

Camaleão: privacidade e segurança na internet por esteganografia em imagens

Anderson Rocha¹

Siome Goldenstein¹

Heitor Costa²

Lucas Chaves²

¹ Instituto de Computação
Universidade Estadual de Campinas
{anderson.rocha, siome}@ic.unicamp.br
² Departamento de Ciência da Computação
Universidade Federal de Lavras
{heitor, lucas}@ufla.br

Abstract

A esteganografia, arte e ciência das comunicações secretas, inclui um vasto conjunto de métodos para comunicações secretas tais como tintas “invisíveis”, micro-pontos, arranjo de caracteres (*character arrangement*) entre outras. Os principais objetivos deste trabalho foram pesquisar as principais técnicas de esteganografia em imagens digitais da atualidade e desenvolver um software capaz de permitir a comunicação segura pela internet.

1. Introdução

A busca por novos meios eficientes e eficazes de proteção digital é um campo de pesquisa fundamentado nos mais variados campos da ciência.

Uma das áreas que tem recebido muita atenção recentemente é a *esteganografia*. Esta é a arte de mascarar informações como uma forma de evitar a sua detecção. *Esteganografia* deriva do grego, sendo *estegano* = *esconder*, *mascarar* e *grafia* = *escrita*. Logo, *esteganografia* é a arte da *escrita encoberta* ou, de forma mais abrangente, é a arte das comunicações encobertas [1].

A *esteganografia* inclui um vasto conjunto de métodos para comunicações secretas desenvolvidos ao longo da história. Atualmente, trabalha-se na estruturação e no desenvolvimento da *esteganografia digital*. Esta consiste em um conjunto de técnicas e algoritmos capazes de permitir uma comunicação digital mais segura em um tempo em que seus *e-mails* podem estar sendo lidos

e os seus passos em um computador pessoal rastreados.

Neste âmbito, o principal objetivo do trabalho foi aumentar a robustez das técnicas existentes. Para isso, criou-se uma nova técnica *esteganográfica*, unindo a força da cifragem de blocos do algoritmo criptográfico DES [2] e um conjunto de permutações cíclicas, às técnicas existentes.

2. Importância do trabalho desenvolvido

Juntamente com a *criptografia*, a *esteganografia* apresenta-se como uma tecnologia apta a auxiliar as pessoas a aumentarem sua privacidade *on-line*. No entanto, este alto grau de sigilo preocupa as autoridades políticas e policiais. Segundo [3], muitas propostas de controle de privacidade já existem ou estão em andamento tais como: PATRIOT¹, Carnivore², DMCA³, CAPPS II⁴, entre outros.

Contudo, tem-se uma visão deturpada de que segurança e privacidade são termos antagônicos. Isto é, caso as pessoas não possam ser vigiadas, elas representam perigo ou para outras pessoas ou para o país.

Poucos sabem, mas grande parte do conteúdo em circulação pela *Internet* é constantemente vigiado pelo projeto *Echelon*. Este projeto visa filtrar toda a informação em circulação pela *internet* em busca de terroristas. O projeto existe em uma associação dos países EUA,

¹ Provide Appropriate Tools Required to Intercept and Obstruct Terrorism.

² Programa do FBI para vigiar o correio eletrônico.

³ Digital Milenium Copyright Act

⁴ Computer Assisted Passenger Pre-Screening System

Reino Unido, Austrália e Canadá. Outro projeto não menos relevante é o *UKUSA*. O termo é uma justaposição das siglas UK (*United Kingdom*) e USA (*United States of America*). Este projeto visa filtrar toda e qualquer informação em nome da segurança nacional dos países envolvidos. O *Echelon* e o *UKUSA* são dois atentados contra a liberdade de expressão dos cidadãos.

3. Resultados e implementação

Ao longo deste trabalho, foi desenvolvido o *Camaleão*⁵: um software para proteção digital utilizando esteganografia que permite a comunicação segura pela internet por fazer uso da esteganografia.

3.1 Robustez do software

A robustez da solução implementada se deve a três fatores: as senhas ou chaves de deslocamento, as permutações cíclicas entre os blocos e a cifragem interna dos blocos que podem ocorrer na mensagem antes do mascaramento.

3.1.1 As senhas

A senha, ou chave de deslocamento, é uma seqüência numérica de tamanho n . Os elementos pertencentes à chave estão mapeados no intervalo $\{0, \dots, m\}$ sendo m um valor máximo. O valor m é dado a partir do módulo k em que se deseja criar a chave. Exemplo: Seja C uma chave de tamanho $n = 5$ e módulo $k = 3$. Cada elemento de C será um número inteiro pertencente ao intervalo $\{0, 1, 2\}$. A chave é criada a partir de um gerador pseudo-aleatório de números.

3.1.2 Cifragem de blocos e permutações cíclicas

Os autores desenvolveram uma abordagem chamada *cifragem por blocos com permutações cíclicas*. O processo é apresentado na Figura 1.

A mensagem a ser escondida é dividida em N blocos de tamanho fixo. A partir desse momento, os N blocos são independentemente criptografados com o algoritmo DES usando como chave simétrica a chave de deslocamento gerada. Isto produz N blocos criptografados C . Os blocos C são então permutados entre si ciclicamente de acordo com a chave de deslocamento. Em seguida, mais um processo de *criptografia* é feito internamente em cada bloco. Desta vez, o processo de *criptografia* é feito através de permutações cíclicas. O

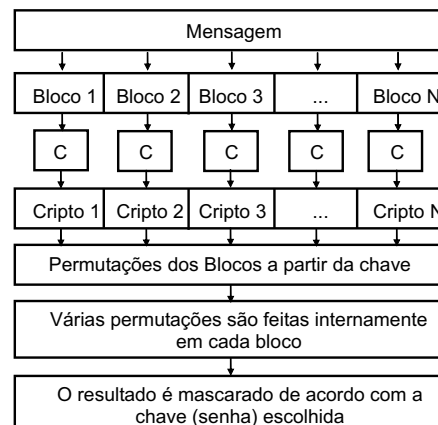


Figura 1: Exemplo de ocultamento de uma mensagem

conjunto de *bits* resultante de todas estas operações é então escondido na imagem de cobertura a partir da chave de deslocamento gerada. Todo este processo é feito de modo a manter a *estego-imagem* resultante estatisticamente o mais próximo possível da imagem original.

4. Considerações finais

Este artigo apresentou as principais técnicas de mascaramento, em especial, mascaramento em imagens. Foi mostrado o método de mascaramento de dados em imagens baseado na cifragem de blocos e permutações cíclicas que foi utilizado na implementação feita.

A *esteganografia*, quando bem utilizada, fornece meios eficientes e eficazes na busca por proteção digital. Associando *criptografia* e *esteganografia*, como solução implementada, as pessoas têm o poder de comunicar-se em segredo pela internet mantendo sua identidade íntegra e secreta tendo mais uma opção para exercerem seu direito à liberdade e privacidade.

Referências

- [1] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - a survey," in *Proceedings of IEEE*, July 1999, pp. 1062–1078, special issue on Protection on multimedia content.
- [2] B. Schneier, *Applied Cryptography*. New York: John Wiley & Sons, 1995, ISBN 0-47111-709-9.
- [3] EFF, "EFF – The Electronic Frontier Foundation," Disponível em www.eff.org, 2003, Último acesso em 10 de agosto de 2004.

⁵Disponível em <http://andersonrocha.cjb.net>