ANDERSON DE REZENDE ROCHA

DESENVOLVIMENTO DE UM SOFTWARE PARA SEGURANÇA DIGITAL UTILIZANDO ESTEGANOGRAFIA

Pré-projeto apresentado ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da disciplina Projeto Orientado I.

Orientador
Prof. Heitor Augustus Xavier Costa

Co-Orientador
Prof. Lucas Monteiro Chaves

Lavras
Minas Gerais - Brasil
2003

ANDERSON DE REZENDE ROCHA

DESENVOLVIMENTO DE UM SOFTWARE PARA SEGURANÇA DIGITAL UTILIZANDO ESTEGANOGRAFIA

Pré-projeto apresentado ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da disciplina Projeto Orientado I.

Prof. Heitor Augustus Xavier Costa
(Orientador)

Prof. Lucas Monteiro Chaves
(Co-Orientador)

Lavras
Minas Gerais - Brasil

Sumário

Lista de Figuras

Resumo

A busca por novos meios eficientes e eficazes de proteção digital é um campo de pesquisas fundamentado nos mais variados campos 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 arranjement*), assinaturas digitais, canais escondidos (*covert channels*), comunicações por espalhamento de espectro (*spread spectrum communications*) entre outras. Neste âmbito, o principal objetivo deste trabalho é desenvolver um produto de *software* onde será possível acompanhar o funcionamento de algumas técnicas *esteganográficas*.

Abstract

Digital protection is a research area which needs efficient ways to make it possible. The *steganography* is configured as one of these eletronic protection way. It includes a set of methods for private communications such as *invisible inks*, *micro-dots*, *character arranjement*, *digital signatures*, *covert channels* and *spread spectrum communications*. So, main objective of work is to develop a software which will allow to know some *steganografic* techniques.

Capítulo 1

Introdução

A busca por novos meios eficientes e eficazes de proteção digital é um campo de pesquisas fundamentado nos mais variados campos da ciência. Basicamente, este campo de pesquisa se divide em duas ramificações. De um lado, estão aqueles que buscam técnicas para se obter maior proteção digital. Do outro lado, estão aqueles que querem minar a proteção, i.e., 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. Segundo [Popa, 1998], *esteganografia* deriva do grego, donde *estegano = esconder, mascarar* e *grafia = escrita*. Logo, *esteganografia* é a arte da *escrita encoberta*.

A *esteganografia* inclui um vasto conjunto de métodos para comunicações secretas desenvolvidos ao longo da história. Dentre tais métodos estão: tintas "invisíveis", micro-pontos, arranjo de caracteres (*character arranjement*), 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 seus *e-mails* podem estar sendo lidos e os seus passos em um computador pessoal 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 pudesse ser perfeitamente copiado aumentou exponencialmente. Isto está levando a uma imensa quantidade de reproduções destas formas de comunicação de mensagens não autorizadas pelo mundo todo. Como contra-medidas, técnicas avançadas de "marcas-d'água" (*watermarking*), ou mesmo técnicas de seriação (*fingerprinting*), estruturadas na *esteganografia* buscam restringir a pirataria indiscriminada.

A proposta do trabalho é estudar as principais técnicas de *esteganografia* da atualidade, embasadas ou não nas técnicas clássicas, e evidenciar seus impactos na sociedade como um todo. Também é proposta a implementação de algumas técnicas esteganográfico-digitais como futuras ferramentas didáticas. Deste modo, quaisquer interessados poderão ter um conhecimento ilustrado desta nova área.

1.1 Motivação

Há uma enorme quantidade de aplicações para a *esteganografia* e para o chamado *mascaramento digital de dados*. Dentre as diversas utilidades, pode-se destacar:

- agências militares e de inteligência precisam de comunicações reservadas. Mesmo se o conteúdo é criptografado, a detecção de um sinal nos modernos campos de batalha pode levar rapidamente a identificação e ataque aos remetentes e destinatários. Por esta razão, os militares utilizam técnicas de espalhamento de espectro e modulação;

- os criminosos também dão grande importância às comunicações reservadas. Eles preferem tecnologias como telefones móveis pré-pagos e telefones que mudam de identidade freqüentemente;

- a justiça e as agências de inteligência estão interessadas em conhecer estas tecnologias e suas fraquezas, assim como detectar e rastrear mensagens escondidas;

- tentativas recentes de alguns governos, por exemplo o dos EUA, de limitar os usos da criptografia têm estimulado as pessoas a buscar meios alternativos para garantir suas comunicações anônimas e seus direitos à liberdade de expressão [Wallich, 2003];

- esquemas para eleições digitais e dinheiro eletrônico precisam fazer uso de técnicas de comunicação anônimas.

Assim sendo, a *esteganografia* pode aumentar a privacidade individual. Esta não vem para substituir a criptografia. Vem, em contrapartida, para complementá-la. Os poderes da segurança digital podem aumentar consideravelmente quando, ao se transmitir uma mensagem, esta for criptografada e, em seguida, esteganografada. Por quê? Imagine a dificuldade em tentar quebrar um código ao qual não se sabe, ao menos, de sua existência.

1.2 Objetivos

O trabalho visa atender aos seguintes objetivos:

- propiciar um maior contato com as principais técnicas de proteção digital e, em especial, as técnicas de *esteganografia*;
- estudar técnicas clássicas de *esteganografia* e suas contribuições para as modernas técnicas esteganográfico-digitais;
- pesquisar técnicas esteganográfico-digitais existentes atualmente;
- Analisar o desempenho de tais técnicas e seu aproveitamento real como meio de proteção digital;
- identificar as vantagens e desvantagens de tais técnicas;
- buscar, na literatura, e/ou propor possíveis soluções para minimizar estas desvantagens;
- desenvolver um produto de *software* onde será possível acompanhar o processo de algumas técnicas esteganográficas. Pretende-se implementar pelo menos três destas técnicas. Objetiva-se criar uma ferramenta didática que permita apresentar, na prática, o funcionamento das técnicas;
- disponibilizar todo o material bibliográfico utilizado para o desenvolvimento da pesquisa. Desta forma, há a divulgação dos estudos de privacidade e proteção digital, bem como a situação corrente do trabalho. Para isso, será construída uma página (*site*) e disponibilizada na rede mundial de computadores (*internet*);
- divulgar mais este tema, que, certamente, não sairá das mídias informativas nos próximos anos.

1.3 Metodologia

Pretende-se realizar o trabalho utilizando-se os materiais e métodos descritos a seguir.

- Foi realizado um levantamento bibliográfico, na *internet* e em bibliotecas, de artigos científicos clássicos e atuais relacionados ao tema. Este levantamento continuará ao longo de todo o desenvolvimento do trabalho;
- Em paralelo, foi realizado um estudo do que seria a *esteganografia*, propriamente dita. Isto está sendo feito através de uma análise detalhada do material sendo coletado;
- Também em paralelo, foi realizado um estudo sobre os impactos da *esteganografia* no mundo. As mudanças que estão ocorrendo, o que está e o que não está sendo afetado entre outras;
- Findas estas etapas, serão encaminhados estudos das técnicas esteganográficas clássicas e as suas contribuições para os modernos sistemas esteganográficos atuais;
- Feito isso, parte-se para um estudo de algumas técnicas esteganográfico-digitais. Estas são o estado da arte da *esteganografia*;
- Após estes estudos preliminares, inicia-se um estudo de como seriam implementadas, computacionalmente, tais técnicas servindo como ferramenta didática a futuros interessados;
- Dá-se início à implementação, uma vez que as suas formas já foram definidas. A preocupação de construir códigos-fonte manuteníveis será constante. O paradigma de programação a ser utilizado é a orientação a objetos e a linguagem de programação será Java [Sun Microsystems, 2003] devido a alguns aspectos intrínsecos considerados importantes, por exemplo, a portabilidade entre sistemas operacionais [Deitel and Deitel, 2001];
- Terminada a implementação, passa-se para a etapa de testes em laboratório com o uso de exemplos práticos;
- Caso ocorra algum problema durante os testes de laboratório, retorna-se à etapa de simulação e, se necessário, retorna-se à etapa de projeto e estudo;
- Uma vez que o produto de *software* esteja funcionando satisfatoriamente, passa-se para a fase de finalização onde será desenvolvida uma documentação para posterior divulgação na *internet*;

- Ao término da monografia, artigos serão elaborados para divulgação através da submissão a eventos e periódicos científicos relacionados ao tema.

1.4 Descrição dos capítulos posteriores

A seguir é apresentada uma descrição sucinta dos capítulos deste trabalho. O capítulo 2 apresenta os principais termos utilizados na área de *esteganografia digital*. Em seguida, no capítulo 3, é feita uma retrospectiva histórica da *esteganografia* até os dias atuais. No capítulo 4, apresentam-se características, vantagens e desvantagens das principais técnicas esteganográficas da atualidade, sejam elas herdadas do passado ou inventadas há pouco tempo. Posteriormente, no capítulo 5, mostra-se o cronograma da pesquisa que está sendo seguido e, no capítulo 6, mostra-se a equipe que estará ligada ao projeto. No capítulo 7, descreve-se o estágio atual da pesquisa, o que já foi feito e o que ainda se pretende fazer. Finalmente, o capítulo 8 apresenta as principais referências utilizadas neste trabalho até o momento.

Capítulo 2

Terminologia

Como já dito, há um interesse cada vez maior, por diferentes comunidades de pesquisa, no campo da *esteganografia*, marcas d'água e seriação digitais. Com certeza, isso leva a uma certa confusão na terminologia. A seguir encontra-se um estudo dos principais termos utilizados nestas áreas. É importante salientar que estas definições ainda não são totalmente aceitas, podendo existir pequenas variações na literatura.

Segundo [Petitcolas et al., 1999], o modelo geral de ocultamento de dados (*information hiding*) pode ser descrito como se segue. O dado embutido (*embedded*) é a mensagem 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*) caso o meio de cobertura seja uma imagem, áudio de cobertura (*cover-audio*) ou mesmo texto de cobertura (*cover-text*). Após o processo de inserção dos dados na mensagem de cobertura obtém-se o chamado estego-objeto (*stego-object*) que é, por sua vez, uma mensagem inócua contendo secretamente uma mensagem de maior importância. A figura 2.1 apresenta como o processo pode ser interpretado.

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.

Parafraseando [Petitcolas et al., 1999], um ataque com sucesso à *esteganografia* consiste em conseguir detectar a existência de uma mensagem escondida em algum meio observado. Por outro lado, os sistemas de marcação de *copyright* ou *watermarking* têm requisitos adicionais de robustez contra possíveis ataques. Deste modo, um ataque bem-sucedido consiste em conseguir detectar e remover a

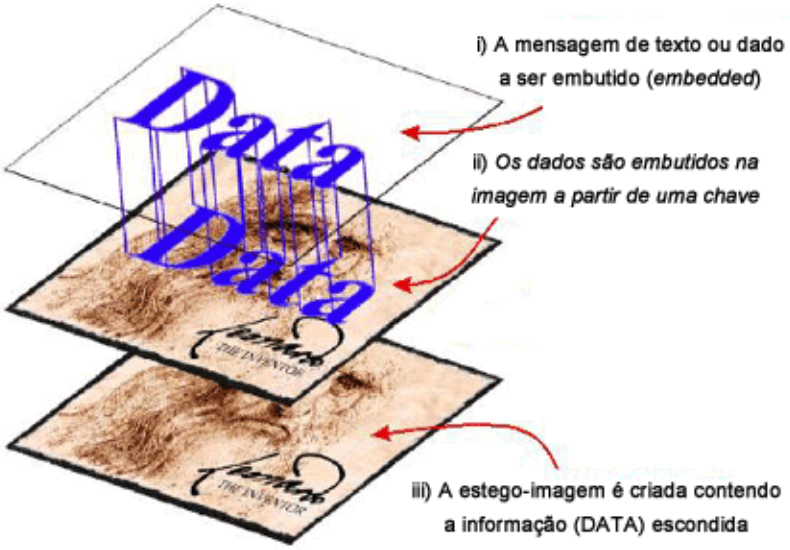

Figura 2.1: Exemplo de ocultamento de uma mensagem

marcação digital.

Continuando, o sistema de seriação digital (*fingerprinting*), também conhecido como *labels*, consiste de uma série de números embutidos no material a ser protegido. Isto permite identificar, por exemplo, que um cliente quebrou um acordo de propriedade intelectual.

Finalmente, pode-se delimitar a grande-área de pesquisa conhecida como ocultamento da informação (*information hiding*) como apresentado na figura 2.2.

No segundo nível da hierarquia têm-se: *canais abertos*, *esteganografia*, *anonimato* e *marcação de copyright*.

Entende-se por *canais secretos*, a criação de uma comunicação entre duas partes em que o meio é secreto e seguro. Um exemplo seria as conversações militares em faixas de freqüências moduladas.

Continuando, a arte da *esteganografia* constitui a segunda ramificação da hierarquia. Pode ser dividida em *lingüística* e *técnica*. Quando a mensagem é fisicamente escondida, tal como a maioria dos exemplos apresentados no capítulo 3, configura-se a chamada *esteganografia técnica*. Por outro lado, quando a mensagem é trabalhada e o seu ocultamento depende de propriedades lingüísticas, tal como a *esteganografia digital*, configura-se a chamada *esteganografia lingüística*.

Anonimato é um conjunto de técnicas para tentar navegar na *internet*, por exemplo, sem ser localizado. Isto poderia ser feito utilizando *sites* de desvio, por

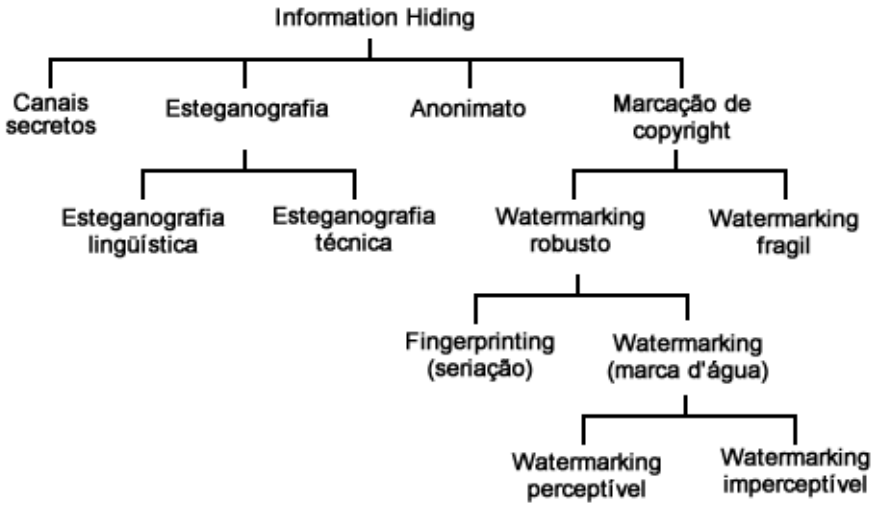

Figura 2.2: A hierarquia do *information hiding* [Pfitzmann, 1996]

exemplo o `www.anonymizer.com`, e/ou *remailers* — *sites* capazes de enviar mensagens secretas não revelando seu remetente —.

Marcação de copyright é a tentativa de manter ou provar a propriedade intelectual sobre algum tipo de mídia, seja esta eletrônica ou impressa. Neste sentido, *sistemas de marcação robustos* (*watermarking robusto*) são aqueles que mesmo após tentativas de remoção permanecem intactos. Por outro lado, *sistemas de marcação frágeis* (*Watermarking frágil*) são aqueles em que qualquer modificação na mídia acarretaria perda na marcação. Estes sistemas são úteis para impedir a cópia ilegal, ao se copiar um material original o resultado seria um material não marcado e, por conseguinte, pirata. *Sistemas de marcação imperceptível* (*Watermarking imperceptível*) são aqueles em que as logomarcas dos autores, por exemplo, encontram-se no material, mas não são diretamente visíveis. Em contrapartida, *marcação visível* (*Watermarking visível*) é aquela em que o autor deseja mostrar sua autoria a todos que observarem sua criação. Um exemplo desta última forma é formado pelas imagens disponibilizadas na biblioteca do Vaticano `http://bav.vatican.va`. Segundo [Mintzer et al., 1996], nesta biblioteca as imagens possuem um sistema de marcação digital visível como pode ser observado na figura 2.3.

Figura 2.3: Exemplo de *marcação visível*. Biblioteca do Vaticano

Capítulo 3

Análise histórica

3.1 A esteganografia clássica

Através de toda a história, as pessoas têm tentado as mais 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].

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.

Outra técnica bastante utilizada através da História foi o uso de tabletes de madeira cobertos de cera. Estes tabletes serviam como meio de escrita para a época, Grécia Antiga. Os textos eram escritos sobre a cera e, quando se tornavam inúteis, a cera era derretida e uma nova camada de cera era colocada sobre a madeira. Isto gerava outro tablete de cera novo e pronto para escrita. Seguindo esta idéia, Heródoto conta que Demeratus, um grego exilado na corte persa, ficara sabendo que o rei da Pérsia, Xerxes, o Grande, estava planejando invadir seu país natal. Movido de sentimentos de patriotismo para com seu país, Demeratus resolveu, então, encontrar um meio de avisar a corte grega sobre os plano audaciosos de Xerxes.

A maneira encontrada foi utilizar os já famosos tabletes de cera. No entanto, ele não agiu pela forma normal em que se escrevia nos tabletes. Ao invés de escrever na cera sobre a madeira, o que tornaria seu texto visível a todos, tal como se fosse um texto em folha de papel atualmente, Demeratus derreteu toda a cera, escreveu a mensagem na própria madeira e depois a recobriu com cera novamente como se estivesse construindo um tablete de cera novo. Este procedimento, por parte de Demeratus, fez com que o texto na madeira ficasse encoberto pela cera. Os tabletes foram então enviados como se fossem tabletes em branco para exportação. Passaram sem problemas na fronteira persa e chegaram em tempo na Grécia. Contudo, como ninguém na Grécia sabia do procedimento do emissor da mensagem, os tabletes ficaram um bom tempo sem serem decifrados. Isto prosseguiu até que uma mulher grega de nome Gorgo, desconfiada dos tais tabletes, resolveu derreter a cera. Com isso, Gorgo tornara-se a primeira mulher criptoanalista da história e a corte grega fora salva pela engenhosa idéia de Demeratus.

Outro relato interessante vem do grego Enéas, o Tático, escritor de várias matérias militares. Ele inventou uma técnica esteganográfica intitulada astrogal. O astrogal consistia em uma madeira com vários furos, cada qual representando uma letra. Quando alguém desejasse enviar uma mensagem, este deveria passar um barbante pelos furos correspondentes às letras da mensagem a ser transmitida. Cabia ao receptor da mensagem acompanhar as várias ligações de pontos feitas pelo barbante e, assim, decifrar a mensagem. Quando era interceptado por alguém, este engenho era tido apenas como um brinquedo de criança.

Durante a Renascença, Giovanni Porta, um dos maiores criptoanalistas de seu tempo, ”aperfeiçoou” a técnica da lebre de Harpagus. A proposta de Porta era alimentar um cachorro com a mensagem. Desta forma, o cachorro seria enviado como seu portador. O receptor ao recebê-lo, o mataria e recuperaria a mensagem.

Segundo [Kahn, 1996], Porta é bastante conhecido no campo da comunicação secreta. Também é sua a criação da famosa *cifra indecifrável* (*Le chiffre indéchiffrable*), um dos primeiros sistemas de criptografia por substituição polialfabética. A figura 3.1 apresenta este famoso trabalho de Porta.

Ainda nesta época, Johannes Trithemius, um abade alemão, publicou uma trilogia em latim intitulada *Steganographia: hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*. No terceiro volume desta obra, Trithemius escondeu o Salmo 23 da Bíblia Sagrada através da utilização de algumas tabelas contendo números. Os escritos foram descobertos apenas no século XX devido aos esforços dos pesquisadores Thomas Ernst, da Universidade de Pittsburg, e Jim Reeds, do AT&T Labs [Kolata, 2003].

Outra técnica interessante e simpática que aparece durante a História faz uso de inúmeras variações de tintas “invisíveis” (*invisible inks*). Segundo [Kuhn, 1996]

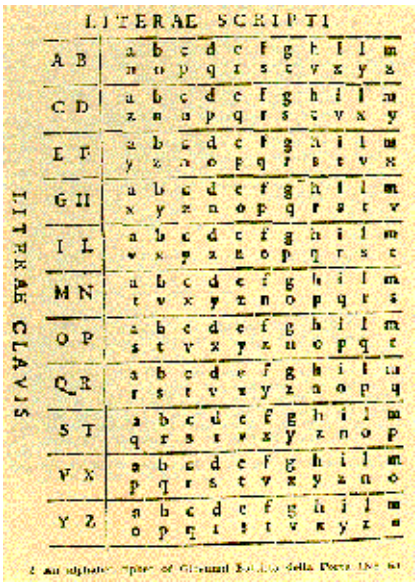

Figura 3.1: A cifra polialfabética de Porta

e [Kahn, 1996], tais tintas não são novidades e já apareciam em relatos de Plínio, o Velho, ou mesmo Ovídio, no século I DC, 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.

As primeiras tintas eram simples fluídos orgânicos que não exigiam nenhuma técnica especial para serem reveladas. Algumas vezes bastava apenas aquecer o papel e a mensagem aparecia. Isto pode ser confirmado com as tintas baseadas em fluídos de suco de limão, por exemplo.

No entanto, durante a primeira guerra mundial, espiões alemães colocavam pequenos “pontos” de tinta invisível sobre letras de revistas e jornais de grande circulação. As folhas de revistas “pontuadas”, quando aquecidas, revelavam a seqüência das letras e, por conseguinte, toda a mensagem ali escondida [Kuhn, 1996].

Suspeitando de atividades semelhantes às dos alemães na primeira grande guerra, os americanos recrutaram inúmeros profissionais qualificados durante a guerra-fria. O objetivo era “scanear” as principais publicações impressas em circulação no país em busca de mensagens secretas dos soviéticos ali escondidas.

Como resultado do progresso global da ciência, outras formas mais poderosas de tintas invisíveis foram aparecendo através da história. De forma geral, as tin-

Figura 3.2: Trithemius e uma das tabelas encontradas em *Steganographia*

tas invisíveis são químicas que, misturadas a outras químicas, tornam o resultado visível. Alguns historiadores mencionam o uso de tais químicas desde os tempos clássicos. Uma delas é o uso do ácido galotânico — feito a partir de nozes — que se torna visível em contato com sulfato de cobre.

Um exemplo mais próximo dos tempos contemporâneos foi aplicado pelo espião nazista George Dasch, na segunda guerra mundial. Dasch escreveu mensagens em seu lenço utilizando uma solução de sulfato de cobre. A mensagem poderia ser decodificada utilizando-se vapor de amônia [Kuhn, 1996].

Durante as duas guerras mundiais, os químicos tinham de estudar várias formas possíveis e imagináveis de combinações químicas das mais diversas substâncias. Estas seriam para esconder ou mesmo para descobrir mensagens e criar procedimentos-padrão de detecção para censores nas fronteiras. Estes tinham que utilizar inúmeras escovinhas sobre mensagens interceptadas, borrifar uma enorme combinação de químicas, entre outras coisas, objetivando descobrir mensagens secretas ali colocadas utilizando-se tintas invisíveis.

De acordo com [Johnson and Jajodia, 1998], outros exemplos, através da história, aparecem no campo da fotografia. Devido aos inúmeros avanços neste campo, com um grande aumento na qualidade das fotos bem como uma sucessiva redução em seus tamanhos, tornou-se possível reduzir fotos de páginas de texto inteiras a tamanhos consideráveis. Uma aplicação desta técnica de redução aconteceu na guerra franco-prussiana. Quando Paris estava sitiada pela Prússia, seus habitantes escreviam mensagens e então fotografavam-nas. Em seguida, reduziam ao máximo os negativos. Utilizando-se de pombos-correio, enviavam as

mensagens para fora de Paris, conseguindo estabelecer um canal de comunicação com os arredores da cidade sitiada.

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 de uma das sentenças. A mensagem gerada era então enviada sem levantar maiores suspeitas. Esta engenhosidade ficou conhecida como *tecnologia do micro-ponto*.

Outras formas clássicas de comunicação secreta são os *semagramas* e os *códigos abertos*.

Semagramas são formas de comunicação secreta que não estão na forma escrita. A utilização dos semagramas também pode ser encontrada na segunda guerra mundial. Como narra [Kahn, 1996], em certa ocasião, os censores americanos interceptaram um carregamento de relógios e mudaram toda a disposição destes na caixa bem como a de seus ponteiros. Havia o medo de que a disposição dos ponteiros e dos relógios escondesse alguma mensagem secreta.

Por outro lado, *códigos abertos* fazem o uso da ilusão ou de palavras código. Como exemplo, têm-se as ações de Vallerie Dickinson — uma espiã a serviço do Japão na segunda grande guerra — que usava vestidos de bonecas para avisar aos japoneses sobre ações americanas. Pequenos vestidos representavam *destroyers* e grandes vestidos poderiam representar *couraçados* ou *cruisers*.

Cifras nulas (*null ciphers*) também foram muito utilizadas. De acordo com [Johnson and Jajodia, 1998], através desta técnica uma mensagem é escondida dentro de outra aparentemente inocente. Um exemplo clássico é a obra *Hypnerotomachia Poliphili* de 1499. Neste livro, um padre, de nome Colona, codificou a mensagem "Padre Colona ama Polia apaixonadamente" (*Father Colona Passionately loves Polia*) em cada primeira letra de um novo capítulo. Infelizmente a Igreja Católica não tolerou o abuso e, quando tempos depois, decifrou a mensagem, condenou o padre à morte. Um exemplo mais claro de *cifras nulas* pode ser encontrado a seguir. Este texto é uma cifra nula enviada por um espião alemão na segunda grande guerra.

> *Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.*

A mensagem codificada pode ser extraída pela captura de toda segunda letra de cada palavra. Isto resulta em:

Pershing sails from NY June 1.

Girolammo Cardano também dá uma grande contribuição à *esteganografia* através de seu engenho conhecido como “grelha de cardano”. Tal técnica consistia em um papelão com furos em locais estratégicos. Tanto o emissor quando o receptor, em posse de uma grelha dessas poderia se comunicar colocando-a sobre uma grande quantidade de texto e apenas apareceriam as palavras sob os furos da grelha.

Um exemplo mais atual de *esteganografia* pode ser encontrado no governo da primeira-ministra britânica Margareth Tatcher nos anos oitenta. Desconfiada de que alguns de seus ministros não lhe eram mais leais, a ministra ordenou à sua casa civil que codificasse os principais documentos do governo com *códigos de deslocamento de linha* de modo que não se pudesse falsificá-los. Infelizmente, a primeira-ministra não teve êxito e a informação vazou para a imprensa. Seus planos tiveram de ser estrategicamente reconsiderados.

De acordo com [Judge, 2001], em certas ocasiões, os emissores não possuem o interesse em esconder as mensagens. No entanto, se todos aqueles que são capazes de entendê-la deixarem de existir a mensagem torna-se, de alguma forma, escondida dado que não há mais quem a decifre. Neste sentido, pode-se citar os “geoglifos” do platô de Nazca no Peru. Um exemplo encontra-se na figura 3.3. Estes foram decifrados recentemente a partir de uma vista aérea. Algumas das histórias aqui contadas ainda são recentes. Atualmente traficantes de drogas escondem “papelotes” dentro de seus corpos, engolindo-os. São as chamadas “mulas” (jargão policial). Isto remonta à técnica de Giovanni Porta no Renascimento.

No Brasil, até meados da década de 80, algumas provas de concursos públicos eram corrigidas utilizando-se cartões perfurados semelhantes à técnica da grelha inventada por Girolammo Cardano. Quando postas sobre os cartões-respostas dos candidatos, revelavam se o candidato havia acertado ou errado as questões da prova.

3.2 A esteganografia digital

Atualmente, a *esteganografia* não foi esquecida. Ela foi modificada em sinal de acompanhamento dos novos tempos. Na era da informação não faz mais sentido escrever textos em tabletes de madeira ou mesmo borrifar pontos em uma revista através da utilização de tintas ”invisíveis”. Qualquer meio de *esteganografia* na

Figura 3.3: Um “geoglifo” no platô de Nazca, Peru.

atualidade, inevitavelmente, deve utilizar-se de 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.

Como será explicado no capítulo 4, há inúmeras formas de esteganografia digital atualmente. Pode-se utilizar imagens, sons, textos, entre outros, como meios de cobertura para mensagens a serem transmitidas.

Capítulo 4

Técnicas esteganográficas

4.1 Visão geral

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 um *stream* de dados contínuos como, por exemplo, uma transmissão telefônica. O último pode ser um arquivo como um arquivo ".WAV", por exemplo.

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 histograma. Mudanças em alguma 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*. 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*.

De forma geral, tanto o emissor quanto o receptor da mensagem compartilham uma chave secreta e a usam com um gerador de *streams* (*stream generator*) de modo a conseguir selecionar os vários locais do objeto de cobertura que serão utilizados para esconder a mensagem desejada.

Embora as técnicas de LSB consigam esconder os dados aos olhos humanos, elas podem ser facilmente destruídas computacionalmente utilizando algoritmos de compressão com perdas de dados (*lossy compression algorithms*). Estes algoritmos selecionam apenas as partes mais significativas do objeto de cobertura. Isto significa que os *bits* menos significativos têm uma chance menor de serem selecionados [Katzenbeisser and Petitcolas, 2000].

Outra forma de destruir os dados escondidos utilizando técnicas LSB consiste em fazer pequenas alterações no objeto de cobertura utilizando filtros de baixa passagem (*low-pass filters*). Estes filtros são capazes de inserir modificações superficiais nos objetos de cobertura praticamente invalidando-os [Katzenbeisser and Petitcolas, 2000].

Uma forma para contornar tais ataques é esconder a mensagem em vários locais do objeto de cobertura. Além disso, a utilização de códigos de correção de erros (*CRCs — check redundance codes*) também se mostra uma solução eficaz.

Como descrito nos objetivos, pretende-se com o trabalho, implementar um produto de *software* capaz de trabalhar com algumas técnicas digitais de *esteganografia*. Foram escolhidas, essencialmente, as técnicas que utilizam imagens como sendo objetos de cobertura, podendo esconder tanto outras imagens quanto textos. As imagens foram escolhidas como meio de carregamento devido ao seu disseminado manuseio diário pela rede mundial de computadores e pela relativa facilidade em que os usuários conseguem manipulá-las. A seguir, tem-se uma explicação mais detalhada sobre o processo de utilização de imagens como objetos de cobertura.

4.2 Técnicas de codificação em imagem

Informações podem ser escondidas de muitas maneiras diferentes utilizando imagens como meio de cobertura.

Segundo [Anderson and Petitcolas, 1998], a inserção de uma mensagem plana pode ser feita codificando cada *bit* de informação na imagem. Uma codificação mais complexa pode ser feita para encaixar a mensagem somente em áreas de ruído da imagem, i.e., aquelas em que haverá menor atenção. A mensagem pode também ser dispersa aleatoriamente toda a superfície de ”ruídos” da imagem.

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 à imagens, com graus variados de sucesso. O método de inserção no *bit* menos significativo é provavelmente uma das melhores técnicas de *esteganografia* em imagem.

4.2.1 Inserção no bit menos significativo

As técnicas de LSB podem ser aplicadas a cada *byte* de uma imagem 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, finalmente, 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.

Acompanhe o exemplo da figura 4.1 para entender melhor. Suponha que se deseja esconder a letra **E** dentro da porção de imagem.

```
(00100111 11101001 11001000 11101010)  [a, R, G, B]
(10100111 11001000 11101001 11101000)  [a, R, G, B]
(11001000 00100111 11101001 00100111)  [a, R, G, B]
```

Figura 4.1: Porção de uma imagem de cobertura

Na figura 4.1, 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-se apenas os dois primeiros *pixels* da imagem. Assim, utilizando-se a técnica LSB, tem-se o resultado mostrado na figura 4.2

Os trechos em negrito representam os LSBs. Em sublinhado os *bits* que tiveram que ser modificados para esconder a letra **E**.

Figura 4.2: Porção da estego-imagem gerada pela porção de imagem 4.1

Como exemplo da grande quantidade de dados que podem ser escondidos, suponha uma imagem com tamanho de 1024 por 768 *pixels*. Neste caso, têm-se 786.432 *pixels* no total. Como cada *pixel* pode codificar 4 *bits* tem-se uma possibilidade de esconder cerca de 390 *kilobytes* de dados neste objeto de cobertura.

Uma forma de prover maior robustez às inserções LSB é trabalhar com *stream-generators* capazes de escolher várias posições diferentes e aleatórias na imagem de cobertura, bem como utilizar chaves esteganográficas seguindo o estilo da criptografia de chave pública.

4.2.2 Técnicas de filtragem e mascaramento

Segundo [Johnson and Jajodia, 1998], técnicas de *filtragem e mascaramento* são restritas à imagens em tons de cinza (*grayscale*). Estas técnicas escondem a informação através da criação de uma imagem semelhantemente as 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. Isto é, deve-se ao fato de que as modificações em *bits* mais significativos de imagens em cores geram alta quantidade de ”ruído” tornando as informações detectáveis.

4.2.3 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].

Capítulo 5

Cronograma

Na figura 5.1, é apresentada uma proposta para o cronograma de atividades a ser seguida no desenvolvimento do trabalho.

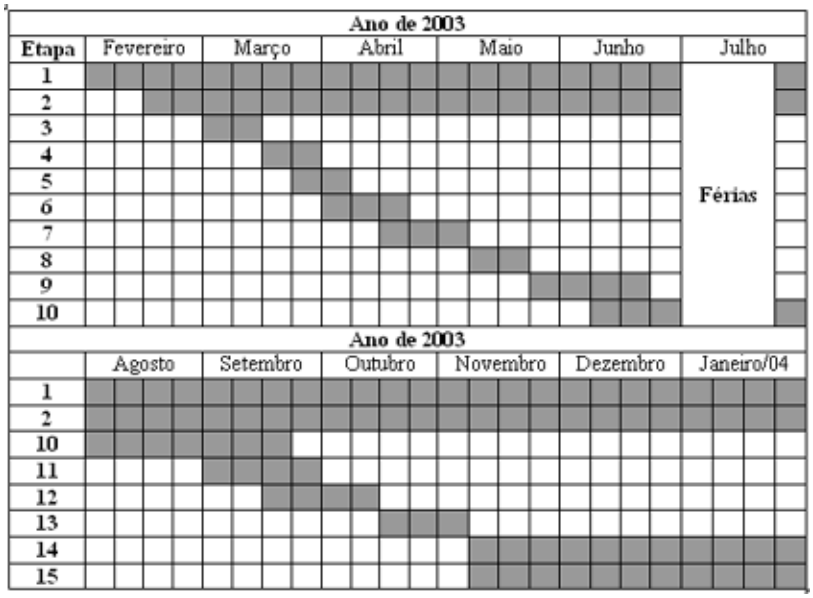

Figura 5.1: Cronograma de atividades

1. Coleta de material bibliográfico.
   Procura de artigos especializados, livros, sites na internet.

2. Desenvolvimento do site da pesquisa e criação de uma lista de discussão.
   Iniciar o site que conterá os avanços da pesquisa de modo que outros interessados possam ter um ponto de partida para se iterar mais sobre o assunto. Este site irá ser atualizado durante toda a pesquisa

3. Introdução à esteganografia clássica e sua história.
   Estudar as formas clássicas de esteganografia apontando sua evolução ao longo da história.

4. Contribuições da esteganografia clássica.
   Levantar as principais contribuições das formas clássicas de esteganografia para os modernos sistemas esteganográfico-digitais.

5. Impactos da esteganografia digital na sociedade como um todo.
   Como forma de proteção de propriedade intelectual e privacidade individual como a sociedade se comportará diante de tais inovações. Quais serão os efeitos de curto, médio e longo prazos.

6. Estudo aprofundado de técnicas esteganográfico-digitais.
   Listar e explicar o funcionamento das principais técnicas esteganográfico-digitais da atualidade. Algumas destas técnicas podem ser: mascaramento através de imagens digitais por inserção em bits menos significativos, filtragem e mascaramento, transformações algorítmicas entre outras.

7. Vantagens e desvantagens de tais técnicas.
   Nem todo sistema baseado em técnicas esteganográfico-digitais é perfeito. Listar e apontar as principais limitações de alguns sistemas e possíveis contra-medidas para tais problemas encontradas na literatura relacionada.

8. Procura de idéias de como implementar algumas das técnicas estudadas.
   Buscar, na literatura relacionada, formas clássicas de solução das técnicas estudadas.

9. Implementação de um ambiente simulador de técnicas esteganográficas.
   Construção de um produto de software que possa simular a execução de algumas técnicas esteganográficas. Este ambiente será desenvolvido utilizando-se a linguagem de programação Java por ser mais portável.

10. Implementação das técnicas previamente selecionadas.
    Findas as buscas por idéias de implementação, nesta fase, técnicas selecionadas na fase 9 serão efetivamente criadas em computador.

11. Testes de verificação da implementação.
    Testes serão realizados no produto de software construído.

12. Análise das técnicas.
    Listar as principais dificuldades na implementação de tais técnicas e possíveis tentativas para superar estas dificuldades.

13. Geração de documentação.
    Como tudo será disponibilizado na internet é necessário que uma documentação sobre os fontes do produto de software desenvolvido esteja disponível. Esta será a fase onde todos os códigos fontes desenvolvidos na pesquisa serão documentados.

14. Escrita da monografia a ser entregue para conclusão de curso.
    Tudo o que for desenvolvido constará na monografia que será entregue para conclusão de curso.

15. Escrita de artigos.
    Escrita de artigos relacionados à pesquisa e submissão a eventos e/ou periódicos científicos relacionados ao tema.

Capítulo 6

Equipe técnica

Aluno: Anderson de Rezende Rocha
Titulação: graduação em Ciência da Computação (em curso)
Dedicação: integral
Resumo curricular: graduando do curso de Bacharelado em Ciência da Computação da *Universidade Federal de Lavras* (UFLA) atualmente cursando o 7º período. Adquiriu experiência em pesquisa científica durante o período de maio de 2001 a julho de 2002 com o projeto intitulado *Desenvolvimento de uma arquitetura para simulação do funcionamento distribuído e paralelo do cérebro*, na área de *Inteligência Artificial*. No período de agosto de 2002 até atualmente trabalha no projeto intitulado *Desenvolvimento de um simulador de algoritmos quânticos utilizando a computação convencional*, na área de *computação quântica*. Estes trabalhos são projetos de pesquisa do PIBIC com registro de número **105133 / 2001-9** no *Conselho Nacional de Desenvolvimento Científico e Tecnológico* (CNPq).

Orientador do projeto: Heitor Augustus Xavier Costa
Titulação: doutor em Ciência da Computação (em curso)
Cargo: professor 3º grau
Dedicação: exclusiva
Resumo curricular: bacharel em Informática pela *Universidade Federal Fluminense* (UFF-Niterói), RJ, em 1994. Mestre em Informática pela *Pontifícia Universidade Católica* do Rio de Janeiro (PUC-Rio), em 1997. Doutorando pela *Escola Politécnica da Universidade de São Paulo* (Poli/USP-SP). Retornou do doutorado em fevereiro e atua na área de *Engenharia de Software*. Lecionou 01 (um) ano na *Pontifícia Universidade Católica do Rio de Janeiro* (PUC-Rio) e 02 (dois) anos na *Universidade Federal Fluminense* (UFF-Niterói). Atualmente leciona na *Universidade Federal de Lavras* para o Curso de Ciência da Computação onde é professor

assistente de 3º grau com dedicação exclusiva desde 1998.

Co-orientador do projeto: Lucas Monteiro Chaves
Titulação: pós-doutor em Matemática
Cargo: professor 3º grau
Dedicação: exclusiva
Resumo curricular: graduação em Matemática pela *Universidade Federal de Minas Gerais* (UFMG) em 1977-1979. Engenharia Elétrica pela *Universidade Federal de Minas Gerais*, 1977-1984. Mestrado em Matemática pela *Universidade Federal de Minas Gerais*, 1980-1982 Doutorado em Matemática (área de concentração Geometria Diferencial) na *Universidade Estadual de Campinas*, 1987-1991. Pós-doutorado em 1997 na *Universidade Estadual de Campinas*. Áreas de pesquisa: *Probabilidade e Combinatória*. Atualmente leciona na *Universidade Federal de Lavras* em regime de dedicação exclusiva.

Capítulo 7

Estágio atual da pesquisa

Até o momento, conseguiu-se levantar alguns requisitos para implementação da ferramenta proposta.

Através da utilização dos LSBs, a ferramenta a ser implementada deverá permitir a inserção de figuras em figuras, textos em figuras e textos criptografados em figuras. Caso a pesquisa evolua de maneira satisfatória, pretende-se implementar, ainda, alguma técnica que utilize transformações algorítmicas na imagem.

Cada técnica implementada será estudada quanto às suas propriedades estatísticas. Serão feitas análises de entropia, histograma, entre outros.

Além disso, pretende-se fazer um levantamento das principais implicações e considerações entre a utilização da esteganografia digital em relação à sociedade em geral. Estariam, os grupos terroristas, utilizando a esteganografia como meio de comunicação? A esteganografia realmente habilita a proteção digital ou é apenas uma armadilha digital? Questões como essa deverão ser respondidas ao longo do trabalho.

Referências Bibliográficas

[Anderson and Petitcolas, 1998] Anderson, R. J. and Petitcolas, F. A. P. (1998). On the limits of steganography. In *IEEE Journal of Selected Areas in Communications*. Special issue on Copyright & Privacy Protection.

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

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

[Deitel and Deitel, 2001] Deitel, H. M. and Deitel, P. J. (2001). *Java como programar*. Bookman Editora, Porto Alegre. Tradução de Edson Furnankiewicz.

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

[Judge, 2001] Judge, J. C. (2001). Steganography: Past, present, future. In *Proceedings of the First International Information-Hiding Workshop*. The SANS Institute. Último acesso em 15 de maio de 2003.

[Kahn, 1996] Kahn, D. (1996). *The CODEBREAKERS: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, Boston. ISBN 0684831309.

[Katzenbeisser and Petitcolas, 2000] Katzenbeisser, S. and Petitcolas, F. A. (2000). *Information hiding, techniques for steganography and digital watermarking*. Artech House, Boston.

[Kolata, 2003] Kolata, G. (2003). A mystery unraveled, twice. Disponível em `cryptome.unicast.org/cryptome022401/tri.crack.htm`. Acessado em 15 de abril de 2003.

[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`.

[Mintzer et al., 1996] Mintzer, F. C., Boyle, L. E., and Cases, A. N. (1996). Toward on-line, worldwide access to vatican library materials. In *IBM Journal of Research and Development*, volume 40.

[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.

[Pfitzmann, 1996] Pfitzmann, B. (1996). Information hiding terminology. In *Proceedings of the first international information-hiding workshop*. Springer–Verlag, Berlim.

[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.

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

Apêndice A

Currículo Lattes