Esteganografia de imagens em escala de cinza pela técnica de substituição LSB

Polycarpo Souza Neto, Wellington Dantas de Almeida e Francisco José Alves de Aquino

Resumo – Em uma sociedade cada vez mais dependente da tecnologia e da comunicação, cresce a necessidade da criação de técnicas de proteção da informação. Esteganografia é a técnica onde uma informação é escondida em outra de menor importância. Este trabalho traz uma técnica de esteganografia de imagem baseada na substituição dos bits menos significativos (LSB) de imagens digitais.

Palavras–chave: Esteganografia, bit menos significativo, segurança da informação.

Abstract – In an increasingly dependent on technology and communication society, grows the need for creation of information protection techniques. Steganography is a technique in which information can to be communicating secretly by hiding in another information with changing its significance. This paper presents an approach of image steganography based on replacing the least significant bits (LSB) of steganography to generate digital images was made.

Key-words: Steganography, least significant bit, information security.

I. INTRODUÇÃO

A esteganografia é a arte de ocultar informação dentro de um subconjunto de dados, sem ressaltar a existência da informação escondida [1]. Dentre as técnicas mais utilizadas e mais simples de serem implementadas, encontra-se a escrita no Bit Menos Significativo (LSB) [2]. O algoritmo LSB utiliza uma imagem pública (imagem de cobertura), para esconder outra informação. Esta informação será escondida nos bits menos significativos da imagem de cobertura, e tem como resultado uma imagem com os dados embutidos (estego-imagem. Quando a informação escondida também é uma imagem, ela é chamada de imagem privada.

II. REVISÃO DE LITERATURA

A.Inserção no Bit Menos Significativo

O uso dessa técnica é baseado na modificação dos bits menos significativos (Least Significant Bit) dos valores de pixel no domínio espacial. [3].

Essa técnica possibilita a aplicação em cada pixel de uma imagem codificada em 24bits por pixel. De forma segura podemos selecionar o LSB de cada byte pra ocultar a informação sem mostras de artefatos. Essas técnicas podem inclusive, gerar escrita em bits não seqüenciais, sendo de difícil detecção[5-6].

Polycarpo Souza Neto, Wellington Dantas de Almeida e Francisco José Alves de Aquino¸ Departamento de Engenharia de Telecomunicações, Instituto Federal do CE, Fortaleza-CE, Brasil, E-mails: policarponeto.pn@gmail.com, wellingtondantas39@gmail.com, fcoalves_aq@ifce.edu.br. Este trabalho foi parcialmente financiado pelo CNPq.

B. Filtragem e Mascaramento

As técnicas de filtragem e mascaramento são mais robustas que técnicas como LSB. No entanto, são técnicas com fácil detecção [2]. Ao contrário do LSB, essas técnicas trabalham com bits mais significativos (MSB). Sabendo disso, ao usar imagens em cores, facilmente percebemos artefatos.

C. Algorítimos e Transformações

Essas técnicas aplicam uma certa transformação em blocos de 8x8 pixels na imagem. São selecionados em cada bloco as informações redundantes. Posteriormente, estes coeficientes são utilizados para atribuir a mensagem a ser escondida em um processo, em que cada coeficiente é substituído por um valor pré-determinado para o bit 0 ou 1 [2].Como exemplo temos a Tranformada Discreta do Cosseno (DCT) dada pela seguinte equação:

$$G_f = \frac{1}{2} C_f \sum_{t=0}^{n-1} p_t \cos\left(\frac{(2t+1)f\pi}{2n}\right), \quad onde\ C_f \begin{cases} \frac{1}{\sqrt{2}}, f = 0 \\ 1\ para\ f > 0 \end{cases}. \tag{1}$$

III. METODOLOGIA

No presente trabalho foram usadas imagens de 24 bits para a implementação da técnica de esteganografia. Em todo o processo é utilizado apenas o bit menos significativo da imagem de cobertura para se esconder os bits distintos da informação[4-5]. Neste artigo, utilizamos a imagem quadrada clown.bmp (Fig. 1a) em tons de cinza, na qual será inserida a imagem avion.bmp (Fig.1b), outra imagem quadrada em tons de cinza de mesma dimensão. A técnica consiste na substituição do bit menos significativo de cada byte da imagem de cobertura[5], por fim, recuperar a informação, e mostrar as diferença por meio de cálculo de frequências, com resultado exibido em histograma.

Calculamos a média e a variância do comportamento do conjunto de bits menos significativos. Para isso foi utilizado o software livre *Scilab*, onde foram feitos todos os códigos e cálculos. Temos por *C* uma imagem em escala de cinza de 24 bits de $Mc \times Nc$ pixels representada por:

$$C = \{x_{ij} \mid 0 \le i \le M_c, 0 \le j \le N_c, x_{ij} \in \{0,1 \ldots,255\}\}. \tag{2}$$


(a)

(b)

Fig.1. (a) A esquerda a imagem pública (imagem cobertura) e a (b) direita a imagem pública (informação).

Por *M* podemos representar a mensagem de n bits que será inserida na imagem de cobertura *C*. Suponhamos que os n bits da mensagem secreta *M* estejam inseridos nos bits menos significativos *k* da imagem de cobertura. Primeiramente a mensagem *M* é rearranjada para ser embutidos nos *k* bits da mensagem *M'*, onde esta pode ser representada por:

$$M' = \{m'_i | 0 \leq i \leq n', m'_i \in \{0,1 \dots, 2^k - 1\}\}, \quad (3)$$

onde $n' < M_c$ x N_c. O mapeamento dos n bits da mensagem secreta $M = \{m_i\}$ e da mensagem embutida pode ser definida da seguinte forma:

$$m'_i = \sum_{j=0}^{k-1} m_{i\ x\ k+j} \times 2^{k-1-j} . \quad (4)$$

Segundamente, o conjunto de *n'* pixels {*xl1*, *xl2*, ..., *xln'*} são escolhidos da imagem *C* como uma sequência pré-determinada. O processo de embutir é completado substituindo os *k* bits menos significativos de xl_i por m_i. Matematicamente, o valor do pixel xl_i escolhido é guardado nos k bits da mensagem m'_i e é modificado para a forma de estegopíxel da seguinte forma:

$$x'_{l_i} = x_{l_i} - x_{l_i} \, mod 2^k + m'_i. \quad (5)$$

e o processo reverso é dado por :

$$m'_i = x_{l_i} \, mod 2^k. \quad (6)$$

Se *xl1,xl2...xln* são os valores dos dados, então podemos escrever a média causada pela alteração dos bits menos significativos como:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_{li}}{n}. \quad (7)$$

A variância é definida como o desvio quadrático médio da média' e é calculada de uma amostra de dados como

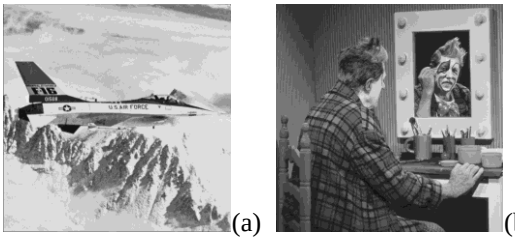
$$s^2 = \frac{\sum_{i=1}^{n} (x_{li}^2) - n\bar{x}^2}{n-1}. \quad (8)$$

IV. Resultados

Diante dos resultados, foi observado que quando fazemos a substituição dos LSB da imagem de cobertura (Fig.1a), não são gerados artefatos, sendo difícil a descoberta da existência da informação (Fig.1b). Optou-se pela escolha de uma imagem em tons de cinza, pois, imagens coloridas geram artefatos visíveis, como acontece em técnicas mais robustas, como por exemplo, filtragem e mascaramento [2].

Em relação às diferenças visíveis, a estego-imagem (Fig.2b) não possibilita a descoberta da mensagem a "olho nú", não existindo artefatos visíveis, sendo esta idêntica a imagem de cobertura. Para comprovar a precisão da técnica, foram gerados os histogramas das duas imagens (Fig.3) e destes foi feita uma subtração das diferenças, mostradas num terceiro histograma (Fig.4). Vendo o resultado dos histogramas, podemos concluir que os valores dos pixels pouco foram alterados[4].

Por último, observou-se por meio de cálculos estatísticos, que a substituição gera alterações em nível de ruído[4], sendo em média aproximadamente 0,5 e em variância 0,25 (Fig.5) para este estudo .



(a) (b)

Fig.2. A esquerda a imagem privada(a) e a direita a estego-imagem(b).

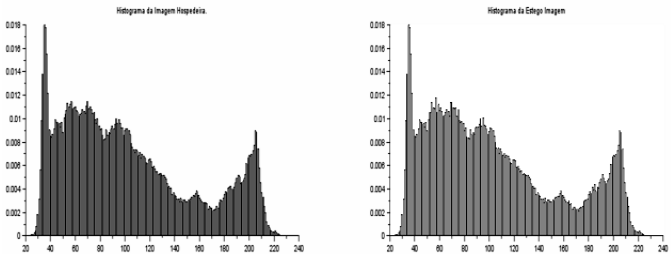


Fig.3. Histograma da imagem de cobertura e a da estego-imagem.

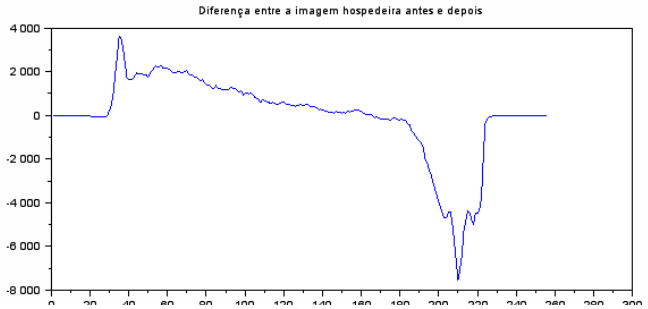


Fig.4. Histograma que mostra as diferenças entre as imagens inicial e final (estego-imagem).

```
100.

20000.    0.5040359    0.2499847
```

Fig.5. Prompt do Scilab que mostra os resultados de média e variância assinalados em vermelho.

Conclusão

Neste trabalho foi implementada uma técnica de esteganografia de imagens em tons de cinza, feitas por meio da substituição do plano LSB. Com os resultados obtidos, fica claro que não há alterações visíveis (artefatos). A técnica contribui para comunicação confidencial, impossibilitando ao atacante a descoberta da informação.

Referências

[1] E.Azevedo, J.G.Faveri, e S. E. Nunes. "Esteganografia." *Revista de Ciências Exatas e Tecnologia* 10.10, 2015.

[2] E. Julio, W. Brazil, e C. Albuquerque, Esteganografia e Suas Aplica¸cões, In: L. Pirmez, F. Delicato, (Org.), Livro de minicursos do SBSEG, 2007, p. 54-102.

[3] K. Ghazanfari, S. Ghaemmaghami, e S. Khosravi, LSB++: an improvement to LSB+ steganography, in TENCON 2011 - IEEE Region 10 Conference,2011, p. 364-368.

[4] J.R.C. Tavares e F.M.B. Junior. "Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel." *IEEE Latin America Transactions* 14.2, 2016, p1058-1064.

[5] H. Gupta, R. Kumar e S. Changlani. "Steganography using LSB bit Substitution for data hiding." *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)* 2.10 ,2013, p-676.

[6] R. Kauar, B. Singh e I. Singh. "A Comparative Study of Combination of Different Bit Positions In Image Steganography." International Journal of Modern Engineering Research 2.5, 2012.