Cripto-esteganografia: imagens inocentes podem transportar arquivos secretos

Vitor Silva Costa – Universidade Federal do Rio de Janeiro – Instituto de Matemática – Departamento de Ciência da Computação – v2costa@gmail.com

Vinícius Gusmão Pereira de Sá – Universidade Federal do Rio de Janeiro – Instituto de Matemática – Departamento de Ciência da Computação– vigusmao@dcc.ufrj.br

Introdução

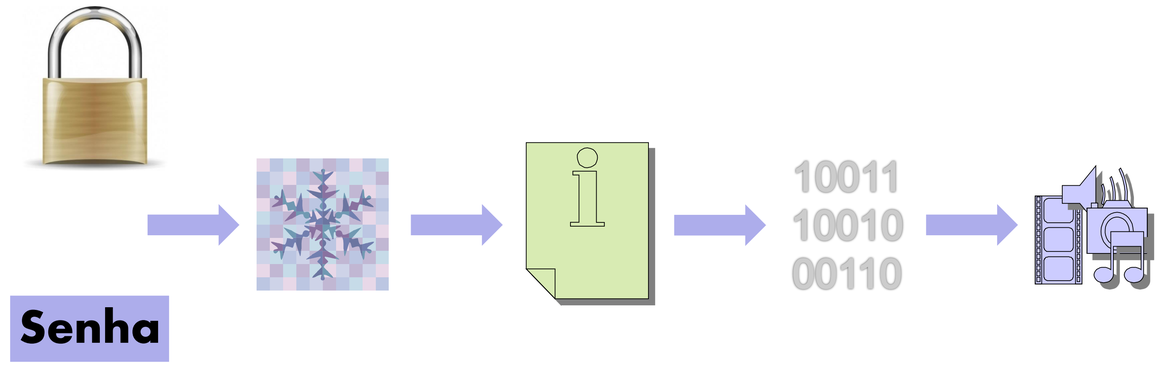
Há muito tempo se discute como armazenar ou transmitir informações confidenciais de forma segura. Essa questão é fundamental nos dias de hoje, sobretudo com a Internet servindo de meio de comunicação para os diversos fins.

Recentemente, diversos casos de quebra de privacidade colocaram o tema no centro das atenções. Esteganografia [3,5] consiste no uso de técnicas para se ocultar uma mensagem dentro de outra, que funcionará como veículo.

Este trabalho mostra não apenas como podemos guardar uma informação qualquer dentro de uma imagem, mas também como podemos deixá-la protegida através de criptografia. Alguns trabalhos correlatos foram publicados [1,4]. Nosso método, no entanto, é original e de simples implementação, podendo ser utilizado tanto para uso pessoal quanto para a troca de mensagens e arquivos entre duas partes através de uma rede insegura.

Metodologia

Recuperação dos Dados



Resultados visuais

Digamos que queremos esconder a seguinte mensagem dentro de uma imagem: “Mensagem secreta - CNMAC 2014”. Podemos observar como a alteração visual gerada na imagem é mínima na figura 1, de forma que a alteração seja imperceptível.

Figura 1: A imagem da esquerda é a original, sem qualquer informação contida dentro dela. Já a imagem da direita é a modificada, contendo nossa mensagem secreta.

Características

- É de simples implementação;
- Permite o armazenamento de arquivos de qualquer tipo;
- Permite o armazenamento de arquivos cujo tamanho, em bytes, seja menor ou igual a 3/8 do número de pixels da imagem-veículo (para uma imagem de 8 megapixels, seria possível armazenar arquivos de até 3 MB);
- O tempo de codificação/decodificação é linear no tamanho do arquivo a ser armazenado;
- É possível esconder diversos arquivos em uma mesma imagem apenas utilizando-se terminadores distintos para diferenciar “fim do arquivo corrente, com outro a seguir” (por exemplo, “000000”) e “fim do último arquivo cripto-esteganografado” (por exemplo, “111111”).

Referências

[1] M. Chroni, A. Fylakis, S. D. Nikolopoulos (2013).Watermarking Images in the Frequency Domain by Exploiting Self-Inverting Permutations. Journal of Information Security 4: 80–91.

[2] R. Durstenfeld (1964). Random permutation. Communications of the ACM 7(7): 420.

[3] N. F. Johnson, S. Jajodia (1998). Exploring Steganography: Seeing the Unseen. IEEE Computer Society, February 1998, 26–34.

[4] A. Patidar, G. Jagnade, L. Madhuri, P. Mehta, R. Seth (2012). Data Security Using Cryptosteganography in Web Application, Computer Engineering and Intelligent Systems 3(4): 74–79.

[5] N. Provos, P.Honeyman (2003). Hide and Seek: an Introduction to Steganography. IEEE Computer Society, May/June 2003, 32–44.