Índice

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. *Esteganografia* deriva do grego, donde *estegano = esconder, mascarar* e *grafia = escrita.* Logo, *estaganografia* 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, arranjamento 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 dentro de 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.

Este trabalho se propõe a 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.

2 – A importância da pesquisa proposta

Além do exposto na sessão anterior, há uma enorme quantidade de aplicações para o mascaramento digital de dados e para a esteganografia. 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 tem estimulado as pessoas a buscar meios alternativos para garantir suas comunicações anônimas e seus direitos à liberdade de expressão;
- 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 drasticamente quando, ao se transmitir uma mensagem, esta for criptografada e, em seguida, esteganografada. Por quê? Imagine a dificuldade em se tentar quebrar um código ao qual não se sabe, ao menos, de sua existência.

3 – Equipe técnica

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). 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 atual: Probabilidade e Combinatória. Atualmente leciona na *Universidade Federal de Lavras* em regime de dedicação exclusiva.

Bolsista: *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) cursando o 7º período. Tem grande interesse em continuar trabalhando com iniciação científica. 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. Ambos os trabalhos são projetos de pesquisa do PIBIC com registro de número **105133/2001-9** no CNPq. Está bastante estimulado a desenvolver um trabalho interessante nas áreas de esteganografia e segurança digitais.

4 – Objetivos

Este projeto visa atender aos seguintes objetivos:

- Dar continuidade à metodologia de desenvolvimento científico experimentado pelo graduando quando de sua atual bolsa de pesquisa.
- Propiciar ao graduando 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 4 destas técnicas. Deste modo, objetiva-se criar uma ferramenta didática que permita apresentar, na prática, o funcionamento destas 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 projeto. Para isso, será construída uma página (*site*) e disponibilizada na rede mundial de computadores (*internet*).
- Divulgar mais este tema, que, com certeza, não sairá das mídias informativas nos próximos anos.

5 – Metodologia

Este projeto atenderá aos seus objetivos utilizando-se os seguintes métodos:

- Será feito um levantamento bibliográfico, na *internet* e em bibliotecas, de artigos científicos clássicos e atuais relacionados ao tema.
- Feita esta fase de estudo inicial, parte-se para o estudo do que seria a esteganografia, propriamente dita. Isto será feito através de uma análise detalhada do material coletado.
- Em seguida, será realizado um estudo sobre os impactos da esteganografia no mundo. As mudanças que estão ocorrendo, o que não será afetado entre outras.
- Finda esta etapa, serão encaminhados estudos das técnicas esteganográficas clássicas e as contribuições destas 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 devido a alguns aspectos intrínsecos considerados importantes, por exemplo, a portabilidade.
- 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 projeto esteja funcionando aceitavelmente, passa-se para a fase de finalização onde será desenvolvida uma documentação para posterior divulgação na *internet.*
- Ao término do projeto, artigos serão elaborados para divulgação através da submissão à eventos e periódicos científicos relacionados ao tema. Além disso, um *produto de software* e uma *monografia de fim de curso* são esperados como resultado final do projeto.

6 – Cronograma e plano de trabalho do bolsista

Abaixo está uma proposta para o cronograma de atividades a ser seguido pelo bolsista:

Ano de 2003																							
Etapa	Agosto				Setembro				Outubro				Novembro				Dezembro				Janeiro/04		
1																							
2																							
3																							
4																							
5																							
6																							
7																							
8																							
9																							
10																							
Ano de 2004																							
	Fevereiro				Março				Abril				Maio				Junho				Julho		
2																							
10																							
11																							
12																							
13																							
14																							
15																							

Férias

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, mascaramento e filtragem, transformações matemáticas etc.

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 do relatório final a ser entregue ao CNPq.

Tudo o que foi desenvolvido constará no relatório final de pesquisa que será entregue ao CNPq.

15 – Escrita de artigos.

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

7 – Referências bibliográficas

[1] PETITCOLAS, Fabien A. P; Anderson, Ross J.; Kuhn, Markus G. *Information Hiding – a survey*. Proceedings of IEEE, special issue on *Protection on multimedia content.* July, 1999.

[2] ANDERSON, Ross J. and Petitcolas, Fabien A. P. *On the limits of steganography.* IEEE Journal of Selected Areas in Communications. Special issue on *Copyright & Privacy Protection.* May 1998.

[3] ARTZ, Donovan. *Digital steganography: hiding data within data.* IEEE Internet Computing. May-june 2001.

[4] JOHNSON, Neil F. and Jajodia, Sushil. *Exploring steganography: seeing the unseen.* IEEE Computer. February, 1998.

[5] KUMAGAI, JEAN. *Mission Impossible?*. Pages. 26-31. IEEE Spectrum. April, 2003.

[6] CASS, Stephen. *Listening in.* Pages. 32-37. IEEE Spectrum. April, 2003.

[7] WALLICH, Paul. *Getting the message.* Pages. 38-43. IEEE Spectrum. April, 2003.

Lavras, maio de 2003

Prof. Heitor Augustus Xavier Costa
Orientador do projeto