos algoritmos LSB 1 bit cíclico e LSB 1 bit com salto são bastante próximos. A depender da imagem escolhida temos uma pequena variação em todos

os índices. Neste caso, concluímos o LSB 1 bit cíclico como sendo melhor porque sua capacidade de ocultação de mensagem é *n* vezes maior que o LSB 1 bit cíclico com salto, onde *n* equivale ao valor especificado para o salto.

4 Bits

A comparação entre a imagem original e a estego-imagem gerada pela aplicação do algoritmo LSB 4 bits com salto fixo (no caso, 3 pixels) é apresentada na Tabela 8.

Analogamente ao que acontece na versão de 1 bit, a comparação entre o LSB 4 bits simples e o LSB 4 bits com salto (Tabela 3 e Tabela 8, respectivamente), podemos perceber que a inclusão do salto entre bits, na inserção da mensagem, proporcionou a geração de estego-imagens mais semelhantes a original. Embora nosso sistema visual não consiga perceber, ao analisarmos os valores podemos perceber uma diminuição do MSE e um aumento do PSNR. As distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra*, por sua vez, também apresentam valores menores, o que também corrobora com a análise. Os índices Q e SSIM, embora apresentem valores próximos para os dois algoritmos, ainda é possível perceber uma pequena vantagem para o LSB 4 bits com salto

Entretanto, na comparação entre o LSB 4 bits cíclico e o LSB 4 bits com salto (Tabela 6 e Tabela 8, respectivamente), podemos perceber diferenças mais significativas. Os valores de MSE foram menores para as imagens geradas por LSB 4 bits cíclico e, consequentemente, o PSNR foi maior. As distâncias *Minkowski* e Euclidiana também foram favoráveis ao LSB 4 bits cíclico enquanto que *Canberra* e *Cityblock* foi favorável ao LSB 4 bits com salto. Já a análise do índice Q, apresenta valores bem próximos para esses dois algoritmos, apenas algumas imagens (Figura 12(j)j e Figura 12(i)) apresentam uma discrepância maior entre elas. Os resultados do SSIM mostram valores muito próximos. Devido a esse comportamento dos índices, podemos apontar, mais uma vez, um melhor desempenho por parte do algoritmo LSB 4 bits cíclico porque sua capacidade de ocultação de mensagem também é *n* vezes maior que o LSB 4 bits cíclico com salto, onde *n* equivale ao valor especificado para o salto.

Tabela 8. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 4 bits com salto de 3 pixels

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	11,72	37,44	1216,87	192708	241,80	10671,57	7,1e-91	0,08	0,865	R	20800
12b	14,55	36,50	1335,91	209984	264,32	17717,68	8,9e-108	0,26	0,799	R	19600
12c	15,08	36,34	1391,38	228083	271,36	18517,70	0,00571	0,52	0,829	R	21200
12d	13,31	36,89	1237,23	198374	244,05	8100,81	0,00328	0,63	0,918	R	18800
12e	15,3	36,28	1368,16	222845	265,06	875,86	0,00588	0,99	0,993	R	19600
12f	14,28	36,58	1047,50	134530	220,57	2807,53	0,00321	0,99	0,991	R	12400
12g	12,79	37,06	860,39	95828	190,22	5068,30	0,00058	0,76	0,958	B	9400
12h	13,73	36,75	1711,11	368022	304,21	6187,56	6,7e-9	0,92	0,968	B	35000
12i	14,17	36,61	1873,40	438537	323,27	5115,44	0,00095	0,64	0,955	B	41170
12j	13,46	36,84	1532,02	297156	281,79	9800,47	0,00066	0,89	0,966	B	28400

4.2.4 LSB Cíclico com Salto Fixo

1 Bit

A comparação entre a imagem original e a estego-imagem gerada pela aplicação do algoritmo LSB 1 bit cíclico com salto fixo (no caso, 3 pixels) é apresentada na Tabela 9.

Tabela 9. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 1 bit cíclico com salto de 3 pixels

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	0,05	61,18	79,11	6258	18,42	1715,76	1,7e-83	0,13	0,999	R,G,B	5200
12b	0,05	61,24	77,37	5987	18,15	2966,65	9,2e-99	0,28	0,999	R,G,B	4900
12c	0,05	61,10	80,44	6471	18,63	3079,32	0,00572	0,59	0,999	R,G,B	5300
12d	0,07	59,33	93,44	8732	20,59	1310,49	0,00326	0,68	0,999	R,G,B	4700
12e	0,07	59,76	91,65	8400	20,32	90,10	0,00585	0,99	0,999	R,G,B	4900
12f	0,07	59,91	71,36	5092	17,20	409,416	0,00320	0,99	0,999	R,G,B	3100
12g	0,06	60,50	57,91	3354	14,97	43,26	0,00174	0,99	0,999	R,G,B	2300
12h	0,05	61,15	103,12	10633	21,99	624,74	4,4e-10	0,99	0,999	R,G,B	8750
12i	0,06	60,49	119,89	14373	24,31	249,19	0,00365	0,99	0,999	R,G,B	10150
12j	0,06	60,62	99,14	9829	21,42	222,56	0,00427	0,99	0,999	R,G,B	7100

A combinação das técnicas de salto entre pixels e alternância na seleção do componente de cor, proporcionou uma melhora na qualidade das imagens geradas em comparação com o LSB 1 bit simples (Tabela 2) e com o LSB 1 bit cíclico

(Tabela 5). Nesses casos, todos os índices foram favoráveis ao LSB 1 bit cíclico com salto.

A análise dos índices de fidelidade entre as imagens geradas pelo LSB 1 bit cíclico com salto (Tabela 9) e o LSB 1 bit simples com salto (Tabela 7), indicam uma boa melhora na qualidade das imagens geradas pelo primeiro. O MSE reduziu e, consequentemente, o PSNR aumentou. As distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra* também reduziram de forma favorável à versão com alternância do componente de cor. Já os índices Q e SSIM, embora tenham apresentado valores muito próximos entre os algoritmos, a diferença ainda foi favorável ao LSB 1 bit cíclico com salto.

4 Bit

A comparação entre a imagem original e a estego-imagem gerada pela aplicação do algoritmo LSB 4 bits cíclico com salto fixo (no caso, 3 pixels) é apresentada na Tabela 10.

Tabela 10. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 4 bits cíclico com salto de 3 pixels

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	3,36	42,86	651,77	93366	135,47	9852,54	1,6e-83	0,08	0,962	R,G,B	20800
12b	3,40	42,81	646,19	91675	134,44	6227,01	8,5e-99	0,26	0,947	R,G,B	19600
12c	3,51	42,67	671,78	99296	137,93	17118,62	0,00568	0,51	0,950	R,G,B	21200
12d	3,44	42,76	629,17	89368	131,72	7548,41	0,00323	0,62	0,973	R,G,B	18800
12e	3,36	42,86	641,30	92159	133,42	938,78	0,00581	0,99	0,994	R,G,B	19600
12f	3,40	42,80	511,54	58486	114,83	2600,82	0,00318	0,99	0,993	R,G,B	12400
12g	2,17	44,77	354,38	34528	84,39	381,69	0,00174	0,96	0,996	R,G,B	9400
12h	2,10	44,90	669,47	116649	131,08	3475,40	4,4e-10	0,97	0,994	R,G,B	35000
12i	2,30	44,50	756,23	152084	141,07	1542,30	0,00364	0,88	0,991	R,G,B	41170
12j	2,28	44,54	631,20	105828	125,19	1741,67	0,00426	0,97	0,995	R,G,B	28400

Analogamente à versão de 1 bit, a combinação das técnicas de salto entre pixels e alternância na seleção do componente de cor, proporcionou uma melhora na qualidade das imagens geradas em comparação com o LSB 4 bits simples (Tabela 3) e com o LSB 4 bits cíclico (Tabela 6). Nesses casos, todos os índices foram favoráveis ao LSB 4 bits cíclico com salto

A análise dos índices de fidelidade entre as imagens geradas pelo LSB 4 bit cíclico com salto (Tabela 10) e o LSB 4 bit simples com salto (Tabela 8), indicam uma boa melhora na qualidade das imagens geradas pelo primeiro. O MSE reduziu grandemente, e consequentemente, o PSNR aumentou. As distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra* também reduziram de forma favorável à versão com alternância do componente de cor. O índice Q apresentou, valores muito próximos entre os dois algoritmos. O SSIM apresentou valores mais favoráveis, mais próximos de 1, nos resultados da versão com alternância de componente de cor.

4.2.5 LSB com Chave para Seleção de Pixels

1 Bit

A comparação entre a imagem original e a estego-imagem gerada pela aplicação do algoritmo LSB 1 bit com chave para seleção de pixels (no caso, chave=*"stegokey"*) é apresentada na Tabela 11.

Tabela 11. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 1 bit com a chave para seleção de pixels definida como "stegokey".

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	0,13	56,81	130,85	17121	25,77	3503,98	7,4e-91	0,15	0,998	R	4076
12b	0,13	56,83	128,54	16524	25,47	7093,75	9e-108	0,30	0,998	R	4076
12c	0,13	57,09	127,76	16322	25,37	6960,18	0,00573	0,58	0,998	R	4076
12d	0,13	56,82	124,73	15558	24,96	3401,58	0,00328	0,67	0,999	R	4076
12e	0,14	56,76	129,47	16763	25,59	69,08	0,00585	0,99	0,999	R	4076
12f	0,13	56,85	101,55	10314	21,77	876,118	0,00321	0,99	0,999	R	2584
12g	0,14	56,61	90,63	8214	20,18	626,82	0,00058	0,96	0,999	B	2005
12h	0,14	56,73	171,52	29421	30,87	1864,16	6,7e-9	0,99	0,999	B	7455
12i	0,14	56,58	188,07	35370	32,82	1120,80	0,00095	0,97	0,999	B	8817
12j	0,14	56,69	155,80	24274	28,95	2135,72	0,00066	0,99	0,999	B	6086

A idéia de adicionar como parâmetro ao LSB 1 bit simples, uma chave que o algoritmo utilizará para definir um vetor de seleção de pixels, proporcionou uma melhora significativa nas imagens geradas.

Ao comparar o resultado dos índices de fidelidade entre as imagens original e as estego-imagens geradas pelos algoritmos LSB 1 bit salto fixo com salto=3 (Tabela 7) e LSB 1 bit com chave para seleção de pixels com chave=*"stegokey"*

(Tabela 11) verificamos uma redução no MSE e, consequentemente, aumento do PSNR para a versão com chave. As distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra*, também diminuíram favoravelmente à versão com seleção baseada em chave. Os índices Q e SSIM, seguiram o comportamento dos demais e também apresentaram valores mais próximos de 1, indicando imagens mais fiéis, para o algoritmo LSB 1 bit com chave para seleção de pixels.

4 Bits

A comparação entre a imagem original e a estego-imagem gerada pela aplicação do algoritmo LSB 4 bits com chave para seleção de pixels (no caso, chave=*"stegokey"*) é apresentada na Tabela 12.

Tabela 12. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 4 bits com a chave para seleção de pixels definida como "stegokey".

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	8,70	38,74	1048,02	146720	217,17	7190,68	7,1e-91	0,14	0,906	R	16304
12b	12,01	37,33	1213,53	173906	247,60	14187,84	8,9e-108	0,29	0,839	R	16304
12c	11,54	37,51	1216,64	174488	248,10	14231,10	0,00571	0,55	0,870	R	16304
12d	11,45	37,54	1147,62	171240	232,03	7082,36	0,00328	0,63	0,930	R	16304
12e	12,79	37,06	1251,22	185887	249,95	730,91	0,00587	0,99	0,994	R	16304
12f	12,13	37,29	965,43	113325	209,50	2373,27	0,00321	0,99	0,992	R	10336
12g	10,96	37,73	796,59	81937	181,07	4295,48	0,00058	0,78	0,964	B	8020
12h	11,82	37,40	1587,95	316203	289,32	5201,80	6,7e-9	0,93	0,973	B	29820
12i	12,04	37,32	1727,35	374816	305,72	4340,58	0,00095	0,66	0,961	B	35268
12j	11,42	37,55	1410,87	253134	266,35	8368,71	0,00066	0,90	0,970	B	24344

Analogamente a versão 1 bit, a idéia de adicionar como parâmetro ao LSB 4 bits simples uma chave que o algoritmo utilizará para definir um vetor de seleção de pixels, proporcionou uma melhora significativa nas imagens geradas.

Ao comparar o resultado dos índices de fidelidade entre as imagens original e as estego-imagens geradas pelos algoritmos LSB 4 bits salto fixo com salto=3 (Tabela 8) e LSB 4 bits com chave para seleção de pixels com chave="*stegokey*" (Tabela 12) verificamos uma redução no MSE, e consequentemente, aumento do PSNR para a versão com chave. As distâncias Euclidiana, *Cityblock*, *Minkowski* e *Canberra*, também diminuíram favoravelmente à versão com seleção baseada em chave. Os índices Q e SSIM, seguiram o comportamento dos demais e também

apresentaram valores mais próximos de 1, indicando imagens mais fiéis, para o algoritmo LSB 4 bits com chave para seleção de pixels.

4.2.6 LSB 1 bit com criptografia

A comparação entre a imagem original e a estego-imagem gerada pela aplicação do algoritmo LSB 1 bit com criptografia AES é apresentada na Tabela 13.

Tabela 13. Análise de similaridade das imagens originais e sua respectiva modificada após aplicação do algoritmo de esteganografia LSB 1 bit com a mensagem previamente cifrada com AES.

Figura	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM	Banda	*MsgBytes*
12a	0,50	51,16	250,80	62900	39,77	17637,08	7,5e-91	0,08	0,990	R	15665
12b	0,48	51,26	244,10	59584	39,06	29882,47	9e-108	0,26	0,984	R	14922
12c	0,50	51,15	253,10	64057	40,01	30319,45	0,00573	0,54	0,987	R	16014
12d	0,49	51,22	237,59	56448	38,36	12820,76	0,00327	0,66	0,994	R	14177
12e	0,49	51,23	244,54	59801	39,10	250,37	0,00586	0,99	0,999	R	14922
12f	0,48	51,31	192,31	36985	33,32	3166,68	0,00321	0,99	0,999	R	9340
12g	0,49	51,23	169,29	28321	30,48	2068,43	0,00058	0,94	0,997	B	7060
12h	0,50	51,17	325,54	105979	47,32	7457,93	6,7e-9	0,99	0,998	B	26455
12i	0,50	51,15	351,50	123550	49,81	3956,50	0,00095	0,92	0,998	B	30880
12j	0,50	51,17	294,36	86647	44,25	7459,57	0,00066	0,99	0,998	B	21627

A única diferença entre esse algoritmo com criptografia e sua versão LSB 1 bit simples, é a prévia cifragem da mensagem utilizando o algoritmo de criptografia AES. Os resultados são muito semelhantes ao LSB 1 bit, e consequentemente, todas as comparações realizadas com o ele também são válidas para essa versão com criptografia. Por esse motivo, optamos por não realizar experimentos e comparações para todas as versões anteriores com o uso de criptografia pois os resultados obtidos pelos índices de similaridade seriam muito próximos, a ponto de considerarmos igual.

4.2.7 Outros experimentos

Foram realizados alguns outros experimentos. Dentre os quais, é válido ressaltar os resultados obtidos com a análise de similaridade mostradas na Tabela 14, Tabela 15, Tabela 16 e Tabela 17, que se encontram no Apêndice A.

Capítulo 5

Conclusão e Trabalhos Futuros

Após o desenvolvimento deste trabalho foi possível comprovar a eficácia do uso de esteganografia em imagens para transmissão de informações. As imagens geradas na realização dos experimentos apresentados no Capítulo 4 são bastante semelhantes se comparadas à “olho nu” com suas respectivas imagens originais, desde que não sejam modificados mais que 4 bits LSB.

Ressalta-se que a necessidade da imagem original se dá apenas porque este trabalho baseia-se na comparação entre ela e sua versão com uso de esteganografia. Em um uso real e efetivo de técnicas de ocultação de informação a imagem original não é enviada juntamente com a modificada e, ainda assim, o receptor poderá ter acesso à mensagem enviada.

Em relação aos atuais índices de fidelidade utilizados para análise de semelhança entre imagens, foi possível perceber que para alguns casos o cálculo do índice apresenta resultados bastante distantes do que percebemos visualmente. O índice Q, por exemplo, apresenta valores bem abaixo do esperado quando utilizado na comparação entre imagens simples (Figura 12(a), por exemplo) e sua respectiva estego-imagens.

5.1 Contribuições

Algumas contribuições do trabalho são:

- Abertura de uma nova área de atuação dentro do curso de Engenharia da Computação do Departamento de Sistemas e Computação, visto que este é o primeiro trabalho realizado nessa área. Isso possibilitará o surgimento de novos trabalhos tomando este como base.

- Proposta de uma nova forma de analisar algoritmos de esteganografia ao comparar o resultado de sua aplicação em termos de semelhança entre a imagem original e modificada. A maioria dos trabalhos existentes envolve a análise de algoritmos em termos de dificuldade de detecção da mensagem inserida. Não é de conhecimento dos autores deste trabalho nenhuma pesquisa que busque uma relação entre a estego-imagem e sua respectiva imagem original.

- Criação de uma ferramenta, *Stego Suite*, contendo as implementações aqui utilizadas e uma interface gráfica intuitiva facilitando novas pesquisas com a implementação de novos algoritmos de esteganografia e, possivelmente, de índices de fidelidade.

- Identificação de problemas envolvendo o uso do índice Q em imagens com estrutura simples e poucas cores (exemplo: Figura 12(a)). No intuito de investigar a razão do problema, foi iniciado uma longa troca de mensagens por e-mail com o criador desse índice, Dr. Zhou Wang. Segundo ele, o índice Q não funciona bem com "imagens simples" e por isso foi criado o índice SSIM. De fato, o SSIM inseriu elementos estruturais através de parâmetros como apresentado anteriormente. No entanto, esses parâmetros possuem valores definidos empiricamente. Ou seja, eles podem retornar os mesmos problemas encontrados no índice Q. Além disso, no artigo original de apresentação do índice Q, essa falha quanto a "imagens simples" não é mencionada.

- Análise da influência da informação inserida, por esteganografia, nas imagens. As estego-imagens geradas são dependentes da mensagem. Ou seja, mensagens diferentes implicam em estego-imagens distintas, embora a tendência natural é que as imagens geradas sejam semelhantes e os valores calculados com os índices de fidelidade bem próximos. Como citado na Seção 4.2.1 é possível, ainda que muito pouco provável, que uma determinada mensagem, ao ser convertida caractere a caractere para bits, possa gerar uma sequência de bits exatamente igual à presente na imagem

original. Nesse caso, a imagem original e sua versão modificada seriam idênticas.

5.2 Dificuldades encontradas

A principalmente dificuldade encontrada foi a necessidade de implementação das técnicas de esteganografia. Inicialmente, esperávamos realizar a análise utilizando implementações existentes. Embora a lista de algoritmos de esteganografia (e de ferramentas [19], inclusive) seja vasta, não existem ferramentas que permitam uma variação de parâmetros que possibilitassem a análise que desejávamos realizar.

Ressalta-se a importância da dificuldade encontrada pelo fato de que a necessidade de implementação dos algoritmos tornou possível um melhor entendimento de todo o processo de ocultação de mensagem por LSB e possibilitou a geração de um artefato a mais como contribuição: a ferramenta *Stego Suite*.

5.3 Trabalhos Futuros

Em termos de trabalhos futuros podemos citar:

- Estudo e implementação de algoritmos que envolvam a utilização de modificação no domínio da freqüência. Esses novos métodos podem ser inseridos na ferramenta desenvolvida e, dessa forma, utilizá-los em novas pesquisas.
- Desenvolver novos índices de similaridade que apresentem maior compatibilidade.
- Incluir na análise novos algoritmos como, por exemplo, o *Outguess* [26].
- Modificação do índice Q para melhorar resultados obtidos em sua utilização em imagens estruturalmente simples.

Bibliografia

[1] Anderson, R., Needham, R., Shamir, A., **The Steganographic File System**, Information Hiding International Workshop, 1998.

[2] Boncelet, C., Retter, C., **Spread Spectrum Image Steganography**, IEEE Transactions on Image Processing, 1999.

[3] Cachin, C., **Digital Steganography**, Zurich Research Laboratory, 2005.

[4] Carvalho, D., **Exploração Tecnológica para Esteganografia em Vídeos Digitais**, Trabalho de Conclusão de Curso, Instituto de Ciências Matemáticas e de Computação, USP, 2005.

[5] Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T., **Watermarking and Steganography**, 2ª Edição, 2008.

[6] Curran, K., Bailey, K., **An Evaluation of Image Based Steganography Methods**, 2003.

[7] Gomes, J., Velho, L., **Computação Gráfica: Imagem**, 2ª Edição, 2002.

[8] Hopper, N., Molnar, D., Wagner, D., **From Weak to Strong Watermarking**, Maio, 2007.

[9] Jackson, J, **Blind Steganography Detection Using Computational Immune System: A work in progress**, International Journal of Digital Evidence, 2003.

[10] Janssen, T., **Understanding image quality**, International Conference on Image Processing, 2001.

[11] Johnson, N., Jajodia, S., **Exploring Steganography, Seeing the Unseen**, IEEE Computer Magazine, Fevereiro 1998.

[12] Khan, F., Gutub, A., **Message Concealment Techniques using Image based Steganography**, Junho, 2008.

[13] Kharnazi, M., Sencar, H., **Performance Study of Common Image Steganography and Steganalysis Techniques**, Journal of Eletronic Imaging, 2006.

[14] Kobuszewski, A., **Protótipo de Software para Ocultar Textos Compactados em Arquivos de Áudio Utilizando Esteganografia**, Trabalho de Conclusão de Curso, Universidade Regional de Blumenau, 2004.

[15] Mao, W., **Modern Cryptography**, 1ª Edição, 2003.

[16] Oliveira, F., **Análise de Segurança de Criptografia e Esteganografia em Sequências de Imagens**, Dissertação de Mestrado, Laboratório Nacional de Computação Cientifica, 2007.

[17] Provos, N., Honeyman, P., **Detecting Steganographic Content on the Internet**, Center of Information Technology Integration, 2001.

[18] Provos, N., Honeyman, P., **Hide and Seek: An Introduction to Steganography**, 2003.

[19] Rocha, A., Costa, H., Chaves, L., **Camaleão: Um Software para Segurança Digital Utilizando Esteganografia**, Unicamp.

[20] Silverstein, D.A., Farrel, J.E, **The relationship between image fidelity and image quality**, International Conference on Image Processing, 1996.

[21] Smith, J., Dodge, C., **Developments in Steganography**, Outubro, 1999.

[22] Wang, Z., Bovik, A., **A Universal Image Quality Index**, IEEE Signal Processing Letters, Março 2002.

[23] Wang, Z., Bovik, A., Sheikh, H., Simoncelli, E., **Image Quality Assessment: From Error Visibility to Structural Similarity**, IEEE Transactions on Image Processing, Abril 2004.

[24] Wayner, P., **Disappearing Cryptography**, 2ª Edição, 2002.

[25] Webb, A., **Statistical Pattern Recognition**, 2ª Edição, 2002.

[26] Outguess, http://www.outguess.org, acesso em 24 de novembro de 2008.

[27] Understanding Peer-to-Peer Networking and File Sharing, http://www.limewire.com/about/p2p.php, acesso em 24 de novembro de 2008.

Apêndice A

Outros experimentos

Apresentamos aqui o resultado da análise de similaridade entre a imagem original e as imagens modificadas com os algoritmos de esteganografia desenvolvidos neste trabalho. A diferença em relação aos experimentos anteriores é que apresentamos por imagem o resultado da aplicação dos algoritmos, sendo a mensagem de igual conteúdo e tamanho para todos eles. Foram selecionadas uma imagem simples, com poucas cores (Figura 12(a)) e as três imagens mais complexas, com mais cores, do banco de imagens (Figura 12(h),(i) e (j)).

Tabela 14. Análise de similaridade entre a Figura 12(a) e sua respectiva modificada após aplicação de algoritmos LSB e mensagem de tamanho 2.035 bytes.

Algoritmo LSB	**MSE**	**PSNR**	**Euclidiana**	***Cityblock***	***Minkowski***	***Canberra***	**Angular**	**Q**	**SSIM**
1 bit simples	0,06	60,16	89,04	7928	19,94	4748,21	7,3e-91	0,89	0,998
4 bits simples	2,11	44,89	516,28	27721	143,99	3474,02	7,3e-91	0,97	0,985
8 bits simples	314,93	23,15	6308,73	238738	1950,54	2036	7,0e-91	0,98	0,989
1 bit cíclico	0,02	65,23	49,62	2462	13,50	1574,26	1,7e-83	0,89	0,999
4 bits cíclico	0,37	52,43	216,72	10319	64,68	3175,15	1,7e-83	0,97	0,992
1 bit simples salto 3	0,07	59,92	91,45	8364	20,30	2540,22	7,3e-91	0,64	0,999
4 bits simples salto 3	1,79	45,61	475,09	24715	134,84	2652,82	7,3e-91	0,92	0,974
1 bit cíclico salto 3	0,02	65,24	49,56	2456	13,49	842,28	1,7e-83	0,66	0,999
4 bits cíclico salto 3	0,36	52,61	212,31	9903	63,93	2435,23	1,7e-83	0,92	0,994
1 bit com chave *stegokey*	0,07	59,89	91,77	8422	20,35	2246,10	7,3e-91	0,58	0,999
4 bits com chave *stegokey*	1,73	45,76	467,13	24229	132,89	2508,32	7,3e-91	0,90	0,974
1 bit com criptografia (AES)	0,06	60,01	90,54	8198	20,16	5270,66	7,3e-91	0,89	0,997

Tabela 15. Análise de similaridade entre a Figura 12(h) e sua respectiva modificada após aplicação de algoritmos LSB e mensagem de tamanho 3.727 bytes

Algoritmo LSB	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM
1 bit simples	0,07	59,75	121,19	14687	24,49	649,97	6,7e-9	0,99	0,999
4 bits simples	1,43	46,58	551,90	38589	142,87	773,52	6,7e-9	0,99	0,997
8 bits simples	352,73	22,66	8671,96	449013	2424,22	2058,08	6,7e-9	0,98	0,987
1 bit cíclico	0,02	64,12	73,27	5368	17,51	218,43	4,4e-10	0,99	0,999
4 bits cíclico	0,02	54,23	228,74	13626	64,02	563,87	4,4e-10	0,99	0,999
1 bit simples salto 3	0,07	59,70	121,88	14854	24,58	1209,69	6,7e-9	0,99	0,999
4 bits simples salto 3	1,38	46,73	542,50	37908	140,39	346,31	6,7e-9	0,98	0,995
1 bit cíclico salto 3	0,02	64,34	71,43	5103	17,22	374,08	4,4e-10	0,99	0,999
4 bits cíclico salto 3	0,25	54,08	232,64	13979	64,90	234,31	4,4e-10	0,99	0,998
1 bit com chave *stegokey*	0,07	59,76	121,01	14645	24,47	1004,14	6,7e-9	0,99	0,999
4 bits com chave *stegokey*	1,39	46,69	544,67	38205	140,75	334,61	6,7e-9	0,98	0,995
1 bit com criptografia (AES)	0,07	59,65	122,52	15011	24,67	725,17	6,7e-9	0,99	0,999

Tabela 16. Análise de similaridade entre a Figura 12(i) e sua respectiva modificada após aplicação de algoritmos LSB e mensagem de tamanho 4.408 bytes

Algoritmo LSB	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM
1 bit simples	0,07	59,63	132,48	17550	25,99	39,10	9,48e-4	0,98	0,999
4 bits simples	1,36	46,79	580,54	43745	146,81	98,66	9,48e-4	0,97	0,997
8 bits simples	296,57	23,41	8570,43	476941	2351,93	1717,39	9,57e-4	0,98	0,987
1 bit cíclico	0,02	64,42	76,30	5821	17,99	22,56	3,64e-3	0,99	0,999
4 bits cíclico	0,24	54,27	245,49	16117	66,52	69,16	3,64e-3	0,99	0,999
1 bit simples salto 3	0,07	59,61	132,65	17598	26,01	401,80	9,48e-4	0,97	0,999
4 bits simples salto 3	1,27	47,08	561,81	42448	142,11	95,06	9,48e-4	0,92	0,994
1 bit cíclico salto 3	0,03	63,90	80,97	6556	18,72	92,71	3,64e-3	0,99	0,999
4 bits cíclico salto 3	0,25	54,22	246,77	16301	66,52	65,62	3,64e-3	0,98	0,998
1 bit com chave *stegokey*	0,07	59,60	132,77	17629	26,03	773,35	9,48e-4	0,97	0,999
4 bits com chave *stegokey*	1,28	47,05	563,26	42792	142,20	95,63	9,48e-4	0,91	0,994
1 bit com criptografia (AES)	0,07	59,62	132,63	17591	26,01	39,17	9,48e-4	0,98	0,999

Tabela 17. Análise de similaridade entre a Figura 12(j) e sua respectiva modificada após aplicação de algoritmos LSB e mensagem de tamanho 3.043 bytes

Algoritmo LSB	MSE	PSNR	Euclidiana	*Cityblock*	*Minkowski*	*Canberra*	Angular	Q	SSIM
1 bit simples	0,07	59,68	110,41	12191	23,01	228,78	6,5e-4	0,99	0,999
4 bits simples	1,42	46,60	497,92	31696	132,59	108,99	6,5e-4	0,98	0,998
8 bits simples	202,45	25,07	5940,74	267331	1766,34	1103,16	6,66e-4	0,98	0,991
1 bit cíclico	0,02	64,48	63,58	4042	15,93	13,86	4,26e-3	0,99	0,999
4 bits cíclico	0,24	54,26	206,00	11422	58,97	32,77	4,26e-3	0,99	0,999
1 bit simples salto 3	0,07	59,66	110,73	12262	23,06	572,55	6,5e-4	0,99	0,999
4 bits simples salto 3	1,44	46,55	501,11	31806	133,61	216,41	6,5e-4	0,96	0,995
1 bit cíclico salto 3	0,02	64,35	64,50	4160	16,08	38,28	4,26e-3	0,99	0,999
4 bits cíclico salto 3	0,24	54,28	205,76	11327	59,26	34,75	4,26e-3	0,98	0,999
1 bit com chave *stegokey*	0,07	59,67	110,54	12219	23,03	651,62	6,5e-4	0,99	0,999
4 bits com chave *stegokey*	1,42	46,61	497,31	31584	132,57	242,30	6,5e-4	0,96	0,995
1 bit com criptografia (AES)	0,07	59,68	110,40	12188	23,01	242,04	6,5e-4	0,99	0,999