

Análise Objetiva do Número de *Bits* Menos Significativos em Esteganografia de Imagens Digitais

Geoffly L. Adonias¹, Ewerton S. Farias¹, Wesley C. Santos¹, Carlos Danilo M. Regis¹

¹Departamento de Engenharia Elétrica
Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB)
João Pessoa – PB – Brazil

gadonias7@gmail.com, ewerton.farias.ee@gmail.com,
weslleyfera@gmail.com, danilo.regis@ifpb.edu.br

Abstract. *Steganography is the science and art of hiding the existence of a message between a sender and an intended recipient. The usual least significant bit (LSB) technique works fine when it comes to settling the quality of the carrier file, but it lacks the ability to carry a lot of characters. In this paper, the number of LSB is incremented up to 5 bits, which increases its capacity to hide more text and, as a result, the quality is overly affected. The carrier receives a message at its maximum capacity and, later, the encoded image is submitted to PSNR, SSIM and PW-SSIM quality tests. Finally, it is concluded that the higher the spatial information the lower the degradation of the carrier.*

Resumo. *Esteganografia é a ciência e arte de ocultar a existência de uma mensagem entre um remetente e um destinatário desejado. A técnica usual de bit menos significativo (LSB) funciona bem quando se trata em manter a qualidade do arquivo da portadora, mas ela falha em transportar muitos caracteres. Neste artigo, o número de LSB é incrementado em até 5 bits, o que aumenta sua capacidade de ocultar mais texto e, conseqüentemente, a qualidade é demasiadamente afetada. A portadora recebe uma mensagem em sua capacidade máxima e, posteriormente, a imagem codificada é submetida a testes de qualidade utilizando as métricas PSNR, SSIM e PW-SSIM. Finalmente, conclui-se que quanto maior a informação espacial menor a degradação da portadora.*

1. Introdução

Ao longo das últimas duas décadas, o rápido desenvolvimento da internet exige que informações confidenciais sejam protegidas contra acessos não autorizados. Isto é realizado através de diversas formas, e uma delas é a esteganografia. O termo esteganografia tem origem das palavras gregas *stegos* que significa *esconder* e *grafia* que significa *escrita* definindo-a como a arte da *escrita escondida* [Poornima and Iswarya 2013]. Esta é uma ciência, técnica e arte de ocultar ou inserir informações ou mensagens em um meio que possua significado próprio (portadora) de modo que um observador não estará ciente da existência de informações ocultas [Jasril et al. 2012].

Existem diferentes tipos de esteganografia:

1. Esteganografia de Texto: Técnica não muito utilizada porque arquivos de texto possuem pequenas quantidades de dados redundantes;

2. Esteganografia de Imagem: Esta técnica é amplamente utilizada pela capacidade de receber muita informação a um baixíssimo nível de degradação da portadora;
3. Esteganografia de Áudio/Vídeo: Comparada aos anteriores, esta é uma técnica muito complexa de ser aplicada [Thangadurai and Devi 2014].

A esteganografia e a criptografia se assemelham no fato de que ambas são utilizadas para esconder informações [Poornima and Iswarya 2013], e diferem entre si de acordo com a comparação ilustrada na Tabela 1 [Thangadurai and Devi 2014].

Tabela 1. Comparação entre Criptografia e Esteganografia.

Criptografia	Esteganografia
Há conhecimento sobre a transmissão de informações	Não há conhecimento sobre a transmissão de informações
Encriptação previne que pessoas não autorizadas revelem o conteúdo da comunicação	Esteganografia previne a descoberta da existência de comunicação
Tecnologia comum	Tecnologia pouco conhecida
Criptografia altera a estrutura da informação	Esteganografia não altera a estrutura da informação

A técnica do *Bit Menos Significativo* (em inglês, *Least Significant Bit – LSB*) é comumente utilizada em esteganografia para inserir e extrair a informação da portadora. De modo geral, este método é baseado na substituição dos *bits* menos significativos da portadora pelos *bits* da informação confidencial [Poornima and Iswarya 2013].

Na literatura, é possível encontrar análises de esteganografia em que é utilizado mais de um *bit* menos significativo. Em [Ker 2007], o autor investiga como detectores de padrão de substituição LSB podem ser adaptados para uma abordagem com dois *bits*. Já em [Jasril et al. 2012], é possível verificar a modificação de quatro *bits*, também utilizando a técnica LSB, em portadoras no formato *Bitmap* (BMP) e *Wave* (WAV) e a análise realizada com a métrica *Peak Signal-to-Noise Ratio* (PSNR). Recentemente, foram desempenhadas análises utilizando o *Root-Mean-Square Error* (RMSE) e a PSNR para esteganografia de imagens coloridas com a codificação de dois a seis *bits* menos significativos [Thakur and Saravanan 2016].

O objetivo deste trabalho é de propor uma avaliação objetiva da modificação de até cinco *bits* menos significativos de uma imagem (portadora) para a inserção de informações (caracteres). O código-fonte deste trabalho está disponível para livre uso sob a *MIT License*¹. A avaliação da qualidade e performance do algoritmo é desempenhada com o uso das métricas PSNR, *Structural Similarity Index* (SSIM) e *Structural Similarity Index with Perceptual Weighting* (PW-SSIM), verificando sua degradação de acordo com seu nível de informação espacial (em inglês, *Spatial Information – SI*), onde se espera que o valor de SI influencie na qualidade da imagem codificada.

¹Disponível em: <https://github.com/gladonias/LSB-Image-Steganography.git>.

2. Referencial Teórico

2.1. Bit Menos Significativo (LSB)

Arquivos digitais são formados por sequências de números binários em que todos os valores possíveis são representados com base em dois números, zero (0) e um (1). Frequentemente, nos referimos a ambos os números como *bits*.

Os *bits* da informação binária são classificados com base na sequência e em sua influência e, são divididos em dois grupos, os *bits* mais significativos (em inglês, *Most Significant Bit* – MSB) e os *bits* menos significativos (LSB), como mostra a Figura 1 [Jasril et al. 2012].

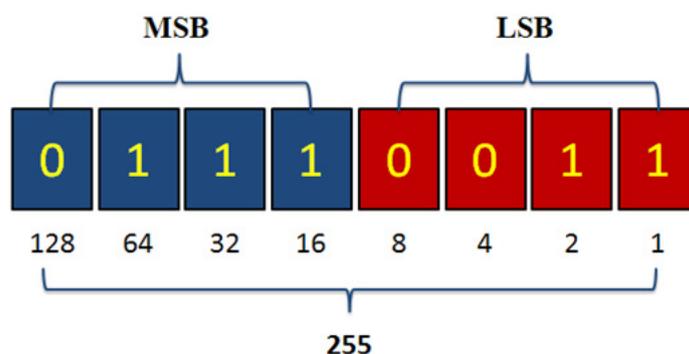


Figura 1. Representação binária [Jasril et al. 2012].

O MSB é a representação dos quatro *bits* que tem maior influência na informação, isso significa que mudanças drásticas ocorreriam se esses *bits* fossem modificados. Enquanto que o LSB é a representação dos quatro *bits* menos influenciáveis quando modificados e não representam uma mudança drástica na informação da portadora [Jasril et al. 2012].

Quando se substitui um LSB, um valor par pode ser incrementado ou inalterado, porém nunca decrementado (LSB é zero); o mesmo acontece de forma inversa para valores ímpares (LSB é um). Nesta propriedade, quando os *pixels* são considerados individualmente, o poder de detecção se torna ineficiente, porém, quando nesta mesma propriedade são considerados pares de *pixels*, os detectores são mais sensíveis até mesmo a presença de pequenas quantidades de dados ocultos pela técnica LSB [Ker 2007]. Na Tabela 2, é possível verificar para uma sequência de quatro *bits*, os valores em que o LSB é 1 e que o LSB é 0.

Pode-se deduzir que a capacidade da portadora em função das dimensões da imagem (em *pixels*) e do número de *bits* menos significativos, é calculada por

$$NC = \frac{W \cdot H \cdot N_{LSB}}{2}, \quad (1)$$

em que NC é o número de caracteres que a portadora suporta, W e H são as dimensões da imagem (em *pixels*) e N_{LSB} é o número de *bits* menos significativos a serem codificados.

Nota-se que, a quantidade de informação a ser codificada é diretamente proporcional à capacidade da portadora; também é importante considerar que o método LSB não

Tabela 2. Sequências de Bits em que o LSB é um e que o LSB é zero.

Sequência em que o LSB é 1	Sequência em que o LSB é 0
0 0 0 1	0 0 0 0
0 0 1 1	0 0 1 0
0 1 0 1	0 1 0 0
0 1 1 1	0 1 1 0
1 0 0 1	1 0 0 0
1 0 1 1	1 0 1 0
1 1 0 1	1 1 0 0
1 1 1 1	1 1 1 0

criptografa a mensagem, apenas a oculta.

Além de fácil implementação, o método LSB é menos suspeito aos olhos humanos por não haver conhecimento sobre a transmissão de informações, e muitas técnicas fazem uso desse método. Por outro lado, o LSB é extremamente sensível a qualquer tipo de filtragem, e quando submetido a edições como escalonamento, rotação, corte e adição de ruído extra, a informação oculta pode ser destruída [Poornima and Iswarya 2013].

2.2. Spatial Information (SI)

SI indica o nível de detalhes espaciais percebido por um observador humano em uma imagem. Esta métrica vem sendo comumente usada para estimar a complexidade de uma imagem. Quanto mais complexa for a imagem, maior será a quantidade de informação espacial [Yu and Winkler 2013, Regis 2013].

Essa estimativa é realizada apenas na imagem original por meio da aplicação dos gradientes de *Sobel* horizontal e vertical, que é definido pelas seguintes máscaras [Yu and Winkler 2013, Regis 2013]:

$$\begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} \quad \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} \quad (2)$$

A aplicação do operador de *Sobel* resulta numa imagem $G = g(x, y)$ que contém as bordas dos objetos de uma imagem $F = f(x, y)$ e indica a quantidade de informação espacial presente na imagem; as bordas definem um limite entre duas regiões na imagem com níveis de cinza relativamente distintos [Regis 2013].

Sejam G_x e G_y as imagens que contenham as bordas nos sentidos horizontal e vertical, respectivamente. A magnitude de informação espacial em cada *pixel* é definida por [Yu and Winkler 2013]:

$$SI_g = \sqrt{G_x^2 + G_y^2} \quad (3)$$

As medidas de SI mais comumente utilizadas para caracterizar a complexidade de uma imagem são a média (*mean*), o valor quadrático médio (*rms*) e o desvio padrão

(*stddev*) dos valores de SI_g em todos os *pixels* da imagem [Yu and Winkler 2013]. Essas medidas são expressas matematicamente como:

$$SI_{mean} = \frac{1}{P} \sum SI_g, \quad (4)$$

$$SI_{rms} = \sqrt{\frac{1}{P} \sum SI_g^2}, \quad (5)$$

$$SI_{stddev} = \sqrt{\frac{1}{P} \sum SI_g^2 - SI_{mean}^2}, \quad (6)$$

em que P é o número de *pixels* da imagem.

2.3. Peak Signal-to-Noise Ratio (PSNR)

A PSNR e o *Mean Square Error* (MSE) são os parâmetros mais comumente utilizados para medir a qualidade entre duas imagens submetidas ao processo de esteganografia. O PSNR indica a semelhança entre duas imagens e é recíproco ao MSE (matematicamente, o PSNR é uma representação logarítmica do MSE) [Joshi et al. 2016, Regis et al. 2015].

O MSE é calculado a partir do valor médio dos erros quadráticos entre os *pixels* da imagem original e da imagem esteganografada, sendo definido como [Regis et al. 2015]

$$MSE(f, h) = \frac{1}{R \cdot C} \sum_{x=1}^C \sum_{y=1}^R (f(x, y) - h(x, y))^2, \quad (7)$$

em que R é o número total de linhas, C é o número total de colunas e, $f(x, y)$ e $h(x, y)$ são os níveis de intensidade de luminância em que x e y representam as coordenadas espaciais de um *pixel*. Quanto melhor a qualidade da imagem avaliada em relação a original, menor é o valor do MSE [Regis et al. 2015].

A PSNR, por sua vez, é medida em decibéis (dB), é inversamente proporcional ao MSE e é definida como [Joshi et al. 2016]

$$PSNR = 10 \cdot \log_{10} \left[\frac{MAX^2}{MSE(f, h)} \right] dB, \quad (8)$$

em que $MAX = 2^b - 1$ é o valor máximo da escala de níveis de cinza construída com b *bits*. Quanto maior o valor da PSNR, maior é a semelhança entre a imagem original e a imagem esteganografada.

Sua popularidade se dá devido a facilidade de implementação e rapidez no processamento, porém, a PSNR se baseia em uma comparação *byte a byte* dos dados, desconsiderando o que eles realmente representam [Regis et al. 2015].

2.4. Structural Similarity Index (SSIM)

O SSIM é uma métrica que utiliza a estatística da imagem para avaliação da qualidade, é construído como um modelo multiplicativo que é constituído de atributos da semelhança estrutural e de informações da luminância e contraste da imagem [Regis et al. 2015, Bae and Kim 2015].

Sejam dois sinais representados por $f = \{f_i | i = 1, 2, \dots, P\}$ e $h = \{h_i | i = 1, 2, \dots, P\}$, sendo f a imagem original e h a imagem esteganografada, define-se SSIM como

$$SSIM(f, h) = l(f, h)^\alpha \cdot c(f, h)^\beta \cdot s(f, h)^\gamma \quad (9)$$

em que $l(\cdot)$, $c(\cdot)$ e $s(\cdot)$, indicam luminância, contraste e atributos de semelhança estrutural [Bae and Kim 2015], respectivamente, e os expoentes α , β e γ são parâmetros utilizados para ajustar a importância de cada atributo e, para efeitos de simplificação, são considerados iguais a 1 [Regis et al. 2015].

A luminância mede a intensidade média de cada *pixel* (μ) entre f e h [Bae and Kim 2015], e é calculada por

$$l(f, h) = \frac{2\mu_f\mu_h + K_1}{\mu_f^2 + \mu_h^2 + K_1} \quad (10)$$

em que a constante K_1 é inserida para evitar instabilidade nos valores como, por exemplo, se o denominador tiver um valor próximo de zero [Bae and Kim 2015, Regis et al. 2015].

Analogamente, a análise do contraste é dada por

$$c(f, h) = \frac{2\theta_f\theta_h + K_2}{\theta_f^2 + \theta_h^2 + K_2} \quad (11)$$

em que θ é o desvio padrão.

Por fim, a análise entre as estruturas é dada por

$$s(f, h) = \frac{2\theta_{fh} + K_3}{\theta_f + \theta_h + K_3} \quad (12)$$

assim como K_1 , as constantes K_2 e K_3 são inseridas para evitar instabilidade nos valores.

A técnica SSIM é utilizada para encontrar artefatos em imagens desde que haja outra imagem considerada como referência [Regis et al. 2015, Farias et al. 2014]. Em comparação com a PSNR (Subseção 2.3) que estima apenas erros absolutos, o SSIM considera a degradação da imagem como uma alteração na informação estrutural [Wang et al. 2004].

2.5. Structural Similarity Index with Perceptual Weighting (PW-SSIM)

Modelos como os mapas de saliência, foco visual e as regiões de interesse, que utilizam métodos de atenção visual em métricas de qualidade de imagem têm sido propostos.

O PW-SSIM usa a ponderação para avaliar a qualidade da imagem dando maior ênfase às regiões visualmente mais importantes [Adonias et al. 2016].

Esta ponderação é calculada da seguinte forma: primeiramente, se calcula a magnitude dos vetores de gradiente na imagem original, por meio das máscaras de *Sobel*, depois é gerado um quadro no qual os valores dos *pixels* são as magnitudes dos gradientes. Em seguida esse quadro é particionado em blocos de 8×8 *pixels* e para cada bloco é calculado o SI [Regis et al. 2015].

Baseado nesta consideração, o valor do SI (Equação 6) foi incorporado ao SSIM levando ao modelo denominado *Structural Similarity Index with Perceptual Weighting* (PW-SSIM) [Regis et al. 2015, Adonias et al. 2016], e é definido como

$$PWSSIM(f, h) = \frac{\sum_{i=1}^B SSIM_i(f, h) \cdot SI_i}{\sum_{i=1}^B SI_i} \quad (13)$$

em que B é a quantidade de blocos na imagem, f é a imagem original e h é a imagem esteganografada. O SI é calculado apenas para a imagem original, considerando que este é o melhor valor, desta forma, sendo o melhor valor para ponderação [Regis et al. 2015, Adonias et al. 2016]. Imagens que possuem valor de SI igual a zero, não retornam valores de PW-SSIM.

3. Metodologia

Neste trabalho foram utilizadas imagens coloridas com dimensões de 128×128 *pixels*, no formato PNG (*Portable Network Graphics*). Independente do esquema de cores, a imagem é submetida a um processo de conversão para o esquema cores RGB (*Red, Green e Blue*) com canal A (*alpha*) ativo. Essa conversão é realizada para garantir o espaço disponível na portadora de acordo com o número de *bits* menos significativos e evitar que informações sejam perdidas.

O esquema de cores RGBA é uma extensão do esquema RGB com um canal *alpha* que especifica a opacidade de uma cor. Os parâmetros são especificados da forma (R, G, B, A) em que os parâmetros R, G e B variam de 0 a 255 e o parâmetro A varia de 0,0 a 1,0.

Os textos foram gerados utilizando o *Blind Text Generator*². As quantidades de caracteres dos textos foram calculadas (Equação 1) de modo a ocupar todo o espaço disponível na imagem de acordo com o número de *bits* menos significativos indicado pelo usuário. As codificações foram realizadas variando o número de *bits* de 1 a 5 (Tabela 3).

Um *pixel* é composto pelos elementos R, G, B e A, cada um desses elementos possuem oito *bits* (totalizando 32 *bits* por *pixel*). Na Figura 2, é possível verificar o esquema de codificação com apenas um *bit* menos significativo. Um caractere possui oito *bits*, cada um desses *bits* é inserido nos parâmetros R, G, B e A, desta forma, para um *bit* menos significativo, serão utilizados dois *pixels* para comportar um caractere.

²Disponível em: <http://www.blindtextgenerator.com/lorem-ipsu>. Acesso em 16 de outubro de 2017.

Tabela 3. Relação Entre o Número de LSB e a Capacidade da Portadora.

Número de LSB	Capacidade da Portadora (caracteres)
1	8.192
2	16.384
3	24.576
4	32.768
5	40.960

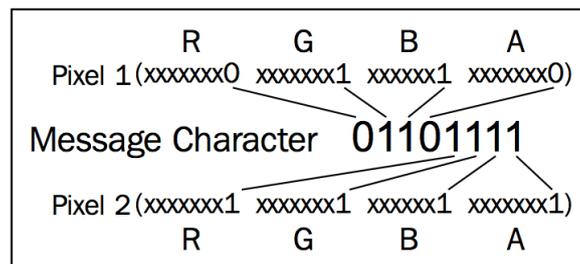


Figura 2. Esquema de inserção da mensagem na portadora (1 bit) [Buchanan et al. 2015].

O algoritmo desenvolvido na linguagem de programação *Python*, funciona da seguinte forma: primeiramente, indica-se a imagem (portadora), a mensagem, o nome do arquivo de saída e o número de *bits* menos significativos a serem alocados para a inserção da mensagem, depois a imagem é convertida para o esquema de cores RGBA, com isso, a imagem começa a receber a mensagem *bit a bit* e, por fim, a nova imagem é exportada para o mesmo formato.

O funcionamento do algoritmo descrito anteriormente, está ilustrado no fluxograma da Figura 3.

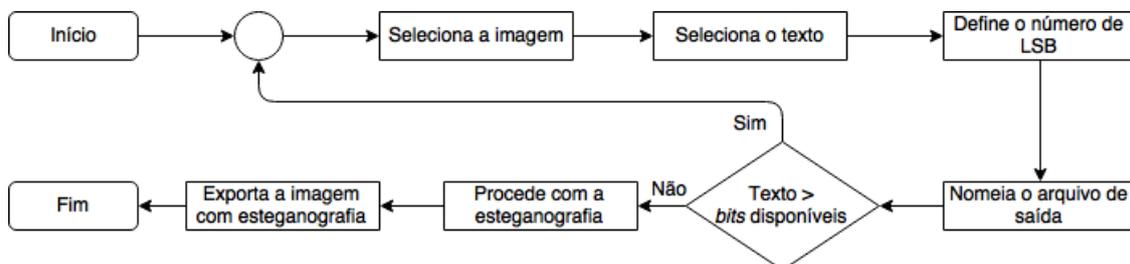


Figura 3. Fluxograma do algoritmo de esteganografia.

As imagens foram selecionadas por meio do serviço de pesquisa *Google Images*TM. A Figura 4(a) foi escolhida propositalmente para que pudéssemos avaliar o desempenho do algoritmo em uma imagem que não possui informação espacial, ou seja, seu valor de SI é zero. As demais imagens foram escolhidas aleatoriamente e ordenadas alfabeticamente, como pode-se verificar na Tabela 4.

Essas imagens estão ilustradas na Figura 4.

Tabela 4. Valores de SI de Cada Imagem Submetida a Esteganografia.

Imagem	SI_{mean}	SI_{rms}	SI_{stddev}	Imagem	SI_{mean}	SI_{rms}	SI_{stddev}
Black	0	0	0	Flowers	118.48	176.2	130.42
Blonde	133.5	190.32	135.64	Lights	69.13	131.2	111.51
Bubble	91.37	131.88	95.1	Pencils	155.44	212.15	144.39
Buildings	118.11	184.2	141.35	Pillows	65.69	96.46	70.64
Butterfly	175.24	245.24	171.56	Rainbow	61.09	151.41	138.53
Candy	94.57	153.13	120.44	Sky	47.06	76.43	60.23
Car	89.38	159.52	132.12	Sunrise	52.67	90.96	74.16
Castle	73.85	132.15	109.59	Tree	155.4	201.46	128.21
Cat	91.54	154.96	125.03	Wave	109.33	147.35	98.79
Dog	105.57	150.81	107.7	Woman	58.48	87.45	65.02

4. Resultados

Na Figura 5, é possível verificar um exemplo da degradação da imagem durante o processo. A imagem original (Figura 5(a)) é submetida ao processo de esteganografia variando o número de *bits* menos significativos e a quantidade de caracteres a ser inserida na imagem conforme descrito na Tabela 3.

A Figura 5(b) mostra o resultado da esteganografia com um *bit* menos significativo, em que a imagem carrega exatamente 8.192 caracteres. Nas Figuras 5(c), 5(d), 5(e) e 5(f), as imagens foram codificadas com dois, três, quatro e cinco *bits* menos significativos, respectivamente, e carregam 16.384, 24.576, 32.768 e 40.960 caracteres, respectivamente.

A PSNR e a SSIM foi aplicada em todas as imagens da Figura 4. Nas Figuras 5(b) a 5(f), é possível verificar visualmente como a qualidade é degradada conforme aumentamos o número de *bits* menos significativos. A Figura 6(a) mostra a avaliação da PSNR, em que é perceptível uma diferença entre a Figura 4(a), que possui valor de SI nulo, e as demais imagens.

Nas Figuras 6(b) e 6(c), o SSIM e o PWSSIM mostram uma tendência na qual as imagens com maiores valores de SI sofrem uma menor degradação com o aumento do número de *bits* menos significativos no processo de esteganografia.

Conforme discutido anteriormente, a PW-SSIM apresenta melhores resultados em comparação de qualidade por se tratar de um método que enfatiza as regiões visualmente mais importantes.

A Figura 4(a) não aparece nos resultados do PW-SSIM, pois se trata de uma imagem com valor de SI nulo e, pelo fato de que a métrica utiliza esse valor como divisor (Equação 13), a PW-SSIM retorna *NaN* (*Not a Number*). Desta forma, estaremos avaliando apenas as Figuras 4(b) a 4(t).

Constata-se também que imagens com maior valor de SI, são menos afetadas na qualidade conforme elas são submetidas a esteganografia com maiores números de *bits* menos significativos.

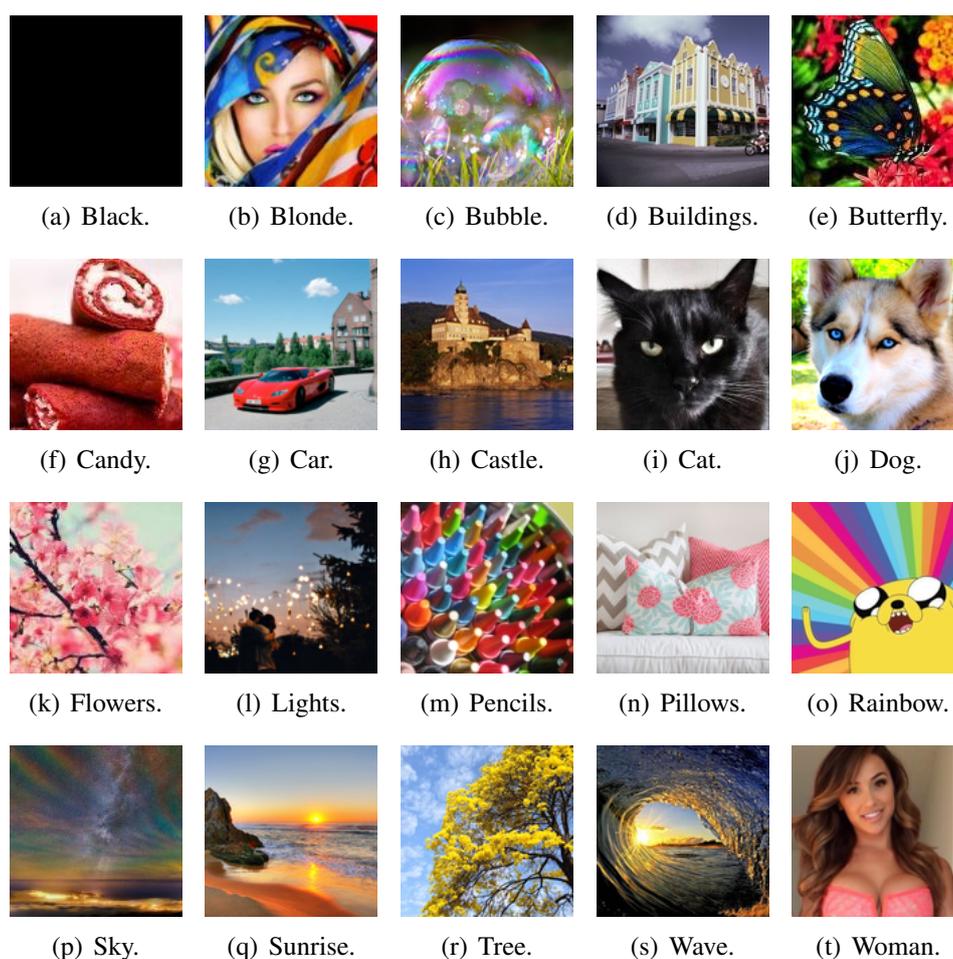


Figura 4. Imagens utilizadas no processo de esteganografia.

5. Conclusão

Devido ao aumento do número de dispositivos conectados à rede mundial de computadores, roubos de informações sigilosas e invasões de privacidade se tornaram mais frequentes. A esteganografia ajuda a minimizar esse problema fazendo com que, ao contrário da criptografia, uma mensagem possa ser transmitida sem que sua existência seja percebida ou conhecida.

O método descrito neste trabalho mostrou que, com o aumento do número de *bits* menos significativos em imagens com diferentes valores de informação espacial, se cria uma tendência em que imagens com maiores valores de SI sofrem uma menor degradação conforme se aumenta o número de LSB. Esses resultados podem ser visualmente constatados na Figura 5 e matematicamente verificados nos gráficos da Figura 6.

A fim de manter um nível de qualidade aceitável e relativamente imperceptível à visão humana, recomendamos o uso de até três *bits* menos significativos para a inserção de informação na portadora (imagem). Porém, na Figura 6(c) é possível verificar que para alto valores de SI, é possível utilizar até quatro *bits* menos significativos, pois obteve-se um valor de semelhança superior a 98%, como foi o caso da Figura 4(e).

A maior contribuição desta ferramenta é sua fácil implementação, até mesmo por

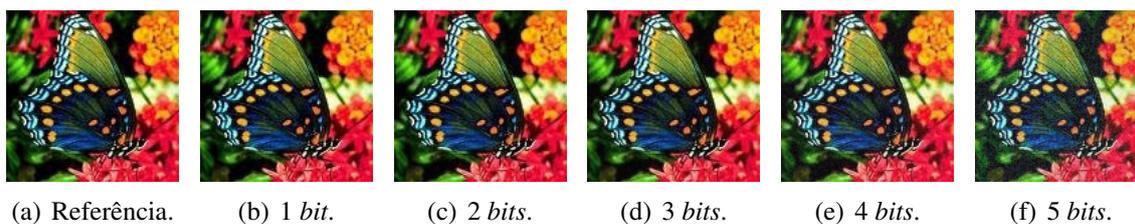
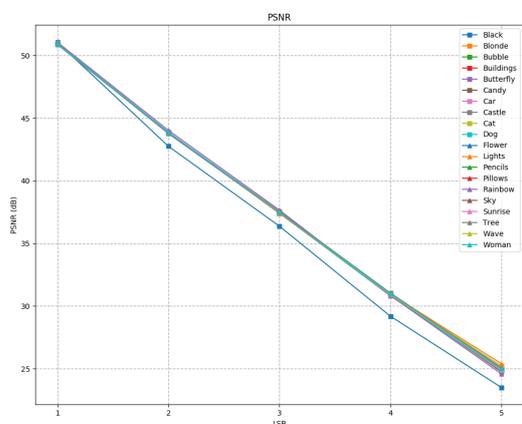
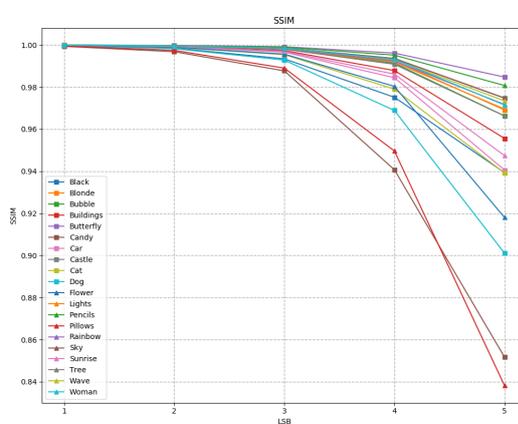


Figura 5. Mosaico do processo de esteganografia conforme aumento de LSB.

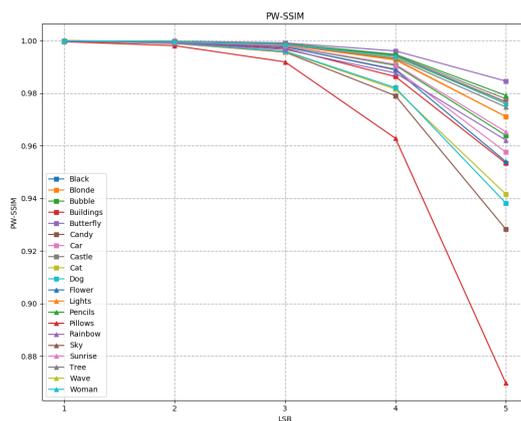
usuários com pouco conhecimento técnico, possibilitando o transporte de informações confidenciais por canais ou ambientes não seguros.



(a) Gráfico da PSNR da esteganografiadas imagens da Figura 4.



(b) Gráfico da SSIM da esteganografiadas imagens da Figura 4.



(c) Gráfico da PW-SSIM da esteganografia das imagens da Figura 4 (exceto a Figura 4(a)).

Figura 6. Gráficos dos resultados da PSNR, SSIM e PW-SSIM.

Para trabalhos futuros, seria ideal a codificação de um maior número de imagens para que se possa obter análises estatísticas precisas que avaliem o grau de degradação das portadoras em relação à sua informação espacial.

Referências

- Adonias, G. L., Oliveira, J. F. F., Regis, C. D. M., and Alencar, M. S. (2016). Avaliação da Qualidade usando PW-SSIM para vídeos codificados pelo HEVC e H.264. In *XXXIV Brazilian Telecommunications and Signal Processing Symposium (SBrT)*, pages 773–774.
- Bae, S. H. and Kim, M. (2015). A novel SSIM index for image quality assessment using a new luminance adaptation effect model in pixel intensity domain. In *2015 Visual Communications and Image Processing (VCIP)*, pages 1–4.
- Buchanan, C., Ip, T., Mabbitt, A., May, B., and Mound, D. (2015). *Python Web Penetration Testing Cookbook*. Packt Publishing.
- Farias, E. S., Adonias, G. L., and Regis, C. D. M. (2014). Análise de Similaridade Estrutural de Imagens Esteganografadas com Python. In *Encontro Anual do IECOM em Comunicações Redes e Criptografia (ENCOM)*.
- Jasril, Marzuki, I., and Rahmat, F. (2012). Modification Four Bits of Uncompressed Steganography using Least Significant Bit (LSB) Method. In *2012 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, pages 287–292.
- Joshi, K., Yadav, R., and Allwadhhi, S. (2016). PSNR and MSE based investigation of LSB. In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, pages 280–285.
- Ker, A. D. (2007). Steganalysis of Embedding in Two Least-Significant Bits. *IEEE Transactions on Information Forensics and Security*, 2(1):46–54.
- Poornima, R. and Iswarya, R. J. (2013). An Overview of Digital Image Steganography. *International Journal of Computer Science and Engineering Survey (IJCSSES)*, 4(1):23–30.
- Regis, C. D. M. (2013). *Métrica de Avaliação Objetiva de Vídeo Usando a Informação Espacial, a Temporal e a Disparidade*. PhD thesis, Universidade Federal de Campina Grande.
- Regis, C. D. M., Oliveira, I. P., Cardoso, J. V. M., and Alencar, M. S. (2015). Design of Objective Video Quality Metrics Using Spatial and Temporal Informations. *IEEE Latin America Transactions*, 13(3):790–795.
- Thakur, R. K. and Saravanan, C. (2016). Analysis of steganography with various bits of LSB for color images. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pages 2154–2158.
- Thangadurai, K. and Devi, G. S. (2014). An analysis of LSB based image steganography techniques. In *2014 International Conference on Computer Communication and Informatics*, pages 1–4.
- Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4):600–612.
- Yu, H. and Winkler, S. (2013). Image complexity and spatial information. In *2013 Fifth International Workshop on Quality of Multimedia Experience (QoMEX)*, pages 12–17.