Estudo Comparativo e Implementação de Técnicas Esteganográficas para Ocultamento de Informações

Wellington D. Almeida[1], Polycarpo S. Neto[2] e Francisco J. A. Aquino[3]
[1,3]Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE), Fortaleza, CE
[2]Universidade Federal do Ceará (UFC), Fortaleza, CE
e-mails: {wellingtondantas39, policarponeto.pn}@gmail.com e fcoalves_aq@ifce.edu.br

***Resumo*— Um importante fator para proteger os dados que trafegam pelos sistemas de comunicações não seguros é a inclusão de técnicas criptológicas. Assim, o estudo de esteganografia ganhou notoriedade para o setor de multimídia, pois permite identificar a propriedade intelectual da obra, diminuir a falsificação e reprodução indevida. A esteganografia também pode ser usada para desenvolver aplicações para comunicações sigilosas entre organizações militares. Neste contexto, este artigo apresenta a implementação e um estudo comparativo de duas das técnicas esteganográficas: a transformada discreta do cosseno e a dos bits menos significativos, que são aplicadas no ocultamento de informações.**

Palavras-chave*— *Esteganografia, Bits menos significativos, Identificação de autoria, Transformada discreta do cosseno.

I. INTRODUÇÃO

O uso dos meios de comunicações digitais, mais notadamente da *internet*, cresceu na mesma proporção que os casos de arquivos de dados copiados e adulterados para fins de violação dos direitos autorais, sem o devido conhecimento do proprietário do arquivo. Com isso, surgiu a necessidade de esconder uma identificação secreta [1] que possa ser uma aliada para provar a propriedade de direitos de autor.

Técnicas para a ocultação de informações são utilizadas desde a antiguidade [2]. No entanto, com o surgimento de materiais digitalizados, como arquivos de imagem, áudio e vídeo, a necessidade de desenvolver formas de proteção do conteúdo por meio de técnicas digitais ficou evidente. Técnicas de criptografia e esteganografia vêm trazendo resultados positivos, principalmente porque são muitas as pesquisas que desenvolvem novas formas para tornar a troca de dados mais segura por meio da confidencialidade, integridade e disponibilidade [3].

Os termos criptografia e esteganografia são dois ramos da criptologia. A criptografia significa em grego "escrita cifrada", ou seja, é o estudo de técnicas que transformam uma escrita original para outra ilegível. Por outro lado, esteganografia significa "escrita escondida", ou seja, é a arte de esconder uma informação de forma que não possa ser possível identificar o conteúdo da mensagem escondida [4]. A vantagem da esteganografia é que suas informações secretas não atraem a atenção de ninguém, diferente da criptografia, que mesmo que seja muito difícil decifrar o código cifrado, sempre chama a atenção de todos. A história da criptologia mostra que a maioria dos sistemas de criptografia desenvolvidos foram quebrados [5]. Porém, com a união das técnicas de criptografia e esteganografia, tem-se obtido mais segurança.

Recebido em abril de 2017. Aceito em agosto de 2017

Um dos principais objetivos da esteganografia é de esconder dados que possam ser transmitidos de forma segura em um meio digital hospedeiro, conhecido como cobertura (em inglês, "*cover*"), completamente indetectável, de tal maneira que ninguém possa desconfiar que exista alguma informação secreta inserida nesse meio hospedeiro. Uma das principais ações da esteganografia é o armazenamento da informação secreta no arquivo hospedeiro, que pode ser em arquivos de texto, áudio, imagem ou em vídeo [1].

O restante do artigo está dividido como segue. Na Seção II é apresentado um breve resumo sobre a esteganografia e as suas subáreas. A Seção III apresenta um estudo resumido e a aplicabilidade das técnicas esteganográficas mais estudadas e utilizadas atualmente. Na Seção IV é apresentada uma metodologia mais complexa de como ocultar informações secretas utilizando os bits menos significativos e a transformada discreta do cosseno. A Seção V apresenta os resultados e discussões das simulações realizadas utilizando os dois métodos. Por fim, a Seção VI expõe as conclusões.

II. ESTEGANOGRAFIA

As técnicas esteganográficas têm sido usadas desde a Grécia antiga, quando informações eram enviadas na pele de escravos para um destinatário apropriado que conhecia a forma de esconder a informação [6]. Porém os meios para esconder dados secretos atualmente são diferentes de antigamente, pelo fato de atualmente serem empregados em meios digitais.

Como mencionado, com a esteganografia é possível ocultar informações sigilosas em meios hospedeiros, assim como também é possível a recuperação dessas informações com a técnica inversa. A figura 1 apresenta etapas para ocultamento e extração de dados.

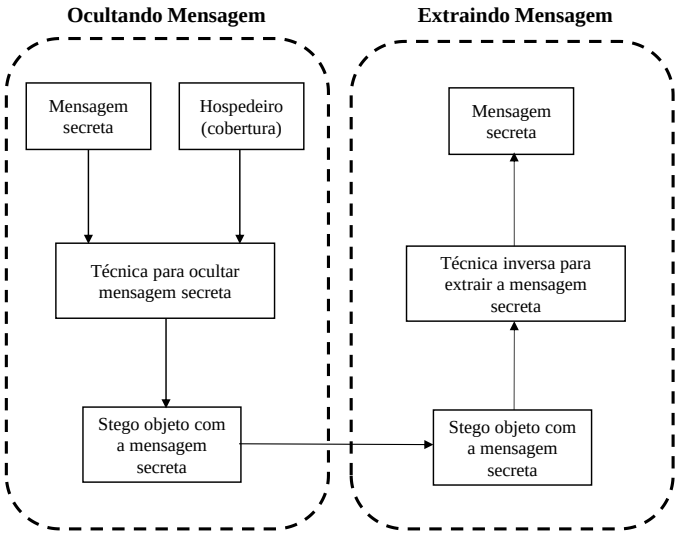

Figura 1. Etapas para ocultar e extrair informações secretas em meios hospedeiros utilizando esteganografia.

A esteganografia possui várias técnicas para ocultamento de informações secretas. Determinadas técnicas se enquadram em meios hospedeiros específicos, assim como podem ser trabalhadas no domínio espacial ou no domínio de frequência, e possuem algumas vantagens e desvantagens em relação à segurança, recorte e compressão.

Na Figura 2 é apresentada a classificação de acordo com o tipo de domínio das técnicas e os meios de cobertura que podem abrigar uma informação secreta.

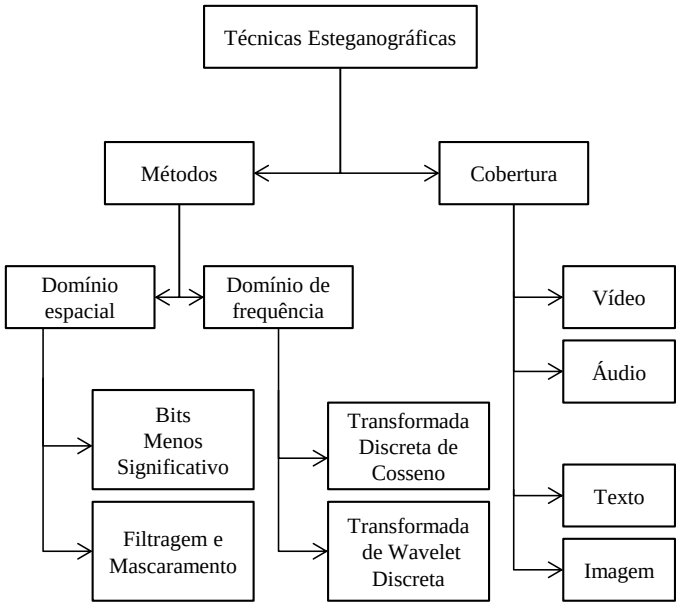

Figura 2. Classificação com alguns tipos de técnicas da esteganografia e os meios hospedeiros.

III. Técnicas Esteganográficas

A. *Transformada Discreta de Cosseno*

A Transformada Discreta do Cosseno, (abreviado em inglês, DCT) usa funções matemáticas baseadas em cosseno, para transformar a imagem do domínio espacial para o domínio de frequência [7]. Isto é, separa a imagem em sub-bandas espectrais no que diz respeito à sua qualidade visual, em componentes de alta, média e baixa frequência [8].

As partes visíveis mais importantes da imagem se encontram nas componentes de baixa frequência, enquanto que as componentes de alta frequência são as que apresentam mais vulnerabilidades em relação à compressão e ruídos [9]. Por isso, no trabalho desenvolvido, são utilizados os componentes do meio para incorporar a mensagem secreta de modo que a visibilidade da imagem não seja afetada.

Em imagens JPEG são utilizados sucessivos blocos com 8 x 8 *pixels* da imagem, formando 64 coeficientes cada, em que $F(u,v)$ é dado por (1).

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)cos(C_1)cos(C_2)\right], (1)$$

Em que:

$C_1 = \frac{(2x+1)u\pi}{16}$ e $C_2 = \frac{(2y+1)v\pi}{16}$;

$C(x) = \begin{cases} \frac{1}{\sqrt{2}}, & se\ X=0 \\ 1, & outros. \end{cases}$ e $f(x,y)$: valores da imagem original.

Após o cálculo de todos os coeficientes, é realizada a operação de quantização dos 64 elementos, são selecionados os *bits* menos significados da imagem depois do processo de DCT e são substituídos pelos bits da mensagem que se deseja esconder na imagem [10].

Para o processo inverso, é aplicada a inversa da transformada discreta de cosseno, (abreviado em inglês, IDCT), apresentado como (2).

$$f(x,y) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} F(u,v)cos(C_1)cos(C_2)\right], (2)$$

B. *Transformada de Wavelet Discreta*

A Transformada de Wavelet Discreta é uma função matemática que é aplicada para um conjunto de dados discretos, tem a capacidade de oferecer algumas informações sobre domínio frequência-tempo. Nesta transformada, o sinal no domínio do tempo é decomposto mediante dois filtros,

passa-baixa e passa-alta para extrair as frequências baixas e altas respectivamente [11].

A esteganografia baseada em *wavelet* é um método de armazenamento nos *bits* menos significativos de um *pixel*. A diferença é que a informação é armazenada nos coeficientes *wavelet* de uma imagem, em vez de alterar os *bits* dos *pixels* reais. O armazenamento nos coeficientes menos significativos de cada bloco transformado de *Haar* 4 x 4 não degrada a imagem. Com isso, armazenando informações nos coeficientes *wavelet*, a mudança nas intensidades da imagem é imperceptível [12].

C. Bits Menos Significativos

O método de inserção dos *bits* menos significativos (do inglês, *Least Significant Bits, LSB*) é o processo mais comum e mais fácil para incorporação de informações em uma cobertura de texto ou imagem [13]. Em imagens, o método se caracteriza por substituir o *bit* menos significativo de cada *pixel* da imagem de cobertura por um *bit* da informação secreta que se deseja esconder, que pode ser por exemplos texto ou mesmo imagens secretas. A imagem estenografada fica visivelmente imperceptível aos olhos humanos, sendo a sua verificação de originalidade realizada somente pelo processamento computacional.

Em imagens em tons de cinza de 8 *bits* por *pixel* é possível inserir 1 *bit* da informação secreta por *byte*. Em imagens RGB de 24 *bits* por *pixel* é possível inserir 3 *bits* da informação secreta, sendo um *bit* em cada canal da imagem [14]. Na Figura 3 é apresentado um modelo de ocultação de um caractere secreto com a substituição nos *bits* menos significativos em uma imagem de 8 *bits*.

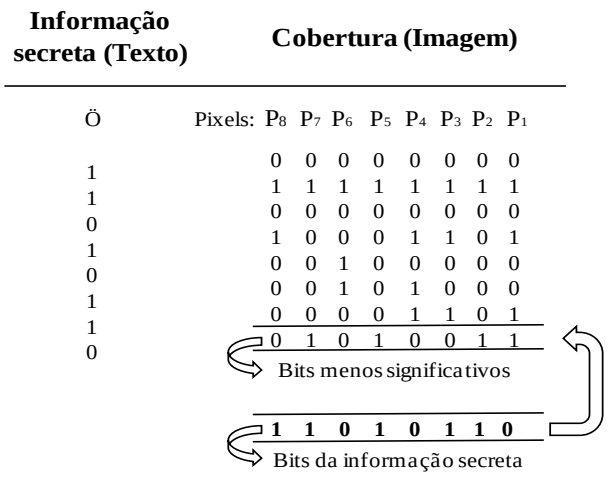

Figura 3. Esquema de inserção de informações sigilosas utilizando o método dos bits menos significativos.

A Figura 3 apresenta a substituição dos *bits* na informação secreta "Ö" que na tabela ASCII representada pelo número 99 decimal ou 11010110 binário, é inserido nos *bits* menos significativos de 8 *pixels* de uma imagem de cobertura.

Em uma imagem de 8 *bits* por *pixel* que tem 256 tonalidades de cores, com a substituição a mudança é relativamente ínfima, não afetando na qualidade ou aparência da imagem. Em uma imagem de 8 *bits* por *pixel* com tamanho de 600 *x* 400 *pixels* seria possível inserir aproximadamente 29*kb* de informação de texto. Isso porque uma imagem com 600 *x* 400 *pixels* têm 240.000 *pixels*, considerando que cada *pixel* esconde 1 *bit* seria possível inserir 240.000 *bits* ou 30.000 *bytes* nesses 240.000 *pixels.*

D. Filtragem e Mascaramento

O método da filtragem e mascaramento oculta informações por meio da marcação de uma imagem, semelhante a uma marca d'água, para tornar os dados despercebidos é necessário a utilização de imagens em tons de cinza. Ao usar imagens coloridas facilmente percebemos artefatos, porque a alteração dos *bits* ocorre uma mudança perceptível de coloração. A vantagem desse método é a informação inserida resistir à compressão, cortes e diferentes tipos de processamento de imagens porque são utilizados os *bits* mais significativos da imagem [15].

IV. METODOLOGIA IMPLEMENTADA

O sistema de inserção de dados sigilosos utilizado neste trabalho é composto de imagens clássicas do processamento digital de imagens para testes. Para os testes foram utilizados *softwares* de computação numérica, que possuem poderosos ambientes para simulações, e foram desenvolvidas as técnicas dos Bits Menos Significativos e da Transformada Discreta de Cosseno.

As imagens utilizadas são em tons de cinza para LSB e para DCT, de mesma dimensão, e nas informações secretas foram utilizadas imagens para LSB e texto para DCT, ou seja, esta seção apresenta formas de como inserir informações secretas (em formas de imagem ou texto) em imagens hospedeiras.

A. Implementação por Bits Menos Significativos

A técnica de LSB consiste na inserção de um *bit* de informação a cada conjunto de 8 *bits* da imagem, para imagens de 8 *bits* por *pixel* [13], formando a imagem

esteganografada, na recuperação da informação, com a técnica inversa, é exibindo a análise de histogramas e cálculos estatísticos.

Cálculos estatísticos como o da média e variância permitem avaliar a informação antes e depois da passagem pelo processamento de imagens, e trazem informações importantes referentes ao comportamento dos *pixels*.

O valor médio, μ_i é calculado pela somatória dos valores de níveis de cinza de todos os n *pixels* da imagem digital i e divididos pelo número total de *pixels* que tem a imagem. De modo que.

$$\mu_i = \frac{\sum_{k-1}^{n}(c_{ki})}{n}. \quad (3)$$

A variância, σ_i^2 é uma média de dispersão em torno média. E em uma imagem i representa o desvio entre o nível de cinza e o nível de cinza médio. De modo que.

$$\sigma_i^2 = \frac{\sum_{k-1}^{n}\left(c_{ki}-\mu_i\right)^2}{n-1}. \quad (4)$$

Todos os cálculos estatísticos têm que serem feitos analisando as dimensões de uma imagem I, sendo T_c o comprimento e T_l a largura da imagem em *pixels*. Uma imagem de T_c x T_l *pixels* é analisada de modo que.

$$I = \left\{I_{T_c x\, T_l} \in N \mid 0 < T_c;\ 0 < T_l\right\}. \quad (5)$$

O nível de cinza de um *pixel* ou ponto é diretamente proporcional ao brilho do tom de cinza naquele ponto e uma imagem digital pode ser representada por uma função bidimensional de intensidade de luz $f(x,y)$, sendo x e y as coordenadas espaciais de qualquer *pixel* da imagem [16]. Na Figura 4 é apresentada a representação da imagem no domínio discreto com a sua subdivisão em *pixels* e o valor correspondente da intensidade de tom de cinza.

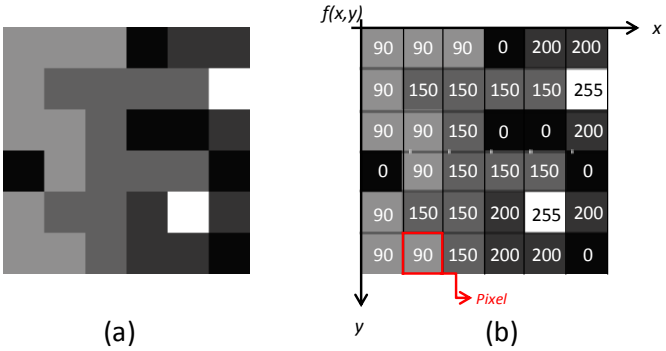

Figura 4. Imagem original (a) e imagem discreta (b) com os respectivos valores de intensidade de cor por *pixel*.

Seja C a intensidade de tom que um *pixel* pode ter, o nível 0 representa o tom mais escuro e o 255 o tom mais claro, ou seja, 256 tons. A expressão (6) representa matematicamente o nível de cinza.

$$C = \left\{f(x,y) \mid f(x,y) \in \{0,1,2,\ldots,253,254,255\}\right\} \quad (6)$$

A Figura 5 apresenta o processo computacional para ocultar informações utilizando a técnica dos bits menos significativos, por meio de qualquer *software* de computação numérica. Neste trabalho foi utilizado o *software* livre *Scilab* (*versão 5.5.2 - 64-bit*).

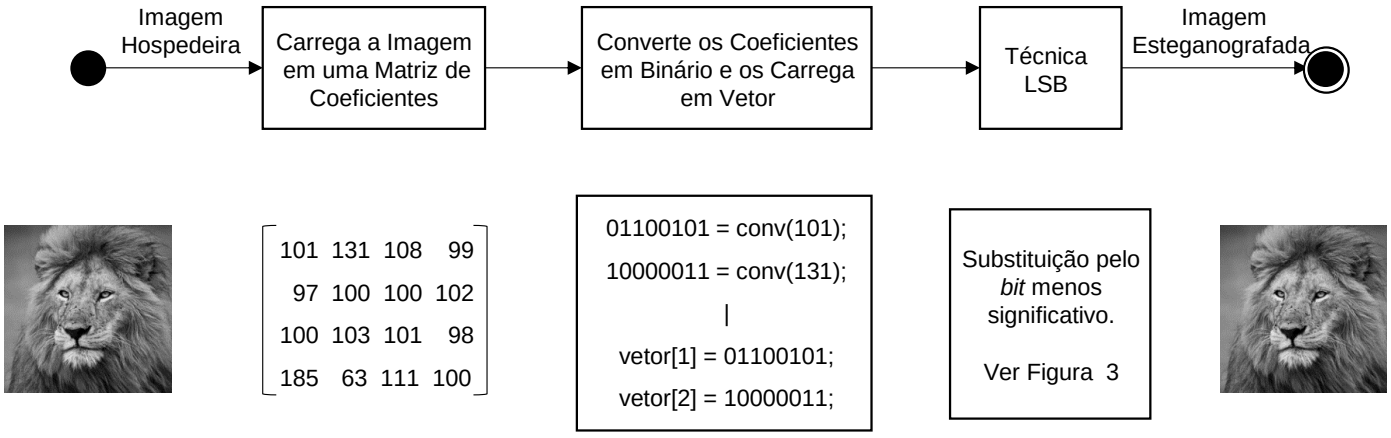

Figura 5. Esquematização computacional para ocultar informações secretas apresentado em etapas, utilizando a técnica dos bits menos significativos, em imagens com tons de cinza.

Na Figura 5, a imagem é carregada e tem os seus coeficientes armazenados em uma matriz, que posteriormente são convertidos em binários e são armazenas em um vetor, em seguida são selecionados os *bits* menos significativos de cada conjunto de 8 *bits*, são trocados por 1 *bit* da informação que será escondida, formando assim a stego-imagem.

B. Implementação por Transformada Discreta de Cosseno

Essa transformada faz com que um conjunto de 8 *x* 8 *pixels* de uma imagem hospedeira seja dividida em bandas de frequência diferentes, tais como em bandas de baixa (F_B), média (F_M) e alta (F_A) frequência, Figura 6.

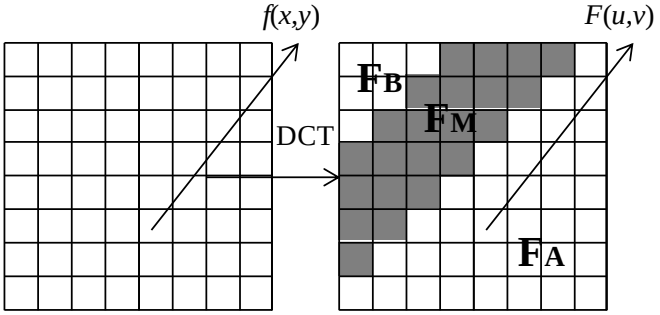

Figura 6. Ilustração do processo da transformada discreta de cosseno em uma imagem.

Com a separação das faixas de frequência é mais simples escolher a faixa de frequência que se deseja inserir a informação. A faixa de frequência média é a escolhida para ocultar a informação pelo método da DCT porque é a banda de frequência menos visível na imagem e resiste à remoção por compressão, uma das vantagens de se utilizar o método da Transformada Discreta de Cosseno. A compressão é uma estratégia de inserir mais conteúdo na imagem, considerando que quanto maior a compressão mais informações secretas podem ser ocultadas na imagem hospedeira [17].

Uma forma eficaz utilizada para ocultar informações secretas, utilizando a técnica da Transformada Discreta de Cosseno é:

- **Etapa 1**: Carregar a informação de cobertura;
- **Etapa 2**: Carregar a informação sigilosa;
- **Etapa 3**: Dividir a imagem de cobertura em blocos de 8 x 8 *pixels*;
- **Etapa 4**: Selecionar a informação e converter para binário;
- **Etapa 5**: Transformar cada bloco pela DCT;
- **Etapa 6**: Calcular o LSB de cada coeficiente gerado;
- **Etapa 7**: Trocar cada coeficiente gerado por 1 bit do dado secreto;
- **Etapa 8**: Escrever a stego-imagem.

V. RESULTADOS E DISCUSSÕES

Esta seção apresenta os resultados obtidos com o desenvolvimento dos métodos de esteganografia estudados. Com a análise dos resultados observou-se que o ocultamento de informações não gerou objetos visíveis aos olhos humanos, e somente pelo processo computacional pode-se observar a diferença entre a imagem original e a stego-imagem gerada.

A. Resultados Utilizando os Bits Menos Significativos em Imagens em Tons de Cinza.

Para o método dos Bits Menos Significativos (LSB) foram utilizadas três imagens *bitmaps* de 512 x 512 *pixels* de tamanho e em tons de cinza. Para testes, preferiu-se imagens em tons de cinza por essas não gerarem artefatos visíveis. Para as imagens hospedeiras testadas são apresentadas os seus respectivos histogramas, que servem para uma análise comparativa entre a imagem original e a marcada. A informação secreta utilizada foi a mesma para todas as imagens testadas, Figura 7.

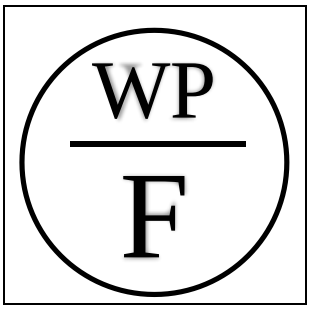

Figura 7. Informação secreta inserida nas imagens hospedeiras.

O símbolo da Figura 7 foi desenvolvido pelos autores e apresenta um emblema com as letras iniciais de cada nome dos autores deste trabalho. Este símbolo foi utilizado como uma informação secreta para ser posteriormente ocultada nas imagens de cobertura (a), (b) e (c) testadas da Figura 8, possui o tamanho de 50 *x* 50 *pixels* em formato *bitmap* e com 8 *bits* por *pixel* e foi totalmente inserido nas imagens.

Na Figura 9 são mostradas as stego-imagens (a), (b) e (c) geradas com o desenvolvimento do método dos Bits Menos Significativos e é notado que os mesmos não apresentaram artefatos ou mudanças visíveis a "olho nu". A Tabela I apresenta os resultados estatísticos obtidos com essa técnica, que foi observado que a substituição gera alterações em nível de ruído, sendo aproximadamente 0,5 para a média e 0,25 para a variância considerando as imagens testadas.

(a) Lenna (b) Square (c) Lion

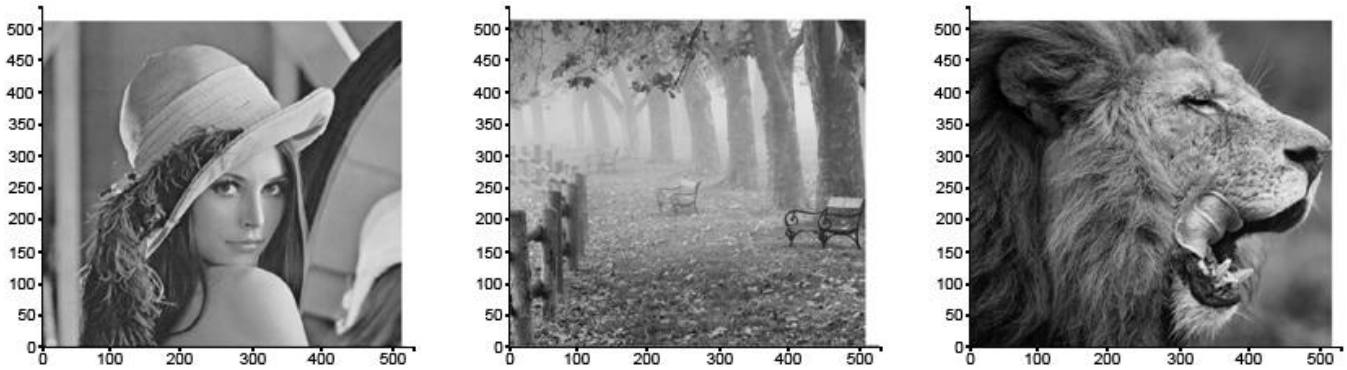

Figura 8. Imagens de cobertura em tons de cinza de 512 *x* 512 *pixels* utilizadas nos testes de ocultamento de esteganografia pelo método do LSB.

(a) Stego-Lenna (b) Stego-Square (c) Stego-Lion

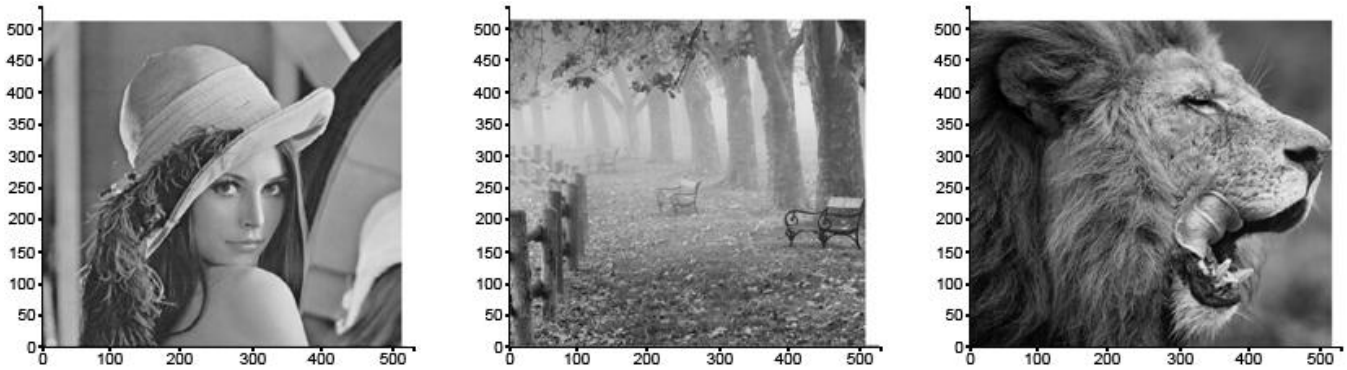

Figura 9. Imagens esteganografadas com o símbolo secreto, depois de passado pelo processo de substituição pelos *bits* menos significativos.

(a) Lenna (b) Square (c) Lion

(d) Stego-Lenna (e) Stego-Square (f) Stego-Lion

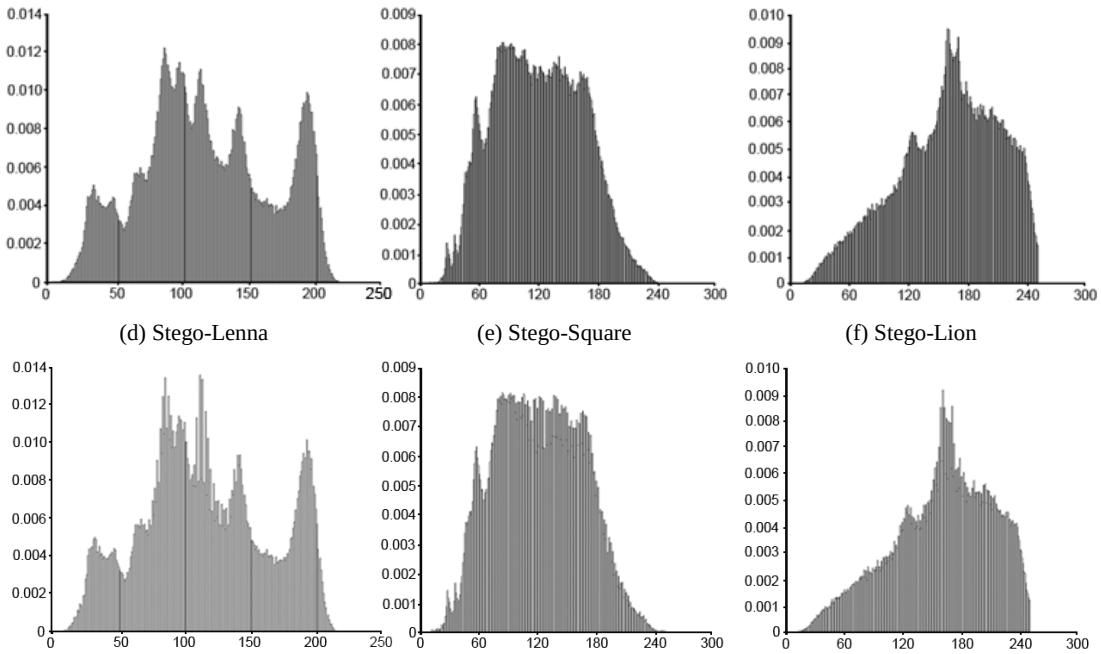

Figura 10. Histograma das imagens originais (a), (b) e (c), e histograma das imagens marcadas (d), (e) e (f).

TABELA I
DADOS ESTATÍSTICO COM O MÉTODO DO LSB

Arquivo	Média*	Variância*	Média^{+}	Variância^{+}
lenna	0.4988937	0.2499997	0.5257950	0.2493356
Square	0.4993629	0.2500005	0.5264931	0.2492991
Lion	0.4993019	0.2500005	0.5261879	0.2493151

*Média e Variância das imagens originais e $^{+}$Média e Variância das imagens esteganografadas.

B. Resultados Utilizando a Transformada Discreta de Cosseno.

Para o método da DCT também foram utilizadas três imagens para testes, de 512 x 512 *pixels*, porém no formato JPEG. A informação secreta também é diferente, ao invés de uma imagem, emblema, foram inseridas mensagens de texto. Pode ser calculada a entropia desse texto, para encontrar um número de *bits* necessários para representá-lo, considerando que o mesmo pode passar por um processo de compressão sem perdas, para ser verificado que com esse processo é possível esconder mais informações ou desenvolver uma codificação no texto de forma que fique mais segura.

Aplicada a técnica DCT na imagem, é observado que a informação foi inserida, sem degradar a qualidade da imagem hospedeira. Na Figura 11 são apresentadas as imagens testadas e as imagens depois do processo da transformada discreta do cosseno. Na Tabela II são apresentados alguns testes estatísticos com as imagens originais e stego-imagens. Observa-se que a razão entre as médias está em uma escala de aproximadamente 10^{-3}.

TABELA II
DADOS ESTATÍSTICOS COM O MÉTODO DCT

Arquivo	Média antes	Média depois	Diferença
lenna	236.2186	235.9998	$9.2691 * 10^{-4}$
vegetables	124.7471	124.6588	$7.0853 * 10^{-4}$
baboon	128.2111	128.1017	$8.5381 * 10^{-4}$

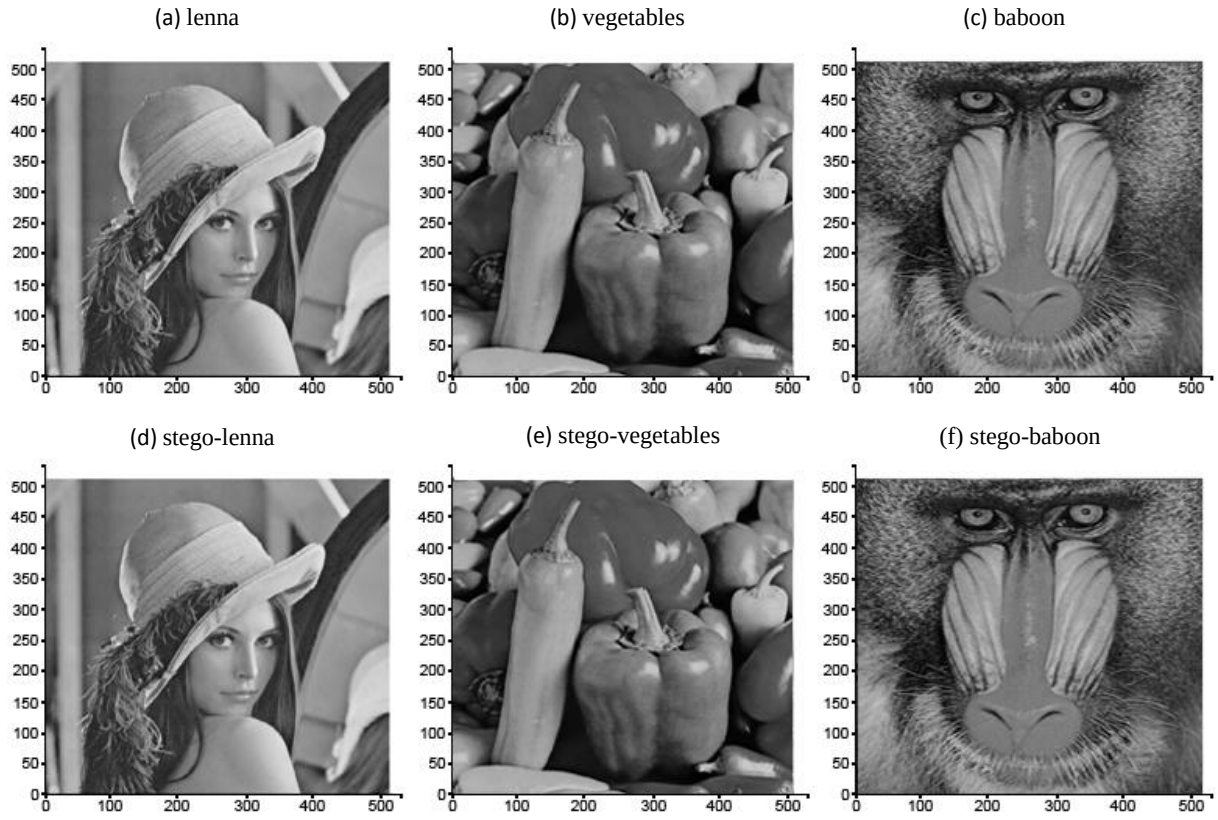

Figura 11. Imagens originais e esteganografadas geradas com o processo de ocultamento utilizando a técnica da Transformada Discreta do Cosseno.

C. Análise Comparativa entre as Técnicas Esteganográficas Implementadas.

Comparando a técnica do DCT com a LSB, a DCT tem a vantagem de resistir à compressão e a alguns processamentos computacionais que geralmente a LSB sofre, porém a DCT tem a desvantagem de exigir maior capacidade de processamento, no que implica em maior quantidade de dados.

A Tabela III apresenta o resumo e algumas vantagens das técnicas esteganográficas implementadas neste trabalho.

TABELA III
MÉTODO UTILIZADO E VANTAGENS DAS TÉCNICAS ESTENOGRÁFICAS

Técnica	Método Utilizado	Vantagens
LSB	Inserção nos bits menos significativos de byte da informação hospedeira.	Fácil de implementar, porém mais fácil de sofrer com ataques de esteganoanálise.
DCT	Oculta as informações alterando os coeficientes DCT.	É mais robusto que o LSB por distribuir a informação mais uniformemente pelo meio hospedeiro.

CONCLUSÃO

Neste artigo foram apresentadas duas técnicas esteganográficas para ocultamento de informações. Foram apresentados os resultados da implementação de duas técnicas e um estudo comparativo entre elas conforme a metodologia empregada. Para isso, foi utilizado *softwares* de computação numérica para desenvolver as ferramentas de inserção que podem ser utilizados para trazer mais segurança nas comunicações de dados, ou para auxiliar na identificação da propriedade intelectual do autor, por meio de ocultação de marcas de copyright.

AGRADECIMENTOS

Os autores deste trabalho agradecem ao Laboratório de Processamento Digital de Sinais (LPDS-IFCE) e aos órgãos de fomentos FUNCAP e CNPq.

REFERÊNCIAS

[1] KISHOR, S. Nanda; RAMAIAH, G.N Kodanda; JILANI, S. A. K. A Review on steganography through multimedia. In: *Research Advances in Integrated Navigation Systems (RAINS), International Conference on*. IEEE, 2016. p. 1-6.

[2] MISHRA, Rina; BHANODIYA, Praveen. A review on steganography and cryptography. In: *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*. IEEE, 2015. p. 119-122

[3] SHARMA, Shivani; GUPTA, Avanhesh; TRIVEDI, Manesh; YADAV, Virendra. Analysis of different text steganography techniques: A Survey. In: *Computational Intelligence & Communication Technology (CICT), 2016 Second International Conference on*. IEEE, 2016. p. 130-133.

[4] QIAN, Tu; MANOHARAN, Sathiamoorthy. A comparative review of steganalysis techniques. In: *Information Science and Security (ICISS), 2015 2nd International Conference on*. IEEE, 2015. p. 1-4.

[5] JUNIOR, Rocha V.C. Aspectos de segurança de cifras de chave-secreta. Revista de Tecnologia da Informação e Comunicação, RTIC, v. 1, 2011, p. 14-19.

[6] HOSSAIN, Kunal; PAREKH, Ranjan. An approach towards image, audio and video steganography. In: *Research in Computational Intelligence and Communication Networks (ICRCICN*), 2016 *Second International Conference on*. IEEE, 2016. p. 302-307.

[7] LAHIRI, Sounak; PAUL Printom; BANERYEE, Supriyo; MILTRA Souvik; GANGOPADHYA, Arunava. Image steganography on coloured images using edge based data hiding in DCT domain. In: *Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016 IEEE 7th Annual*. IEEE, 2016. p. 1-8.

[8] BANIK, Barnali Gupta; BANDYOPADHYAY, Samir Kumar. Implementation of image steganography algorithm using scrambled image and quantization coefficient modification in DCT. In: *Research in Computational Intelligence and Communication Networks (ICRCICN), 2015 IEEE International Conference on*. IEEE, 2015. p. 400-405.

[9] GUNJAL, Monika; JHA, Jasmine. Image steganography using discrete cosine transform (DCT) and blowfish algorithm. *International Journal of Computer Trends and Technology (IJCTT)*, v. 11, 2014. p. 144-150.

[10] HARIRI, Mehdi; KARIMI, Ronak; NOSRATI, Masoud. An introduction to steganography methods. *World Applied Programming*, v. 1, n. 3, 2011. p. 191-195.

[11] PRAMANIK, Sabyasachi; BANDYOPADHYAY, Samir K. Image steganography using wavelet transform and genetic algorithm. *International Journal of Innovative Research in Advanced Engineering*, v. 1, 2014. p. 17-20.

[12] AL-ATABY, Ali; AL-NAIMA, Fawzi. A modified high capacity image steganography technique based on wavelet transform. Changes. *The International Arab Journal of Information Technology*, v. 7, n. 4, 2010 .p 358-364.

[13] AL-AFANDY, Khalid A; FARAGALLAH Osama S; ELMAHALAWY Ahmed; EL-BANBY M. Gh. High security data hiding using image cropping and LSB least significant bit steganography. In: *Information Science and Technology (CiSt), 2016 4th IEEE International Colloquium on*. IEEE, 2016. p. 400-404.

[14] NEETA, Deshpande; SNEHAL, Kamalapur; JACOBS, Daisy. Implementation of LSB steganography and its evaluation for various bits. In: *2006 1st International Conference on Digital Information Management*. IEEE, 2006. p. 173-178.

[15] KER, Andrew D. Steganalysis of LSB matching in grayscale images. IEEE signal processing letters, v. 12, n. 6, 2005. p. 441-444.

[16] GONZALEZ, Rafael C.; WOODS, Richard E.; EDDINS, S. L. Morphological imagage processing. Digital Image Processing, v. 3, 2008. p. 627- 688.

[17] KAUR, Blossom; KAUR, Amandeep; SINGH, Jasdeep. Steganographic approach for hiding image in DCT domain. *International Journal of Advances in Engineering & Technology*, v. 1, n. 3, 2011. p. 72-78.