CNMAI Congresso Nacional de Matemática Aplicada à Indústria 2014
18 a 21 de novembro de 2014, Caldas Novas - Goiás

ESTEGANOGRAFIA BASEADA NA PARIDADE DOS *BITS* MENOS SIGNIFICATIVOS

1

Resumo. *Comunicação segura é de extrema importância para aplicações que lidam com informações confidenciais. A esteganografia é uma prática de comunicação imperceptível, a qual consiste em esconder mensagens em mídias que são, aparentemente, irrelevantes. Em contrapartida à esteganografia, existem técnicas de estaganálise que visam identificar mensagens ocultas. Este artigo propõe uma nova técnica de esteganografia em imagens digitais. Resultados experimentais indicam que técnica devolvida é mais resistente do que a LSB aos ataques de esteganálise RS e ataque visual, enquanto que a qualidade visual dos esteganogramas (imagens com mensagem embutidas) é mantida.*

Palavras-chave: *Esteganografia, esteganálise, ataque RS e ataque visual*

1. INTRODUÇÃO

Existe uma grande preocupação com privacidade de certos dados que trafegam na *World Wide Web* (WWW). A criptografia é uma das formas de garantir a segurança destes dados devido à dificuldade de decodificação da mensagem, isto é, obter a estrutura lógica dos dados. Porém, a criptografia não oculta a percepção da comunicação em si, pois dados criptografados são identificados facilmente (Cox et al., 2008). Já por meio de técnicas de estenografia digital, mensagens são ocultadas dentro de outros dados aparentemente irrelevantes, de forma que a comunicação passe despercebida. Em contra partida, existem técnicas com o objetivo de identificar a prática de esteganografia, chamadas de esteganálise (Cox et al., 2008; Li et al., 2011; Chanu et al., 2012; Artz, 2001). Logo, além de ocultar a percepção da comunicação pelos sentidos humanos, a esteganografia deve resistir a ataques da esteganálise. Este trabalho propõe uma nova técnica de esteganografia em imagens digitais, robusta à esteganálise RS (Fridrich et al., 2001) e ao ataque visual (Sharp, 2001).

Este artigo está organizado da seguinte forma. A seção 2 apresenta conceitos básicos necessários para o entendimento da técnica proposta. A seção 3 descreve os principais trabalhos relacionados a esta pesquisa. A seção 4 detalha a técnica proposta. A seção 5 apresenta os resultados obtidos ao aplicar os ataques de esteganografia, RS e ataque visual, nos esteganogramas gerados pela técnica LSB e pela técnica proposta. A seção 6 apresenta as conclusões desta pesquisa.

2. CONCEITOS BÁSICOS

Esta seção apresenta conceitos básicos de segurança da informação, imagens digitais, esteganografia e esteganálise. O leitor habituado com estes conceitos pode ir direto para a seção 3.

Com a popularização da Internet, as ameaças da segurança da informação estão em constante evolução. Coleta e divulgação de dados sigilosos por pessoas maliciosas através da WWW pode colocar pessoas e instituições em posição delicada, o que faz com que seja dada grande importância à segurança dos dados.

Da mesma maneira que se têm desenvolvido técnicas científicas para aumentar a segurança de dados, os *hackers* têm explorado as vulnerabilidades de segurança da informação para ter acesso a dados preciosos. Se antes, medidas simples de proteção garantiam a segurança, atualmente elas devem ser revistas e, possivelmente, reforçadas (Moreira, 2001). Quanto maior a importância de um dado, maior deve ser a preocupação com a sua segurança. Existem três técnicas computacionais básicas para prover a segurança de informações (Cox et al., 2008): criptografia, marca d'água e esteganografia.

A criptografia converte dados legíveis em algo sem sentido, e posteriormente, recupera os dados originais a partir desses dados sem sentido (Burnett e Paine, 2001). A técnica de criptografia mais utilizada na WWW é a criptografia de chaves RSA, a qual é usada para proteger dados importantes, como senhas de bancos, números de cartões de crédito, informações pessoais, conversas sigilosas, entre outras (Coutinho, 2005). Porém, a criptografia não oculta a percepção da comunicação em si, pois dados criptografados são facilmente identificados (Burnett e Paine, 2001; Cox et al., 2008).

Marca d'água ou *watermarking* (Cox et al., 2008; Bianchi e Piva, 2013) é a prática de alterar uma mídia (áudio, vídeo ou imagem) por embutir uma "marca" sobre aquela mídia. Seu principal uso e na proteção dos direitos autorais. As marcas d'água podem ser de fácil percepção ou estarem ocultas na mídia portadora (Cox et al., 2008). O principal objetivo de uma marca d'água é que ela seja robusta a modificação da mídia (compressão, conversões de formato, conversão digital-analógico, entre outras). Mesmo que a mídia sofra alterações a marca d'água deve ser capaz de identificá-la.

A esteganografia é uma prática de comunicação imperceptível. Existem registros de métodos de esteganografia utilizados na idade do ouro na Grécia, onde se utilizava placas de madeiras revestida com cera como portadoras para ocultar mensagens. A cera das placas de madeira era derretida e escrita uma mensagem na madeira, e posteriormente era passada uma nova camada de cera e escrito algo irrelevante na cera, assim a mensagem importante ficava ocultada (Li et al., 2011). Seguindo o mesmo preceito de ocultar informações, atualmente, a esteganografia é implementada digitalmente escondendo dados dentro de outros dados que aparentemente são irrelevantes. Enquanto que na criptografia a existência da comunicação pode ser facilmente detectada, na esteganografia o objetivo é camuflar para que a comunicação passe despercebida (Artz, 2001).

As técnicas de esteganografia podem ser classificadas em: esteganografia no domínio espacial de imagem, esteganografia no domínio da frequência de imagem e esteganografia adaptativa (Cheddad et al., 2010; Chanu et al., 2012). A esteganografia no domínio espacial está ligada a alteração dos *bits* menos significativos da mídia portadora, de forma sequencial ou aleatória, de modo que a alteração fique imperceptível aos sentidos humanos. Esteganografia no domínio da frequência de imagem se baseia em transformadas tais como: transformada discreta do cosseno, transformada discreta de Wavelet, transformada discreta de Fourier, decomposição em valores singulares, entre outras. Basicamente, as técnicas de esteganografia no domínio da frequência de imagem se baseiam em inserir a mensagem nos *bits* menos significativos dos coeficientes calculados pelas transformadas. A técnica adaptativa se baseia em estatísticas das imagens para determinar em quais *pixels* devem ser inserida a mensagem secreta. A ideia é degradar as propriedades estatísticas da imagem original o mínimo possível. Os principais métodos da literatura definem os *pixels* a ser transformados com base em estatísticas de *pixels* vizinhos. Neste artigo o foco é em técnicas no domínio espacial de imagem.

Esteganálise é uma família de técnicas usadas como contra medida à esteganografia, ou seja, sua função é identificar esteganogramas (mídias com mensagens inseridas), porém, a mensagem em si não precisa necessariamente ser decodificada. Técnicas de esteganálise pode ser agrupadas em duas categorias (Chanu et al., 2012; Luo et al., 2008; Kharrazi e Sencar, 2004): 1) métodos específicos – quando se presume o método esteganográfico usado e 2) métodos universais – que realizam uma classificação binária baseada em aspectos inerentes das mídias que, normalmente, são violados por esteganografia.

2.1. Imagens digitais

Existem dois tipos básicos de imagem digital: vetorial e mapa de *bits*. Neste trabalho utiliza-se mapa de *bits*, que é uma matriz bidimensional (linha e coluna), em que cada elemento corresponde a um *pixel*. Mapas de *bits* também pode ser categorizadas em: imagens em níveis de cinza, onde existe um canal (uma matriz) de que define a tonalidade de cinza de cada *pixel*, e imagens coloridas, onde normalmente existe três canais de cores (três matrizes), onde a combinação de três componentes de cor gera a cor do píxel. O sistema RGB, composto pelas cores vermelho (*red*), verde (*green*) e azul (*blue*) é o mais usado em imagens digitais (Gonzalez e Woods, 2008). Para imagens de 24 *bits* de resolução de cor, normalmente, os valores dos canais RGB são representações numérica no intervalo de 0 a 255, que logicamente podem ser expressados como números binários de oito *bits*.

Valores muito próximos são de difícil distinção pelo sistema visual humano.

O termo portadora é utilizado neste artigo para denominar a mídia que será usada para esconder uma mensagem dentro dela. No caso deste trabalho, as mídias portadoras são imagens do tipo *bitmap*. Mensagem secreta é a mensagem que será embutida na portadora. A mensagem secreta pode ser um texto, uma imagem, um áudio, ou qualquer outra mídia digital. A carga útil da portadora corresponde a quantidade de *bits* da mensagem secreta que a portadora pode guardar. Por exemplo, se pode-se esconder três *bits* da mensagem secreta por *pixel* de uma imagem, então, a carga útil será a quantidade de *pixels* da imagem vezes três.

2.2. Esteganografia LSB

A técnica mais conhecida de esteganografia em imagens é a *Least Significant Bit* (LSB). Nesta técnica, utiliza-se os *bits* menos significativos dos elementos das matrizes de cores para inserção de *bits* da mensagem, onde o *bit* menos significativo é substituído pelo *bit* correspondente da mensasagem secreta. Quando o destinatário receber a imagem portadora, basta apenas coletar o *bit* menos significativo de cada *pixel* e remontar a mensagem.

2.3. Esteganálise

A esteganálise é a contra medida a esteganografia. Técnicas de esteganálise se dedicam a identificar mídias com esteganogramas. Não necessariamente as técnicas de esteganálise se dedicam a obter a mensagens secreta. Grande parte das técnicas tentam apenas reconhecer se uma mídia portadora tem ou não uma mensagem embutida (Wang e Wang, 2004; Chanu et al., 2012).

2.3.1. Ataque Visual

Ataque visual basicamente destaca o *bit* menos significativo desejado, trocando-o com o *bit* mais significativo, recebendo mais destaque pode se perceber anomalias como a inserção de ruídos aleatórios (Sharp, 2001). Existem casos em que técnicas não utilizam especificamente o *bit* menos significativo, inserindo a mensagem secreta no último ou penúltimo *bit* menos significativo. Porém, quanto maior a significância do *bit* alterado maior será a diferença visual na portadora. O ataque visual pode detectar a mensagem nestas posições, trocado a posição suspeita de conter o *bit* da mensagem secreta com o de maior significância.

2.3.2. Ataque RS

O Ataque RS Fridrich et al. (2001) utiliza a premissa que todas imagens tem uma certa propriedade estatística. Quando se aplica alguma técnica de esteganografia em uma imagem insere-se um ruído semelhante ao aleatório, alterando a propriedade estatística da imagem. Por exemplo, se o *bit* menos significativos for 1 em vários *pixels* seguidos, a probabilidade dele ser 1 novamente, num próximo *pixel* é muito grande. Ao se utilizar a esteganografia LSB os *bits* menos significativos tomam um padrão aleatório. O ataque RS analisa as inter-relações entres os *pixels* presentes nas imagens. Este método pode ser aplicado tanto a imagens coloridas quanto a imagens em níveis de cinza (Wang e Wang, 2004; Chanu et al., 2012; Cox et al., 2008).

3. TRABALHOS RELACIONADOS

Em (Lin e Hsueh, 2008), os autores utilizam três *pixels* de imagens em níveis de cinza para inserir dois *bits* da mensagem secreta. A diferença absoluta entre o primeiro e o segundo *bit* menos significativos, do primeiro e do segundo *pixel*, respectivamente, é ajustada, caso necessário, para corresponder ao primeiro *bit* da mensagem. Tal ajuste é feito trocando um destes *bits*. Da mesma forma, a diferença entre o segundo e o terceiro, é ajustada, caso necessário, para representar o próximo *bit* da mensagem. Com a aplicação das técnicas de esteganálise, este método se comporta um tanto quanto similar ao método LSB, pois a informação está concentrada apenas no *bit* menos significativo de cada *pixel*. Outro ponto negativo desta técnica é a carga útil da mensagem portadora, que é de 2/3 da quantidade de *pixels* da imagem.

Em (Wang e Niu, 2010), para aumentar a carga útil de imagens monocromáticas, os autores utilizam os 3 *bits* menos significativos de cada *pixel* para esconder a mensagem secreta, porém, o valor pode se distanciar bastante do valor real do *pixel*. Para resolver este problema é ajustado através de um algoritmo genético os próximos *bits* de forma a minimizar a diferença, tal que a inserção do *bit* da mensagem não altere visualmente a imagem. Contudo o processo de ajuste dos outros *bits* por algoritmo genético tem um alto custo computacional, o que limita a eficiência da comunicação.

4. TÉCNICA PROPOSTA

Neste trabalho foram utilizadas imagens coloridas com o propósito de utilizar as 3 matrizes de cores para inserção da mensagem, insenrido 1 *bit* da mensagem a cada componente de cor de cada *pixel*. Logo, considerando imagens coloridas, representadas conforme o sistema de cor RGB, a cada *pixel* esconde-se 3 *bits* da mensagem, maximizando a carga útil da portadora.

Na técnica desenvolvida, os *bits* da mensagem secreta são inseridos na paridade dos três *bits* menos significativos. A mensagem secreta é convertida em uma sequência de números binários (*bits*), onde cada *bit* da mensagem deve ser inserido na paridade dos três *bits* menos significativos de cada componente de cor de *pixel*. Se em um componente de cor de *pixel*, houver necessidade de armazenar o *bit* 0 a soma dos 3 *bits* menos significativos deve ser par. Similarmente, se o *bit* a ser armazenado for 1, a soma dos 3 *bits* menos significativos da componente de cor de *pixel* deve ser ímpar. Logo, para inserir a mensagem é verificado a paridade dos componentes de cor dos *pixels* e feito seu ajuste, caso necessário.

A equação 1 calcula a paridade dos três *bits* menos significativos de uma componente de cor de um *pixel*, onde c representa o valor de uma componente de cor de um *pixel* e $\mod$ corresponde ao resto da divisão. Se a paridade não for a desejada para esconder o *bit* correspondente da mensagem, inverte-se um dos 3 *bits* menos significativos para refletir a necessidade de armazenamento. A escolha da posição a ser trocada é feita de forma aleatória, visando descentralizar o plano de *bit* da portadora que guarda a mensagem secreta. Desta maneira, se for utilizado o ataque visual ou o ataque RS no *bit* menos significativo, que corresponde ao plano de *bit* 0, as anomalias serão menores do que se todos os *bits* da mensagem secreta estivessem neste plano de *bit*.

$$Paridade = \left(\sum_{i=0}^{2} \left(\frac{c}{2^i} \mod 2 \right) \mod 2 \right) \tag{1}$$

A equação 2 é utilizada para ajustar do componente de cor de um *pixel* c, da matriz de *pixels*, para que este contenha a paridade desejada, onde r é um valor aleatório do conjunto $\{0, 1, 2\}$, que representa o plano de *bit* da componente de cor, que será alterado.

$$c' = \begin{cases} c - 2^r, & \text{se } ((c/2^r) \mod 2) = 1 \\ c + 2^r, & \text{se } ((c/2^r) \mod 2) = 0 \end{cases} \tag{2}$$

No processo de inserção da mensagem secreta, para definir o fim de mensagem foi inserido a sequência de *bits* “11111111” que corresponde ao caractere ”ÿ”. Esse marcador foi utilizado pelo fato deste caractere ser extremamente raro em textos em português e em inglês.

Quando o destinatário recebe o esteganograma, ele utiliza um algoritmo que verifica a paridade dos três *bits* menos significativos de cada componente de cor de *pixel*, para extrair a mensagem. Se a paridade for par, o *bit* correspondente da mensagem é 0 e, se a paridade é impar, o *bit* correspondente da mensagem é 1. Os *bits* extraídos são aglomerados em *bytes* e, em seguida, convertidos para caracteres com base na tabela ASCII (*American Standard Code for Information Interchange*). O algoritmo pára ao encontrar o caractere “ÿ” e, então, exibe a mensagem secreta ao destinatário.

A Tabela 1 contém um exemplo de inserção da sequência de *bits* “010011110111010” em 15 bytes da portadora, os quais poderiam corresponder aos componentes de cor R (*red*), G (*green*) e B (*blue*) de cinco *pixels* de uma imagem colorida. A primeira coluna contém das componentes de cor dos *pixels* da portadora sem a mensagem secreta. A segunda coluna contém os *bits* da mensagem secreta. Finalmente, a terceira coluna contém os 15 *bytes* da portadora após inserida a mensagem (esteganograma).

5. RESULTADOS

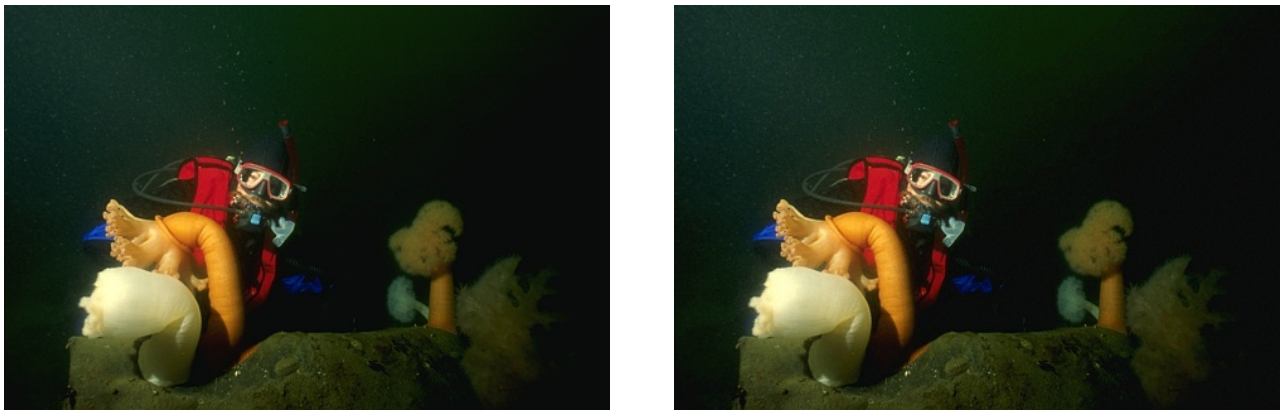
Todas as imagens originais utilizadas neste projeto pertencem ao *Berkeley Segmentation Dataset*, disponível em `http://www.eecs.berkeley.edu/Research/Projects/CS/vision/bsds/`. Para analisar o desempenho da técnica proposta foi utilizado o programa *StegSecret* desenvolvido por Alfonso Muñoz e disponível em `http://stegsecret.sourceforge.net`. O *StegSecret* implementa a técnica RS de acordo com especificações descritas em (Fridrich et al., 2001).

A Figura 1 mostra a imagem portadora antes (a) e depois (b) de ser inserido uma mensagem secreta aleatória de 57899 *bytes*, que corresponde a carga útil da imagem, através da técnica proposta neste artigo. Visualmente

Valor de componente de cor da portadora	*Bit* da mensagem	Valor de componente de cor da portadora depois de inserido o *bit* correspodendente da mensagem
00010011	0	00010011
00101100	1	00101100
00101000	0	00101000
00010001	0	00010011
00101010	1	00101010
00100110	1	00100100
00001110	1	00001100
00100111	1	00100111
00100001	0	00100000
00010001	1	00010001
00101010	1	00101010
00100100	1	00100100
00011000	0	00011000
00110001	1	00110001
00101011	0	00101011

Tabela 1. Sequência de *bytes* antes e depois da inserção da mensagem secreta

não se nota diferenças significativas nas imagens. A Figuras 2-(a) e -(b) mostram *um zoom* na região do óculos do mergulhador das Figuras 1-(a) e -(b), respectivamente. Pode se notar que as diferenças de cores dos *pixels* são dificilmente percebidas visualmente.

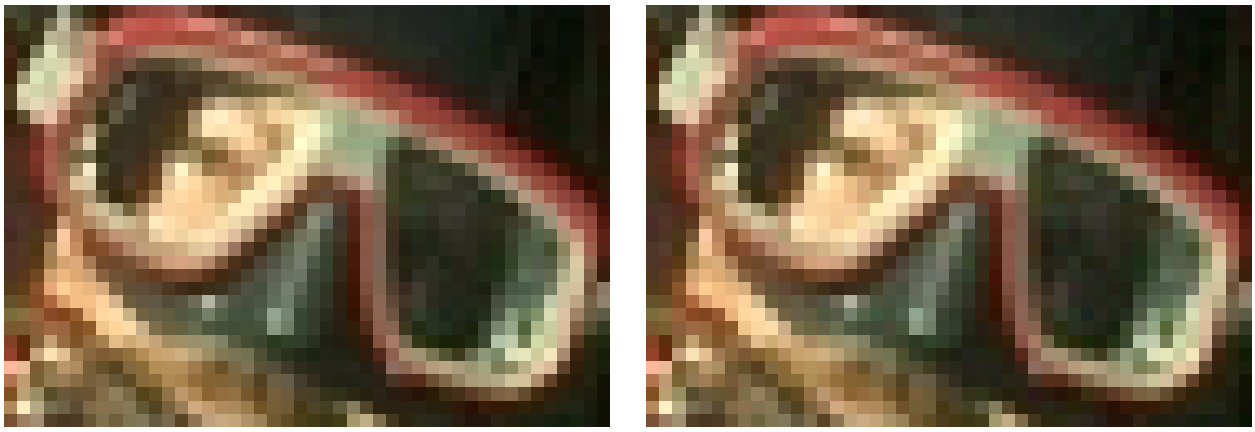


(a) **Imagem original** (b) **Esteganograma gerado pela técnica proposta**

Figura 1. (a) Imagem original e (b) esteganograma gerado pela técnica proposta

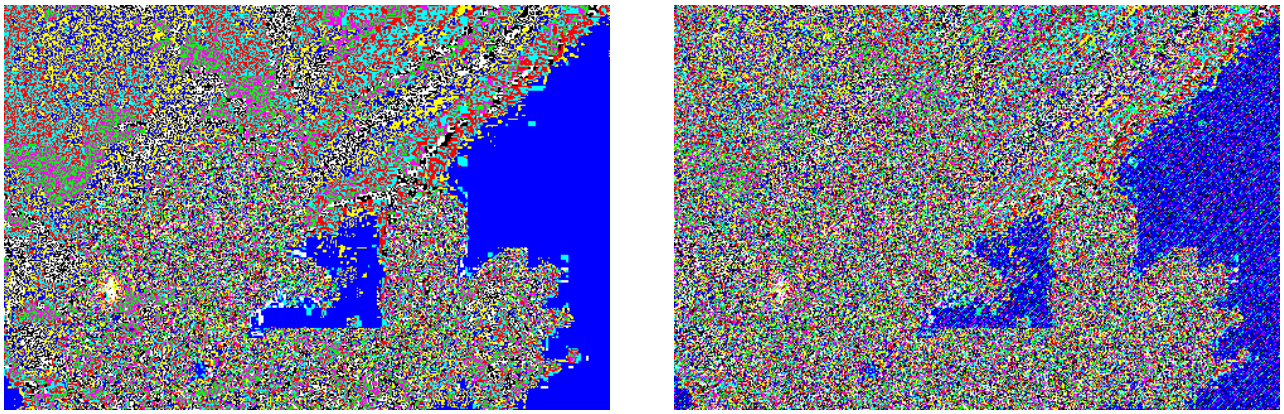
A Figura 3-(a) e -(b) mostram os resultados de ataques visuais sobre o *bit* menos significativo da uma imagem original (45096.bmp) e de um esteganograma contendo 57899 *bytes* aleatórios, inseridos pela técnica proposta. Nota-se que o resultado do ataque visual não é um padrão completamente aleatório, o qual seria obtido se a mensagem fosse inserida por meio da técnica LSB.

Na Tabela 2 são mostrados os resultados obtidos ao se aplicar o ataque de esteganálise RS. Foram utilizadas cinco imagens escolhidas aleatoriamente do *Berkeley Segmentation Dataset*. As estimativas do tamanho da mensagem secreta, calculadas pelo ataque RS, para as técnicas LSB e a técnica proposta, são dadas na terceira e quarta coluna, respectivamente. Todas as imagens portadoras tem resolução de 481×321 *pixels* e o tamanho da mensagem inserida é de 57899 *bytes* que corresponde a carga útil de cada imagem conforme ambas as técnicas. Notamos que mesmo em imagens sem mensagem embutida, o algoritmo RS indica um determinado tamanho da mensagem, ou seja, falsos positivos ou um *bias* conforme reportado pelo autores da técnica em Fridrich et al. (2001). Logo, para melhor análise foi também aplicado o RS na portadora antes de se inserir a mensagem secreta. Em todas as imagens testadas a técnica proposta (última coluna) mostrou-se maior resistência à estimativa de tamanho da mensagem pelo ataque RS, do que a técnica LSB (penúltima coluna). Pode-se notar



(a) ***Zoom* na imagem original** (b) ***Zoom* no esteganograma gerado pela técnica proposta**

Figura 2. *Zoom* na região o óculos do mergulhados das Figuras 1-(a), e -(b), respectivamente



(a) Ataque visual à imagem original (b) Ataque visual ao esteganograma gerado pela técnica proposta

Figura 3. (a) Ataque visual ao primeiro plano de *bits* da imagem original 45096.bmp mostrada na Figura 1-(a); e (b) ataque visual ao primeiro plano de *bits* do esteganograma gerado pela técnica proposta mostrado na Figura 1-(b)

qua o ataque RS estima muito bem o tamanho da mensagem quando usado a técnica LSB. Já quando usado a técnica proposta para a inserção da mensagem secreta o ataque RS não consegue uma boa estimava do tamanho da mensagem inserida.

Na Figura 4 é mostrado um gráfico de estimativa do tamanho de mensagem gerado pelo ataque RS aumentando-se o tamanho da mensagem inserida. Foram feitos 10 incrementos de 1600 *bytes* no tamanho da mensagem secreta à partir de 0 *bytes*. Nota-se no gráfico que, aumentando a mensagem secreta o ataque RS aponta um aumento de tamanho da mensagem na técnica desenvolvida, porém, o aumento é em porção menor que a técnica de LSB. A estimativa do tamanho da mensagem secreta de esteganogramas LSB é muito próximo da tamanho da mensagem inserida; já a estimativa do tamanho da mensagem secreta de esteganogramas gerados pela técnica proposta aproxima pouco do tamanho da mensagem inserida. Assim, pode-se dizer que o ataque RS não consegue verificar precisamente o tamanho da mensagem inserida pelo método proposto.

6. CONCLUSÃO

Neste trabalho foi desenvolvida uma técnica esteganografica que se baseia na paridade dos *bits* menos significativos. O ajuste de paridade foi feito por troca aleatória de um dos três *bits* menos significativos. Assim, há uma descentralização do plano de *bit* da mensagem secreta, o que aumenta a resistência à ataques de esteganálise.

Em todos os testes feitos, o algoritmo proposto, baseado na paridade dos três *bits* menos significativos teve melhor desempenho que o LSB quanto a estimativa do tamanho da mensagem calculada pelo ataque

Identificador da imagem original	*Bias* da imagem original	Esteganograma LSB	Esteganograma gerado pela técnica proposta
45096.bmp	1180	57276	22462
21077.bmp	6102	56189	25777
16077.bmp	6908	57229	25620
37073.bmp	2214	57210	23105
19021.bmp	1124	57582	21535

Tabela 2. Estimativas do tamanho de mensagem por ataque RS

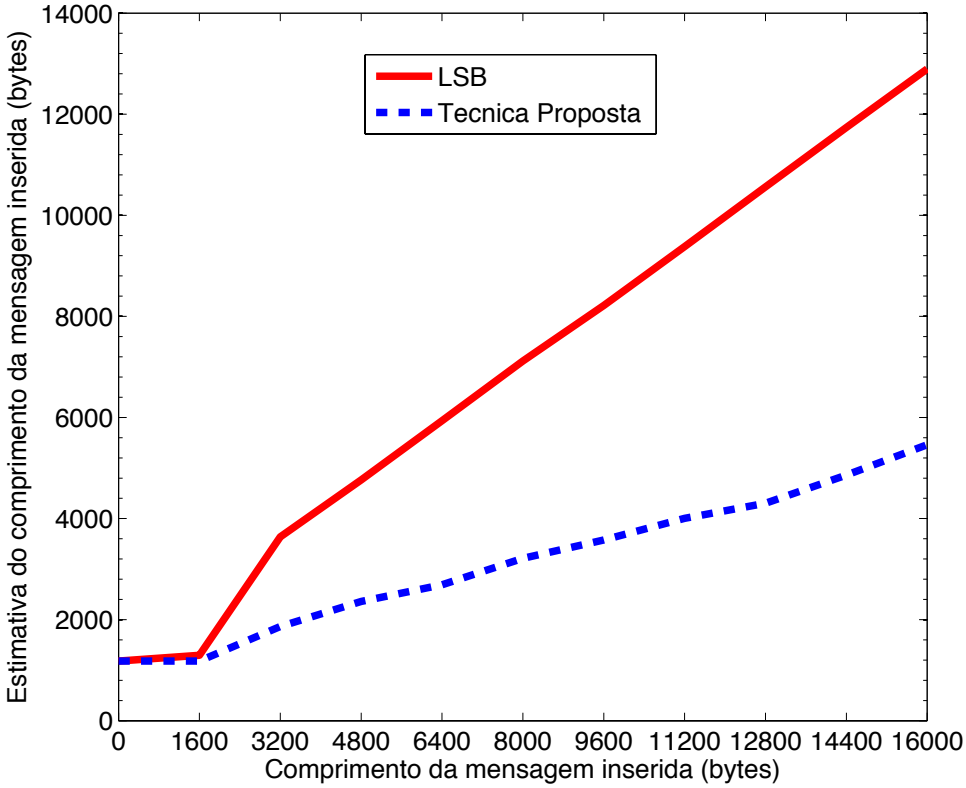


Figura 4. Gráfico de comparação do tamanho da mensagem apontado pelo ataque RS nas técnicas avaliadas em função do aumento do tamanho real da mensagem

RS. Considerando que uma pessoa tenha acesso a um esteganograma gerado pelo método desenvolvido e mas não obtenha a imagem original, mesmo utilizando as técnicas de esteganálise, ataque visual e ataque RS, não identificará precisamente a utilização de esteganografia. Também, as imagens com mensagem secreta embutida continuam com aspectos visuais naturais muito próximos aos das imagens originais, o que não acarreta em suspeita de esteganografia na visualização dos esteganogramas.

REFERÊNCIAS

Artz, D. 2001. Digital steganography: Hiding data within data. *IEEE Internet Computing*, *5*(3), 75–80.

Bianchi, T., e Piva, A. 2013. Secure watermarking for multimedia content protection: A review of its benefits and open issues. *IEEE Signal Processing Magazine*, *30*(2), 87–96.

Burnett, S., e Paine, S. 2001. *RSA Security's Official Guide to Cryptography*. McGraw-Hill. 419p.

Chanu, Y. J., Singh, K. M., e Tuithung, T. 2012. Image steganography and steganalysis: A survey. *International Journal of Computer Applications*, *52*(2), 1–11.

Cheddad, A., Condell, J., Curran, K., e Kevitt, P. M. 2010. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *90*(3), 727–752.

Coutinho, S. C. 2005. *Números Inteiros e Criptografia RSA*. IMPA, segunda ed. 226p.

Cox, I., Miller, M., Bloom, J., Fridrich, J., e Kalker, T. 2008. *Digital Watermarking and Steganography*. Elsevier, 2nd ed. 624p.

Fridrich, J., Goljan, M., e Du, R. 2001. Detecting lsb steganography in color, and gray-scale images. *IEEE MultiMedia*, *8*(4), 22–28.

Gonzalez, R. C., e Woods, R. E. 2008. *Digital Image Processing*. Prentice Hall, 3rd ed. 954p.

Kharrazi, M., e Sencar, N., H. T.and Memon 2004. Image steganography: Concepts and practice. *Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore*, (pp. 1–31).

Li, B., He, J., Huang, J., e Shi, Y. Q. 2011. A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, *2*(2), 142–172.

Lin, C.-C., e Hsueh, N.-L. 2008. A lossless data hiding scheme based on three-pixel block differences. *Pattern Recognition*, *41*(4), 1415–1425.

Luo, X.-Y., Wang, D.-S., Wang, P., e Liu, F.-L. 2008. A review on blind detection for image steganography. *Signal Processing*, *88*(9), 2138 – 2157.

Moreira, N. S. 2001. *Segurança Mínima: uma visão corporativa da segurança de informações*. Axcel Books. 254p.

Sharp, T. 2001. An implementation of key-based digital signal steganography. *Information Hiding. Lecture Notes in Computer Science*, *2137*, 13–26.

Wang, B., S. Yang, e Niu, X. 2010. A secure steganography method based on genetic algorithm. *Journal of Information Hiding and Multimedia Signal Processing*, *1*(1), 28–35.

Wang, H., e Wang, S. 2004. Cyber warfare: steganography vs. steganalysis. *Communications of the ACM*, *47*(10), 76–82.

RESPONSABILIDADE AUTORAL

As opiniões, hipóteses e conclusões expressas neste artigo são de responsabilidade exclusiva dos autores.

STEGANOGRAPHY BASED ON LEAST SIGNIFICANT BITS PARITY

1

Abstract. *Secure communication is of paramount importance for applications that handle confidential information. Steganography is the practice of imperceptible communication, by hiding messages in media that are apparently irrelevant. In contrast to steganography, there are steganalysis techniques to identify hidden messages. This paper proposes a new steganography technique for digital images. Experimental results indicate that the proposed technique is more resistant than the LSB on RS and visual steganalytic attacks. Also, the visual quality of steganograms (images with embedded messages) is maintained.*

Keywords: *Steganography, steganalysis, RS attack and visual attack*