Camaleão: um Software para Segurança Digital Utilizando Esteganografia*

Anderson de Rezende Rocha[1], **Heitor Augustus Xavier Costa (Orientador)**[2], **Lucas Monteiro Chaves (Co-orientador)**[2]

[1]Instituto de Computação
Universidade Estadual de Campinas (Unicamp)
Caixa Postal 6176 – CEP 13084-971, Campinas, SP

anderson.rocha@ic.unicamp.br

[2]Depto. de Ciência da Computação e Depto. de Ciências Exatas
Universidade Federal de Lavras (UFLA)
Caixa Postal 37 – CEP 37200-000, Lavras, MG

{heitor, lucas}@ufla.br

Abstract. *Digital protection is a research area which needs efficient ways to make it possible. The steganography is configured as one of these electronic protection ways. It includes a set of methods for private communications such as invisible inks, micro-dots, character arrangement, digital signatures, covert channels and spread spectrum communications. Therefore, the main objective of work this is to develop a software that allows security communication on the internet by using steganographic techniques in digital images.*

Resumo. *A busca por novos meios eficientes e eficazes de proteção digital é um campo de pesquisas fundamentado nas mais variadas áreas da ciência. A* esteganografia *configura-se como uma destes meios de proteção. Inclui um vasto conjunto de métodos para comunicações secretas tais como tintas "invisíveis", micro-pontos, arranjo de caracteres (character arrangement), assinaturas digitais, canais escondidos (covert channels), comunicações por espalhamento de espectro (spread spectrum communications), entre outras. Neste âmbito, o principal objetivo deste trabalho foi desenvolver um produto de software capaz de permitir a comunicação segura pela internet por fazer uso de técnicas esteganográficas em imagens digitais.*

1. Introdução

A busca por novos meios eficientes e eficazes de proteção digital é um campo de pesquisas fundamentado nas mais variadas áreas da ciência. Basicamente, tem-se duas ramificações. De um lado, estão aqueles que buscam técnicas para obter maior proteção digital. Do

*Financiado pelo PIBIC com registro número 105133/2001-9 no Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

outro lado, estão aqueles que querem minar a proteção, isto é, querem ter acesso à informação sem autorização.

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, donde *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 [Popa, 1998].

A *esteganografia* inclui um vasto conjunto de métodos desenvolvidos ao longo da história. Dentre tais métodos estão: tintas "invisíveis", micro-pontos, arranjo de caracteres (*character arrangement*), assinaturas digitais, canais escondidos (*covert channels*), comunicações por espalhamento de espectro (*spread spectrum communications*) entre outras.

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 *e-mails* podem estar sendo lidos e computadores pessoais rastreados. Estas técnicas podem variar desde a inserção de imagens em outras — fazendo com que uma imagem aparentemente inocente esconda outra com maior importância sem levantar suspeitas — até a escrita de textos inócuos que escondem algum texto secreto em sua estrutura. Tais técnicas também estão presentes nos modernos equipamentos militares que fazem transmissões de rádio e codificam em ondas-curtas mensagens mais importantes.

Este súbito interesse pela *esteganografia* deve-se, também, à busca por técnicas de *copyright* eficientes e eficazes. A partir do momento em que áudio, vídeo e outras formas de comunicação de mensagens tornaram-se disponíveis em formatos digitais, a facilidade com que qualquer um destes possa ser perfeitamente copiado aumentou significativamente. Isto está levando a uma imensa quantidade de reproduções não autorizadas pelo mundo todo. Como contra-medidas, técnicas avançadas de "marcas-d'água" (*watermarking*) ou mesmo técnicas de identificação por digitais (*fingerprinting*), estruturadas na *esteganografia*, buscam restringir a pirataria indiscriminada.

O objetivo do trabalho foi analisar e implementar algumas técnicas *esteganográfico-digitais* como futuras ferramentas didáticas. Deste modo, quaisquer interessados poderão ter um conhecimento ilustrado desta nova área.

A seguir, é apresentada uma descrição sucinta das seções deste artigo. A seção 2 apresenta os principais termos utilizados. A seção 3 mostra uma retrospectiva da *esteganografia* desde os seus primórdios até os dias atuais. Em seguida, a seção 4 apresenta as principais técnicas *esteganográficas* da atualidade e algumas perspectivas de robustez. A seção 5 apresenta os resultados desta pesquisa em relação ao campo da *esteganografia*. A seção 6 apresenta algumas propostas de trabalhos futuros. Finalmente, a seção 7 mostra as principais conclusões referentes ao trabalho.

2. Terminologia

Segundo [Petitcolas et al., 1999], o modelo geral de ocultamento de dados (*information hiding*) pode ser descrito como se segue. O dado embutido (*embedded data*) é a men-

sagem que se deseja enviar de maneira secreta. Freqüentemente, este dado é escondido em uma mensagem inócua (sem maior importância) conhecida como mensagem de cobertura (*cover-message*). As mensagens de cobertura podem variar de nome de acordo com o meio de cobertura sendo utilizado. Deste modo, pode-se definir uma imagem de cobertura (*cover-image*), áudio de cobertura (*cover-audio*) ou texto de cobertura (*cover-text*). Após o processo de inserção dos dados na mensagem de cobertura, obtém-se o chamado estego-objeto (*stego-object*), uma mensagem inócua contendo secretamente uma mensagem de maior importância. A figura 1 apresenta como o processo pode ser interpretado. Um indivíduo escolhe o dado a ser escondido e, a partir de uma chave, mascara estes dados em uma imagem de cobertura previamente selecionada. O resultado é a estego-imagem a ser enviada.

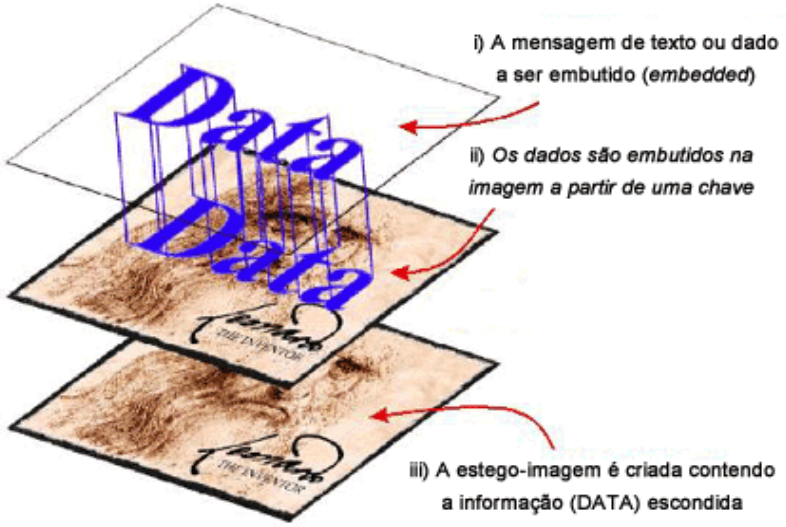

Figura 1: Exemplo de ocultamento de uma mensagem

Uma estego-chave (*stego-key*) é utilizada para controlar o processo de ocultamento de forma a restringir a detecção e/ou recuperação dos dados do material embutido.

3. Análise histórica

Através de toda a história, as pessoas têm tentado inúmeras formas de esconder informações dentro de outros meios, buscando, de alguma forma, mais privacidade para seus meios de comunicação. Duas excelentes fontes podem ser encontradas em [Kuhn, 1996] e [Norman, 1980].

Segundo [Petitcolas et al., 1999], um dos primeiros registros sobre *esteganografia* aparece em algumas descrições de Heródoto, o pai da História, com vários casos sobre sua utilização. Um deles conta que um homem, de nome Harpagus, matou uma lebre e escondeu uma mensagem em suas entranhas. Em seguida, ele enviou a lebre através de seu mensageiro que se passou por um caçador.

Em outro caso, no século V AC, um grego de nome Histaieus, a fim de encorajar Aristágoras de Mileto e seus compatriotas a começar uma revolta contra Medes e os Persas, raspou a cabeça de um de seus escravos mais confiáveis e tatuou uma mensagem

em sua cabeça. Assim que os seus cabelos cresceram, o escravo foi enviado à Grécia com instruções de raspar sua cabeça permitindo aos seus amigos receberem a mensagem [Petitcolas et al., 1999].

Outra técnica interessante que aparece durante a História faz uso de inúmeras variações de tintas "invisíveis" (*invisible inks*). Tais tintas não são novidades e já apareciam em relatos de Plínio, o Velho, e Ovídio no século I DC. Ovídio, em sua *Arte do amor*, propusera o uso do leite para escrita de textos "invisíveis". Para decodificar a mensagem, o receptor deveria borrifar o papel com ferrugem ou carbono negro. Estas substâncias aderiam ao leite e a mensagem era revelada [Kuhn, 1996] e [Kahn, 1996].

Na segunda guerra mundial, com um sucessivo aumento na qualidade das câmeras, lentes e filmes, tornou-se possível, aos espiões nazistas, a criação de uma das formas mais interessantes e engenhosas de comunicação secreta. As mensagens nazistas eram fotografadas e, posteriormente, reduzidas ao tamanho de pontos finais (**.**) em uma sentença. Assim, uma nova mensagem totalmente inocente era escrita contendo o filme ultra-reduzido como final das sentenças. A mensagem gerada era enviada sem levantar maiores suspeitas. Esta engenhosidade ficou conhecida como *tecnologia do micro-ponto* [Singh, 2001].

Atualmente, a *esteganografia* não foi esquecida. Ela foi modificada em sinal de acompanhamento dos novos tempos. Na era da informação, não faz mais sentido "tatuar" textos em cabeças de escravos ou mesmo borrifar pontos em uma revista através da utilização de tintas "invisíveis". Qualquer meio de *esteganografia* na atualidade, inevitavelmente, deve utilizar meios contemporâneos de tecnologia. Embora, em alguns casos, estes meios sejam apenas aperfeiçoamentos de técnicas clássicas.

Neste sentido, várias pesquisas têm sido feitas no campo da *esteganografia digital*. Existe um grande número de documentos digitais disponíveis na *internet*. E, em muitas ocasiões, as pessoas desejam trocar informações de forma rápida e segura. De acordo com [Kumagai, 2003], [Cass, 2003] e [Wallich, 2003], acontecimentos recentes, como o atentado terrorista ao *World Trade Center* em 11 de setembro de 2001, fizeram com que as autoridades passassem a "vigiar" tudo o que circula de forma criptografada ou não pela grande rede. Isto quer dizer que, se antes uma mensagem criptografada poderia passar despercebida, agora ela pode ser interpretada como uma mensagem de alguém suspeito que tem algo a esconder. Em meio a toda esta paranóia, a *esteganografia* vem ganhando grande destaque e conquistando seu espaço.

Outra razão pela qual a *esteganografia digital* vem ganhando destaque na mídia deve-se aos estudos de *copyright* e *watermarking* de documentos eletrônicos. À medida que aumenta a pirataria pela rede mundial de computadores, novos meios mais eficientes e eficazes de proteção intelectual são estudados no intuito de conter as cópias não-autorizadas.

4. Técnicas esteganográficas

De acordo com [Popa, 1998], os principais algoritmos de *esteganografia digital* são baseados na substituição de componentes de ruído de um objeto digital por uma mensagem secreta pseudo-randômica.

Após o processo de embutir os dados, o estego-objeto gerado pode ser dividido em duas classes. Este pode ser um *stream cover* ou um *random access cover*. O primeiro é formado por uma seqüência (*stream*) de dados contínuos como, por exemplo, uma transmissão telefônica. O último pode ser um arquivo do formato ".WAV" [Aura, 1996].

Comparativamente, tem-se que, utilizando-se técnicas de geração de *stream-covers*, não se pode identificar os tamanhos dos dados escondidos nem onde estes começam ou terminam no objeto de cobertura. A sua geração é feita a partir de um *keystream generator*, algo como uma chave de *criptografia* que diz em que ordem os bits devem ser inseridos e recuperados. Esta técnica é conhecida como *método do intervalo randômico* [Popa, 1998].

Por outro lado, os arquivos classificados como *random access cover* permitem ao emissor da mensagem colocar os dados em qualquer ordem no objeto de cobertura, assim como é possível conhecer onde é o início e o fim da mensagem escondida.

Freqüentemente, os *bits* de cobertura são os menos significativos (*LSB — least significant bits*) do objeto de cobertura. Segundo [Popa, 1998], os *bits* menos significativos têm algumas propriedades estatísticas como a entropia e o histograma. Mudanças em algumas destas propriedades poderiam resultar em perdas na qualidade do objeto de cobertura utilizado. Deste modo, a mensagem escondida precisaria "imitar", com grande estilo, os *bits* do objeto de cobertura. Uma possibilidade é gerar vários objetos de cobertura e, então, selecionar aquele com menor variação nas propriedades estatísticas dos *bits* menos significativos. Esta técnica é conhecida como *método da seleção* [Popa, 1998]. Outra possibilidade é gerar uma função chamada imitadora. Tal função teria o objetivo de modificar os *bits* da mensagem a ser escondida de forma que estes tenham a forma mais próxima possível dos *bits* do objeto de cobertura. Esta técnica é conhecida como *método construtivo* [Popa, 1998].

As abordagens mais comuns de inserção de mensagens em imagens incluem técnicas de:

- inserção no *bit* menos significativo;
- técnicas de filtragem e mascaramento;
- algoritmos e transformações.

Cada uma destas pode ser aplicada às imagens, com graus variados de sucesso. O método de inserção no *bit* menos significativo é provavelmente uma das melhores técnicas de *esteganografia* em imagem.

4.1. Inserção no bit menos significativo

Técnicas baseadas em LSB podem ser aplicadas a cada *byte* de uma imagem de 32-*bits*. Estas imagens possuem cada *pixel* codificado em quatro *bytes*. Um para o canal alfa (*alpha transparency*), outro para o canal vermelho (*red*), outro para o canal verde (*green*) e outro para o canal azul (*blue*). Seguramente, pode-se selecionar um *bit* (o menos significativo) em cada *byte* do *pixel* para representar o *bit* a ser escondido sem causar alterações perceptíveis na imagem [Wayner, 2002], [Popa, 1998], [Petitcolas et al., 1999].

Acompanhe o exemplo da figura 2 para entender melhor. Suponha que se deseja esconder a letra **E** dentro da porção de imagem.

Figura 2: Porção de uma imagem de cobertura

Na figura 2, têm-se três *pixels* da imagem de cobertura. Como a letra **E** pode ser escrita em forma binária segundo seu código ASCII como **10000011**, é suficiente utilizar apenas os dois primeiros *pixels* da imagem. Assim, utilizando-se a técnica LSB, tem-se o resultado mostrado na figura 3

Figura 3: Porção da estego-imagem gerada pela porção de imagem 2

Os *bits* em negrito representam os LSBs e os *bits* sublinhados representam as modificações necessárias para esconder a letra **E**.

4.2. Técnicas de filtragem e mascaramento

Segundo [Johnson and Jajodia, 1998], técnicas de *filtragem e mascaramento* são restritas às imagens em tons de cinza (*grayscale*). Estas técnicas escondem a informação através da criação de uma imagem semelhante às marcações de *copyright* em papel. Isto acontece porque as técnicas de *watermarking* garantem que, mesmo se a imagem for modificada por métodos de compressão, a marcação não será removida.

Filtragem e mascaramento são técnicas mais robustas que a inserção LSB no sentido de gerarem estego-imagens imunes a técnicas de compressão e recorte. Ao contrário das modificações LSB, filtragem e mascaramento trabalham com modificações nos *bits mais significativos* das imagens. As imagens de cobertura devem ser em tons de cinza porque estas técnicas não são eficientes em imagens coloridas [Popa, 1998]. Isto deve-se ao fato de que modificações em *bits* mais significativos de imagens em cores geram alta quantidade de "ruído" tornando as informações detectáveis.

4.3. Algoritmos e transformações

Manipulações LSB são rápidas e relativamente fáceis de serem implementadas. No entanto, estas técnicas produzem estego-imagens que podem ser facilmente destruídas através do manuseio da imagem com recorte e/ou compressão [Artz, 2001].

Por outro lado, sabe-se que a compressão de imagens é uma das formas mais eficientes de armazenar imagens de alta qualidade. Desta forma, os algoritmos de transformação geralmente trabalham com formas mais sofisticadas de manuseio de imagens como brilho, saturação e compressão das imagens.

Utilizando técnicas como a *transformação discreta do cosseno*, *transformada discreta de Fourier* e *transformada Z*, entre outras, estes algoritmos tomam como aliado o principal inimigo da inserção LSB: a compressão. Por isso, configuram-se como as mais sofisticadas técnicas de mascaramento de informações em imagens conhecidas [Johnson and Jajodia, 1998] e [Popa, 1998].

5. A ferramenta desenvolvida e os resultados

Como resultado desta pesquisa, foi desenvolvido o *Camaleão: um software para proteção digital utilizando esteganografia* [1].

Camaleão é um *software* que permite a comunicação segura pela *internet* por fazer uso da *esteganografia*. O produto possui várias características tais como:

- *ambiente multiplataforma:* por ter sido desenvolvido na linguagem de programação Java [Sun Microsystems, 2003], o funcionamento do **Camaleão** torna-se praticamente independente do sistema operacional utilizado. O sistema funcionou bem sobre os sistemas operacionais Linux, Windows 9x, Windows XP e Mac OS X. Embora não testado, o **Camaleão** provavelmente funcionará sem problemas sobre o sistema Solaris. Para isso, o usuário deve ter em seu computador a máquina virtual java (JVM – *Java Virtual Machine*) 1.4 ou superior;
- *ambiente bilíngue:* Visando alcançar o maior número de pessoas, o **Camaleão** foi desenvolvido em dois idiomas. O idioma português que funciona em modo nativo e o idioma inglês que funciona como opcional;
- *código aberto:* o **Camaleão** é disponibilizado sob a licença de uso GPL (*General Public GNU Licence*) ou licença pública geral GNU [FSF, 2003]. De acordo com esta licença, o **Camaleão** pode ser modificado e utilizado livremente desde que se mantenha as referências aos autores originais intactas;
- *tipos de mascaramento e recuperação:* o **Camaleão** permite o mascaramento de textos, imagens e quaisquer outros arquivos binários dentro de outras imagens. As imagens de cobertura podem ser de sufixo (extensão) *.jpg* ou *.png*. A imagem de saída (contendo o mascaramento) tem o sufixo *.png*. O processo de mascaramento pode ser baseado em chave de deslocamento ou a partir das configurações-padrão. Caso seja baseado em chave de deslocamento, esta pode ser periódica ou não[2]. Além disso, o mascaramento pode ser linear ou aleatório;
- *robustez:* visando ter uma maior segurança, o sistema permite a geração de chaves de deslocamento configuráveis. É possível gerar chaves de vários tamanhos diferentes sob vários módulos diferentes[3].

As figuras 4 e 5 apresentam algumas telas do ferramenta de *software* desenvolvida.

As imagens produzidas após o processo de mascaramento são praticamente idênticas. Os humanos conseguem capturar mudanças em uma imagem quando estas ocorrem em um fator acima de 3% [Wayner, 2002]. No caso, como o **Camaleão** trabalha apenas com o *bit* menos significativo, o conjunto total de mudanças em uma mensagem que afete todos os LSBs é de apenas $0{,}75\%$ — dado que cada componente de cor tem 8 *bits* a alteração no último *bit* afeta o conjunto em $\frac{2}{256}\%$ —. Caso o segundo *bit* menos significativo também seja alterado, a taxa de alteração sobe para $1{,}56\%$, ainda imperceptível à maioria dos seres humanos [Wayner, 2002].

[1] Vide [Rocha, 2003] para informações adicionais.

[2] De forma geral, para cada entrada (*bit*) de uma mensagem a ser mascarada existe uma entrada (*deslocamento*) respectivo na chave de deslocamento. Chaves periódicas possuem menos entradas que a mensagem a ser mascarada. Assim que acabam as entradas da chave, usa-se novamente as mesmas entradas. Por outro lado, chaves não-periódicas têm o número de entradas maior ou igual ao número de entradas da mensagem a ser escondida.

[3] Chaves de módulo k têm todas as suas entradas menores que k.

Figura 4: Tela inicial do sistema

Figura 5: Mascaramento de um texto

A figura 6 é uma imagem antes de um mascaramento. Seu tamanho é de 133,2 KB. A figura 7, de 134KB, apresenta a estego-imagem resultante em que 35% dos seus LSBs foram alterados pelo processo de mascaramento feito pelo **Camaleão**. Elas são praticamente idênticas.

A discrepância no tamanho final das imagens não é relevante dado que apenas a imagem resultante será enviada ao destinatário. Caso um interceptador capture a estego-imagem antes que ela chegue ao seu destino, ele não terá como comparar os tamanhos dado que ele não possui a imagem original.

Figura 6: Imagem antes do mascaramento – 133,2KB

Figura 7: Imagem após o mascaramento – 134,0KB

5.1. O processo de mascaramento da informação

Neste processo, os *bits* menos significativos de uma imagem de cobertura são alterados segundo as configurações dos *bits* de um segundo arquivo. Este segundo arquivo é a mensagem que se deseja enviar em segredo.

A distância entre dois sucessivos *bits* escondidos é o número de *bits* menos significativos entre eles e é controlado por um número aleatório. Tais distâncias pertencem ao intervalo $\{0, \ldots, m\}$, onde m denota um valor máximo, e é um segredo entre o emissor e o receptor. Esta chave corresponde a uma chave simétrica em um *criptosistema* simétrico. Sem o conhecimento da sucessão correta de distâncias entre os *bits*, qualquer agressor terá poucas chances de êxito ao tentar recuperar a mensagem escondida.

A figura 8 descreve o processo de mascaramento. O emissor modifica o *stream* original usando a chave secreta. Caso não exista uma chave de deslocamento, o **Camaleão** efetua o mascaramento segundo as configurações-padrão, isto é, simulando um deslocamento de 1 para todo *bit* a ser mascarado. Para mascarar o primeiro *bit* o emissor precisa saber quantos *bits* deve saltar. No primeiro caso, deve-se saltar um *bit* dado que o deslocamento é zero. Deste modo, basta saltar do LSB atual para o próximo e efetuar o

mascaramento. No entanto, caso o deslocamento seja de dois deve-se contar três LSBs a partir do LSB sendo atualmente utilizado e efetuar o mascaramento.

Stream original	*Stream* a ser mascarado	Chave (distâncias)	*Stream* a ser enviado
00110110	0	0	00110110
00100111	1	0	00100110
10100000	1	2	10100000
10101001	0	0	10101001
00000010	0	1	00000010
10111010	.	.	10111011
00011100	.	.	00011100
01111110	.	.	01111110
01000101	.	.	01000101
11100011	.	.	11100011
10000001	.	.	10000001

Figura 8: O processo de mascaramento segundo uma chave de deslocamento

5.2. O processo de recuperação da informação

Neste processo, os *bits* menos significativos de uma imagem de cobertura são todos extraídos e colocados em uma lista. Os *bits* serão posteriormente selecionados para a formação da mensagem final segundo as configurações da chave de deslocamento que está em posse do receptor da mensagem.

A figura 9 descreve o processo de recuperação. O receptor captura os *bits* certos a partir dos deslocamentos da chave. Isto quer dizer que, para recuperar o primeiro *bit* o receptor verifica o deslocamento relativo na chave. Como a primeira entrada da chave é zero, o segundo LSB da tabela contém um *bit* a ser recuperado. O deslocamento para o terceiro *bit* a ser recuperado também é zero, logo o segundo LSB também contém um *bit* válido. No entanto, o terceiro *bit* a ser recuperado está no sexto LSB dado que o último LSB utilizado foi o terceiro e o deslocamento relativo ao terceiro *bit* válido é de 2.

6. Trabalhos futuros

O campo de pesquisas em *esteganografia digital* está em constante evolução. As técnicas são constantemente inovadas. Neste sentido, apresentam-se a seguir algumas melhorias que poderiam ser desenvolvidas e adequadas ao **Camaleão**.

6.1. Códigos corretores de erros

Um dos grandes problemas da *esteganografia* em imagens consiste em recuperar a mensagem escondida após um ataque geométrico[4] à estego-imagem. Uma das saídas possíveis

[4]Por ataque geométrico entende-se qualquer tentativa de modificar a estrutura da imagem. Alguns ataques conhecidos podem ser giro, deslocamento, limiarização, adição de ruído, filtragem entre outros.

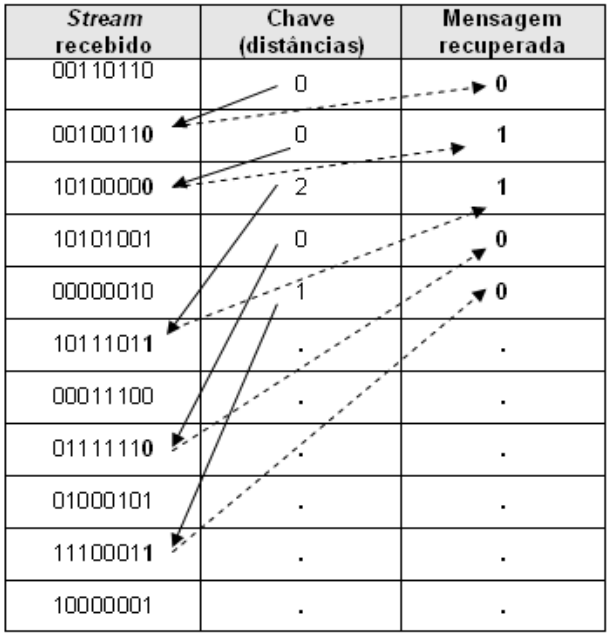

Figura 9: O processo de recuperação segundo uma chave de deslocamento

é aplicar códigos corretores de erro que possibilitem a recuperação da mensagem sem a necessidade de todos os *bits* estarem presentes no lado receptor. Dado que alguns *bits* tenham sido perdidos durante o ataque geométrico, é possível tirar certas conclusões a partir dos códigos corretores.

6.2. Criptografia

Um sistema *esteganográfico* torna-se bastante seguro se associado à *criptografia*. O processo é demonstrado na figura 10.

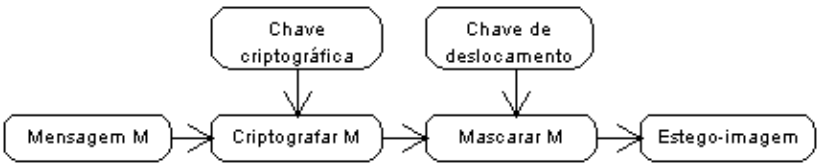

Figura 10: Associando a *criptografia* e a *esteganografia*

Uma mensagem, antes de ser mascarada, é criptografada segundo uma chave. Logo após, a partir de uma chave de deslocamento, escolhe-se os *bits* menos significativos (LSBs) que devem ser alterados na imagem de cobertura. Propõe-se a utilização da *criptografia* como um passo adicional antes de efetuar o mascaramento das mensagens na ferramenta desenvolvida.

6.3. Padrões estatísticos da imagem de cobertura

A análise estatística é um dos pilares da *esteganálise*. Uma das maneiras de aumentar a robustez do sistema desenvolvido é implementar uma função de imitação (*mimicry function*) responsável por analisar a imagem de cobertura, armazenar seus padrões estatísticos

e mascarar a mensagem a partir dos padrões descobertos. Desta forma, após o mascaramento, a imagem produzida tem seus padrões estatísticos pouco alterados. Isto torna a estego-imagem altamente capaz de sobrepujar ataques estatísticos.

6.4. Mascaramento de sons

Todas as técnicas implementadas trabalham com arquivos de imagens. Poderi-se-ia estender o **Camaleão** de modo a adaptá-lo para mascarar mensagens em arquivos de sons. Visto que o funcionamento de um arquivo de som é muito parecido com um arquivo de imagem, esta proposta não é tão complexa quanto possa parecer. Caso isso seja feito, as mensagens mascaradas poderiam ser maiores, uma vez que os arquivos de sons são, na maioria dos casos, maiores que arquivos de imagens.

7. Conclusões

Este artigo apresentou a evolução da *esteganografia* ao longo da história e suas aplicações modernas com a chamada *esteganografia digital*. Foram mostradas as principais técnicas de mascaramento e, em especial, mascaramento em imagens. Também foi mostrada a ferramenta *Camaleão: um software para segurança digital utilizando esteganografia* desenvolvido durante o trabalho. Finalmente, fez-se uma análise das estego-imagens produzidas pela ferramenta segundo o método de esteganálise proposto por [Fridrich et al., 2001].

A esteganografia, quando bem utilizada, fornece meios eficientes e eficazes na busca por proteção digital. Associando *criptografia* e *esteganografia*, as pessoas têm em mãos o poder de comunicar-se em segredo pela rede mundial de computadores mantendo suas identidades íntegras e secretas. Obviamente, a privacidade pode ser aproveitada com fins ilícitos. No entanto, o papel dos autores deste trabalho, enquanto cientistas, é fazer ciência para ajudar a sociedade. Dependerá da sociedade saber aplicar o conhecimento da forma correta.

Referências

[Artz, 2001] Artz, D. (2001). Digital steganography: hiding data within data. In *IEEE Internet Computing*.

[Aura, 1996] Aura, T. (1996). Practical invisibility in digital communication. In *HUT Seminar on Network Security*. Helsink Univerisity of Technology.

[Cass, 2003] Cass, S. (2003). Listening in. In *IEEE Spectrum*, volume 40, pages 32–37.

[Fridrich et al., 2001] Fridrich, J., Goljan, M., and Du, R. (2001). Detecting lsb steganography in color and grayscale images. In *IEEE Proceeding on Multimedia and Security*. IEEE Multimedia.

[FSF, 2003] FSF (2003). FSF – free software foundation. Disponível em `www.fsf.org`.

[Johnson and Jajodia, 1998] Johnson, N. and Jajodia, S. (1998). Exploring steganography: seeing the unseen. In *IEEE Internet Computing*.

[Kahn, 1996] Kahn, D. (1996). *The CODEBREAKERS: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, Boston. ISBN 0-68483-130-9.

[Kuhn, 1996] Kuhn, M. G. (1996). The history of steganography. In *Proceedings of the First International Information-Hiding Workshop*. Springer–Verlag, Berlim.

[Kumagai, 2003] Kumagai, J. (2003). Mission impossible? In *IEEE Spectrum*, volume 40, pages 26–31.

[Sun Microsystems, 2003] Sun Microsystems (2003). The java documentation. Disponível em `java.sun.com`.

[Norman, 1980] Norman, B. (1980). *Secret warfare, the battle of Codes and Ciphers*. Acropolis Books Inc.

[Petitcolas et al., 1999] Petitcolas, F. A., Anderson, R. J., and Kuhn, M. G. (1999). Information hiding - a survey. In *Proceedings of IEEE*. Special issue on Protection on multimedia content.

[Popa, 1998] Popa, R. (1998). An analysis of steganography techniques. Master's thesis, Department of Computer Science and Software Engineering of The "Polytechnic" University of Timisoara, Timisoara, Romênia.

[Rocha, 2003] Rocha, A. R. (2003). Camaleão: um software para segurança digital utilizando esteganografia. In *Monografia de final de curso*. Universidade Federal de Lavras – Departamento de Ciência da Computação. *Disponível em http://andersonrocha.cjb.net*.

[Singh, 2001] Singh, S. (2001). *O livro dos códigos*. Record, Rio de Janeiro. ISBN 8-50105-598-0.

[Wallich, 2003] Wallich, P. (2003). Getting the message. In *IEEE Spectrum*, volume 40, pages 38–43.

[Wayner, 2002] Wayner, P. (2002). *Disappearing cryptography*. Morgan Kaufmann Publishers, San Francisco. ISBN 1-55860-769-2.