UNIVERSIDADE SAGRADO CORAÇÃO

MARIA ROSIANE TEIXEIRA PEREIRA

ESTEGANOGRAFIA: ANÁLISE DE TÉCNICAS APLICADAS A SEGURANÇA DA INFORMAÇÃO

BAURU

2013

MARIA ROSIANE TEIXEIRA PEREIRA

ESTEGANOGRAFIA: ANÁLISE DE TÉCNICAS APLICADAS A SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Dr. Elvio Gilberto da Silva.

BAURU

2013

Pereira, Maria Rosiane Teixeira

P4366e

Esteganografia: análise de técnicas aplicadas a segurança da informação / Maria Rosiane Teixeira Pereira -- 2013.

69f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Informação. 2. Segurança da informação. 3. Perícia forense computacional. 4. Criptografia. 5. Esteganografia. I. Silva, Elvio Gilberto da. II. Título.

MARIA ROSIANE TEIXEIRA PEREIRA

ESTEGANOGRAFIA: ANÁLISE DE TÉCNICAS APLICADAS A SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação, sob orientação do Prof. Dr. Elvio Gilberto da Silva.

Banca examinadora:

_____

Prof. Dr. Elvio Gilberto da Silva
Universidade Sagrado Coração

_____

Prof. Esp. Henrique Pachioni Martins
Universidade Sagrado Coração

_____

Profa. Drª. Patricia Bellin Ribeiro
Universidade Sagrado Coração

Bauru, 03 de Dezembro de 2013.

Dedico este trabalho a minha família, em especial ao meu esposo Cristiano e ao meu filho Raul. Todo ganho envolve alguma perda, perdi algum tempo com vocês, obrigada pela compreensão, vocês fazem parte dessa conquista!

"Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível." (Charles Chaplin, 1889).

AGRADECIMENTOS

Primeiramente agradeço a DEUS pela força e inspiração nesses quatro anos de estudo, e no desenvolvimento deste trabalho.

Agradeço a todos os professores do curso de Ciência da Computação, especialmente ao Prof. Esp. Henrique Pachioni Martins pelo suporte técnico, a Profa. Drª. Patricia Bellin Ribeiro pelas dicas e principalmente ao meu orientador Prof. Dr. Elvio Gilberto da Silva, por toda sabedoria, confiança e apoio prestado para a conclusão deste trabalho.

Agradeço a todos os meus colegas de curso em especial Rodrigo Comegno de Jesus e Thiago da Costa Silva pela companhia, incentivo e sugestões. Agradeço aos meus amigos pela paciência nos momentos que me ouviram falar sobre o curso e sobre o tema Esteganografia!

Agradeço também a minha irmã Maria Geni (Nina), por estar junto comigo durante essa caminhada, por cuidar quando precisei com tanto amor do que eu tenho de mais precioso nessa vida, meu filho Raul. Você nina pode não saber, mas no dia 07/05/2012, ao me responder um bilhete, não me deixou desistir, dizendo que me amava e que era pra eu terminar minha faculdade, que sempre foi meu sonho.

Finalmente agradeço a uma pessoa que foi essencial para que esse sonho tornasse realidade, Pedro Wilson Redondo, obrigada por tudo, pelo apoio desprendido em torno desses anos, por me fazer acreditar que eu era capaz! Não existem palavras para que eu possa expressar o quanto sou grata a você.

RESUMO

A segurança da informação é um tema amplamente discutido e de grande relevância para a tecnologia da informação. Questões como a confidencialidade, integridade e autenticidade de uma mensagem, assim como a privacidade de uma comunicação são pontos que trazem preocupação para os usuários da Internet que trocam milhões de mensagens a cada dia, sejam pessoais ou comerciais, onde sua interceptação e divulgação poderiam comprometer grandes organizações. Especialistas na área da segurança da informação vêm buscando desenvolver técnicas de segurança de dados com intenção de reverter esse quadro. Uma dessas técnicas que vem ganhando espaço é a Esteganografia Digital. Esteganografia pode ser definida como escrita oculta, que utiliza da técnica de ocultar informações dentro de arquivos como, imagens, vídeos, áudio e textos. Historicamente a esteganografia evoluiu em simultaneidade com a Criptografia, ciência que estuda as formas de se escrever uma mensagem em código, tornando-a de difícil entendimento a qualquer pessoa que não deva saber do conteúdo original. Ambas as ciências se complementam e seu uso conjunto enriquece a segurança da comunicação na Internet. Este trabalho apresenta um referencial teórico sobre alguns assuntos que sofrem impacto com o uso da esteganografia. Tais como: Segurança da Informação, criptografia e perícia forense computacional. A proposta deste trabalho aborda testes práticos com algumas ferramentas esteganográficas *free,* encontradas na rede, que utilizem diferentes técnicas, permitindo assim, avaliar a eficácia de cada técnica no mascaramento das informações digitais em relação a ataques feitos através de ferramentas de Perícia Forense Digital.

Palavras-chave: Informação. Segurança da Informação. Perícia Forense Computacional. Criptografia. Esteganografia.

ABSTRACT

Information security is a widely discussed topic of great relevance to information technology. Issues such as confidentiality, integrity and authenticity of a message as well as the privacy of communication are points that bring concern to the ever growing number of Internet users who exchange millions of messages every day, whether personal or commercial, in which their interception and disclosure could compromise large organizations. Experts in the field of information security have been seeking to develop techniques for data security with intent to reverse this situation. One such technique that is gaining ground is the Digital Steganography. Steganography can be defined as hidden writing, which uses the technique to hide information within files like images, videos, audio and text. Historically steganography evolved simultaneously with the Cryptography, the science which studies the ways of writing a message in code, making it difficult for anyone who might not have knowledge about the original content. Both sciences are complementary and their combined use enhances the security of Internet communications. This paper presents a theoretical framework about some issues that are impacted by the use of steganography such as Information Security, Cryptography and Computer Forensics. The proposal also addresses practical tests with some free steganography tools, found on the web, using different techniques and so the effectiveness of each technique will be assessed in masking of digital information in relation to the attacks made through Digital Forensics Expertise.

Keywords: Information. Security. Digital Forensics Expertise. Cryptografy. Stanography.

LISTA DE ILUSTRAÇÕES

Lista de Abreviaturas e Siglas

ASCII	American Standard Code for Information Interchange
BMP	Bitmap
CRCs	Check Redunce Codes
DB	Decibel
DOC	formato de documento do Office Word
GIF	Graphics Interchange Format
JPEG/JPG	Joint Photographic Experts Group (tipo de formato de imagem)
MP3	Moving Picture Experts Group 1 (MPEG) Audio Layer 3 (formato de compactação de áudio)
LSB	Last Significant Bit
MP4	formato de compactação de áudio e vídeo
NTFS	New Technology File System (sistema de arquivos)
PDF	Portable Document Format (formato de arquivo)
RGB	Red, Green e Blue
SAH	Sistema Auditivo Humano
TXT	Texto sem formatação
WAV	Waveform Audio

SUMÁRIO

Capítulo 1 - Introdução

Com o avanço da tecnologia, a troca de informações aumentou estrondosamente e a Internet se tornou o meio de comunicação mais utilizado, não só para comunicação em si, mas também para pesquisas escolares e como meio de fornecer serviços que envolva investimentos. Inicialmente não se previa esse crescimento tão rápido, muito menos que pudessem aparecer pessoas especializadas em roubar informações e utilizá-las com o objetivo terroristas cometendo atentados contra as nações e os seres humanos.

A guerra da informação é uma vertente que amedronta grandes empresas e o próprio governo, pois o uso indevido da informação pode destruir grandes negócios em poucos minutos.

Para não serem descobertas, as pessoas que praticam crime na Internet, denominado cibercrime, se aproveitam de técnicas de segurança da informação, desenvolvidas para o meio digital. Atualmente, uma técnica que consiste no ocultamento de informações e está sendo muito utilizada é a Esteganografia.

A Esteganografia utiliza textos, imagens, sons e vídeos para esconder informações de forma que as mesmas passem despercebidas aos olhos humanos. Acredita-se que grandes atentados terroristas como os de 11 de Setembro de 2001, tenham sido estruturados e planejados utilizando esteganografia como principal meio de comunicação. Assim sendo, uma pessoa com um passatempo de salvar arquivos pornográficos, pode esconder a evidência de crimes de pedofilia com o uso da esteganografia.

Os crimes na Internet se tornaram um desafio para as autoridades e são poucos os trabalhos sobre o assunto no Brasil assim sendo é crescente a necessidade de novas pesquisas nessa linha, considerando que a utilização de computadores em atividades criminosas é cada vez mais comum.

1.1 Objetivos

1.1.1 Objetivo geral

Explorar técnicas de Esteganografia Digital, criptografadas ou não, que consistam no ocultamento de informações, em arquivos de computador. Colaborando assim com usuários que tenham interesse nessa área, com a intenção de adquirir novos conhecimentos, e também com o perito forense computacional, que tem por necessidade conhecer e explorar as diversas técnicas existentes que a principio são desenvolvidas tendo por objetivo a segurança da informação, mas que também são consideradas técnicas anti-forense pelo seu uso ilegítimo, obrigando investigadores a criar novos procedimentos de análise em um crime digital.

1.1.2 Objetivos específicos

- Estudar métodos de Esteganografia e Perícia Forense Digital;
- pesquisar *softwares* que utilizem técnicas diferentes de Esteganografia;
- pesquisar *softwares* de Perícia Forense Digital, que possibilitem analisar a estrutura de um arquivo digital;
- utilizar critérios de segurança da informação para classificar as técnicas de Esteganografia;
- evidenciar pontos fortes e fragilidades de cada técnica.

1.2 Justificativa

Atualmente a Criptografia está sendo utilizada como critério de segurança no âmbito computacional. A maioria das pessoas não tem conhecimento desse fato, no entanto boa parte das conexões feitas através da Internet é criptografada de modo a prover maior segurança das informações.

Já a uso da Esteganografia vem desde antes de Cristo, e suas técnicas conseguem suprir um ponto que a criptografia não consegue: a ocultação da mensagem, um ponto crucial para a segurança da informação. Dessa forma, a Esteganografia foi, e continua sendo de grande importância no cenário mundial.

Técnicas de segurança digital podem ser usadas por razões ilegítimas, no caso da Esteganografia, por exemplo, roubar dados e esconder em um arquivo e emiti-los para fora por meio de um inocente *e-mail*, é uma forma de cometer um crime sem levantar suspeitas. Por está razão a esteganografia é fonte de muita discussão, particularmente quando se suspeitou que terroristas, nos ataques de 11 de setembro, podem tê-la usado para comunicações secretas. Enquanto nenhuma conexão for provada, o interesse indica a eficácia da esteganografia como meios de obscurecer dados.

No entanto, é difícil encontrar material que explore as diversas técnicas existentes de uma maneira que seja possível à classificação de cada uma delas dentro dos critérios de segurança da informação.

Uma pesquisa desenvolvida no ano de 2012 pela *Norton Cybercrime Report* aponta que o cibercrime custa US$ 8 bilhões ao ano no Brasil.

1.3 Estrutura do Trabalho

O **Capítulo 1** contém a introdução do trabalho juntamente com os objetivos e a justificativa para a elaboração da proposta. O **Capítulo 2** contém o referencial teórico**,** onde são abordados conteúdos de suma importância, tais como: informação, segurança da informação, o papel da pericia forense digital e, por fim, técnicas de segurança para a informação digital e a forma como estão sendo usadas nos dias atuais. O **Capítulo 3** contém a metodologia**,** nela são elencados os *softwares* e métodos utilizados para atingir o objetivo proposto. Por fim no **Capítulo 4**, são apresentados os resultados obtidos na realização deste trabalho.

Capítulo 2 - Referencial Teórico

2.1 Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido (ABNT - NBR ISO/IEC, 2006, p. 02).

Segundo Silva (c2008):

> A informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando ela ser lida, modificada ou até mesmo apagada.

Um dos principais bens da humanidade no século XXI é a informação, isso devido à alta tecnologia disponível e ao alcance de todos. O diferencial de profissionais, empresas e grandes organizações hoje é a informação, desde uma técnica de marketing, vendas, e mesmo a forma de apresentar ou colocar um produto no mercado, quando alcançam resultados positivos se tornam alvo de concorrentes, que chegam ao ponto de colocar “olheiros”, para ter acesso a essas informações. A indústria automobilística é um grande exemplo, quando aparecem vários automóveis com *design* parecidos, mas de marcas diferentes.

Diante dessas vertentes surge um novo campo de estudos essencial nos dias atuais que é a segurança da informação.

A segurança da informação é composta por três pilares fundamentais: a confidencialidade, a integridade e a disponibilidade.

Segundo Jasper (2009), cada uma delas reúnem as seguintes características:

- Confidencialidade: garante que somente as entidades permitidas poderão entender o significado da informação. Sigilo requer confidencialidade.
- Integridade: garante que a informação não foi modificada desde a sua geração. Se a informação estiver correta, deve continuar correta, se estiver errada, deve continuar errada.

- Disponibilidade: garante que somente as entidades autorizadas terão acesso à informação e que estas sempre estarão disponíveis quando solicitadas.

Segundo Silva (c2008), “A Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentindo de preservar o valor que possuem para um indivíduo ou organização”.

Para que essa proteção aconteça em uma organização ou empresa, onde envolvem várias pessoas, faz-se necessário adotar políticas de segurança, que utilize de regras para que fique claro a importância de uma informação e até que ponto a mesma pode ser exposta, alterada ou usada.

A política de segurança define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza, e as penalidades às quais está sujeito, caso não a cumpra.

> Uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade) (NIC BR, 2003).

A Internet como principal meio de comunicação, está sendo usada também para transações comerciais envolvendo grandes quantidades de valores financeiros. É importante se atentar ao fato de que na Internet não existem fronteiras que possam limitar essas transações e todos contatos feitos por meio da mesma. Este ambiente se tornou extremamente propício para o surgimento e o crescimento dos chamados crimes cibernéticos, principalmente devido à possibilidade do anonimato

de seus usuários, à facilidade de uso da grande rede e à sua conexão com todo o mundo (COELHO; BENTO, 2004).

Segundo Fernandes e Abreu (2008 p. 140; 141):

> A operação de Segurança da informação geralmente abrange atividades relacionadas à segurança da infra-estrutura de TI, no tocante aos aplicativos, monitoramento da segurança, conscientização para a segurança da informação, gestão de problemas de segurança (resolução de erros conhecidos), elaboração de planos de continuidade do negócio, análises de vulnerabilidades de segurança da informação, estudos de novas tecnologias em segurança da informação, gestão da implantação de novos dispositivos físicos e de software relativos à segurança da informação etc.

De acordo com Izquierdo (2007), a segurança da informação deve focar não somente o setor de informática, rede e assemelhados, como também garantir que as informações em qualquer formato: mídias eletrônicas, papel e até mesmo conversações pessoais ou por telefone, estejam protegidas contra o acesso por pessoas não autorizadas, estejam sempre disponíveis quando necessárias, e que sejam confiáveis, ou seja, não tenham sido corrompidas ou adulteradas por atos de pessoas mal intencionadas.

Nessa visão pode-se entender que a segurança da informação é um assunto estratégico, e deve ser tratado no nível apropriado da organização e que mesmo diante dos riscos relacionados ao uso de computadores e da Internet, não é possível deixar de usar estes recursos.

“A segurança da informação vem sendo cada vez mais discutidas e de grande relevância para a Tecnologia da Informação. Especialistas buscam desenvolver técnicas para garantir a segurança de usuários na internet [...]” (PEREIRA, 2013, p. 80).

Diversos mecanismos são desenvolvidos com o objetivo de garantir a segurança da informação digital.

“Um mecanismo de segurança é qualquer processo projetado para detectar, impedir ou permitir a recuperação de um ataque” (SPANGHERO; MARQUES; CERVANTES, 2010). Dentre os vários existentes a assinatura digital e os protocolos de autenticação são exemplos de mecanismos que estão sendo utilizados para

garantir a veracidade e a proteção de informações importantes que são enviadas pela internet.

2.1.1 Assinatura Digital

Normalmente a veracidade de um documento é dada pela assinatura presente nele, somente assim ele pode ser levado em conta legalmente. Na Internet encontramos um problema, como dar veracidade e autenticidade a um documento enviado pela *Web*?

> A assinatura digital é uma tecnologia que permite dar garantia de integridade e autenticidade a arquivos eletrônicos. É um conjunto de operações criptográficas aplicadas a um determinado arquivo, tendo como resultado o que se convencionou chamar de assinatura digital (CJF, c2012).

A assinatura digital permite comprovar que a mensagem ou arquivo não foi alterado, e que foi assinado pela entidade ou pessoa que possui a chave criptográfica (chave privada) utilizada na assinatura.

> Na assinatura digital, a chave privada é usada para cifragem e a chave pública é usada para decifragem da mensagem. Isto é possível porque os algoritmos de cifragem/decifragem atuais, tal o RSA, são fórmulas matemáticas e suas estruturas são similiares, Forouzan (2004, p. 713).

2.1.2 Protocolos de Autenticação

Autenticação é a técnica onde um processo confirma a identidade de algo ou alguém. Na computação, o conceito de Protocolo de Autenticação é utilizado para atestar que um programa ou uma página na Internet é confiável, algumas maneiras para validar uma identidade incluem uso de senhas, certificados, assinaturas digitais (AMOROSO, 2009). A Figura 1 reúne alguns Protocolos de Autenticação e uma breve definição de cada:

Protocolos de autenticação	Descrição
Autenticação Kerberos V5	Um protocolo usado com uma senha ou um cartão inteligente para logon interativo. É o principal mecanismo de segurança para autenticação em um domínio.
Autenticação SSL/TLS	Um protocolo usado quando um usuário tenta acessar um servidor seguro.
Autenticação NTLM	Um protocolo usado quando o cliente ou servidor usa uma versão anterior do Windows.
Autenticação Digest	A autenticação Digest transmite credenciais através da rede como um hash MD5 ou Message Digest.
Autenticação de passaporte	A autenticação de passaporte é um serviço de autenticação de usuário que oferece logon único.

Figura 1 - Protocolos de Autenticação.
Fonte: Microsoft (c2013). Adaptada pelo autor.

Por mais seguros que pareçam os sistemas de computação, vem sendo violados e paralelamente, novas maneiras para inibir a ação “de invasores” vêm sendo criadas. Porém todos são conhecedores da falta de uma legislação específica, e da dificuldade de descobrir esses invasores, em função disso, os criminosos se aproveitam da complexa tarefa de identifica-los e puni-los. Surge então, a necessidade de identificar os criminosos e comprovar seus atos. Esse esforço de produzir provas contundentes de uma violação digital é conhecido como Computação Forense.

2.2 Perícia Forense

Segundo Costa (2005), perícia é ato traduzido por relatório, laudo, documento ou outra forma de expressão, emitido por profissional que detém conhecimento específico, em matéria a ser discutida. No caso da perícia criminalística a perícia é realizada por perito oficial ou, na ausência deste, por perito nomeado pelo juiz do caso.

Já a Perícia Forense é uma área relativamente nova e tornou-se uma prática investigativa importante tanto para as empresas quanto para a polícia. Utiliza de métodos científicos para identificar, preservar, analisar e documentar evidências do caso investigado (FREITAS, 2011).

2.2.1 Computação Forense

Computação Forense é a ciência que trata do exame, análise e investigação de um incidente computacional, ou seja, que envolvam a computação como meio, sob a ótica forense, sendo ela civil ou penal. Na criminalística a Computação Forense trata o incidente computacional na esfera penal, determinando causas, meios, autoria e consequências (COSTA, 2005).

Vargas (2007), relata que por conta da área de pesquisa Forense Computacional também ser recente, são poucos os trabalhos sobre o assunto no Brasil, entretanto é crescente a necessidade de desenvolvimento nesse sentido, considerando que a utilização de computadores em atividades criminosas é cada vez mais comum.

O profissional responsável pela perícia forense é classificado como perito, para esse profissional existe duas qualificações, o perito criminal é um servidor público, a serviço da justiça, que realiza a análise crítica e científica dos locais onde ocorreram crimes (BRASIL PROFISSÕES, c2007-2013). E o perito judicial, é a pessoa que declara ante um tribunal e que detém a característica particular de possuir conhecimentos técnicos em determinada ciência, arte ou ofício, os quais lhe permite emitir opiniões sobre materiais relevantes para a resolução de um juízo (INFO ESCOLA, c2006-2013).

2.2.2 Perito Forense Computacional

O perito forense computacional tem que juntar competências das mais variadas áreas do conhecimento para atuar especificamente em um único campo. Queiroz e Vargas (2010) fazem uma lista com dicas importantes para ajudar a traçar o perfil desse profissional:

- Ter formação superior em tecnologia;
- Se possível, possuir mestrado acadêmico ou profissional (dentro da área);
- Ter especialização;
- Ser proficiente em língua estrangeira (de preferência em inglês);
- Ter conhecimento das leis que envolvam crimes praticados com o auxílio do computador e da Internet;
- Ter o domínio tecnológico;
- Ter larga experiência profissional (*expertise*);
- Ter interesse real pela área de perícia forense digital;
- Ser interessado em todos os assuntos que dizem respeito à área de perícia forense;
- Ter boa redação (estudar concordância e verbos é fundamental);
- Estudar técnicas de redação jurídicas;
- Ter conhecimento sobre os termos da linguagem do Direito.

Não é o propósito deste trabalho adentrar na teoria da Computação Forense, no entanto serão abordadas as metodologias, bem como, as principais características de cada etapa do processo de investigação, tendo em vista a utilização de uma ferramenta de perícia forense para a realização da análise de imagens contendo arquivos ocultos, objetivo específico desse trabalho.

Para iniciar o procedimento de perícia em um equipamento, existem duas metodologias possíveis de serem adotadas: a) Live Forensics e b) Post Mortem Forensics, sendo que uma delas deve ser escolhida pelo perito.

De acordo com Pereira (2010, p. 3): a **Live Forensics** se caracteriza pela investigação do equipamento ainda em funcionamento, esse método é o único que

permite a aquisição de informações voláteis. Já a **Post Mortem Forensics**, é caracterizada pela análise realizada após o desligamento do equipamento.

A escolha da metodologia adequada vai depender do tipo de delito que será investigado. Após ser definido qual método será utilizado, é iniciado o processo de investigação. Na sequência serão abordadas as características de cada etapa em conformidade com Pereira (2010).

a) **Coleta de dados**: Necessita de mais cuidados, pois é nela que toda a massa crítica de dados será coletada, sendo necessário cuidado especial para manter a integridade das informações. Outras atividades que são realizadas nesta etapa estão relacionadas ao equipamento, que deve ser identificado, devidamente embalado, etiquetada as suas partes e suas identificações registradas no documento.

b) **Exame dos dados**: O objetivo é separar as informações relevantes ao caso de outras sem importância, como os arquivos do próprio sistema. Antes de iniciar o processo é preciso definir quais as ferramentas que serão utilizadas para o exame dos dados. Esta escolha está relacionada a cada tipo de investigação e informações que estão sendo procuradas. Diante disso, pode se definir ferramentas que consigam trazer um número maior de dados úteis. Peritos geralmente utilizam filtros de arquivos, busca por palavras-chave, entre outros procedimentos para agilizar a busca por evidências.

c) **Análise das Informações**: As informações anteriormente separadas são analisadas com o intuito de encontrar dados úteis que auxiliem na investigação do caso. Todos os dados encontrados considerados relevantes devem ser correlacionados com informações referentes à investigação, para que assim seja possível realizar a conclusão.

d) **Interpretação dos resultados**: Nesta última etapa, o objetivo é apresentar um laudo (relatório técnico), que deve informar com toda a veracidade possível, o que foi encontrado nos dados analisados. Todo o processo pericial desde o início, ferramentas e informações que comprovem a integridade das informações devem ser relatadas.

De acordo com o descrito nas etapas anteriormente apresentadas, a Figura 2 demonstra de forma gráfica como é todo o processo de investigação em computação forense.

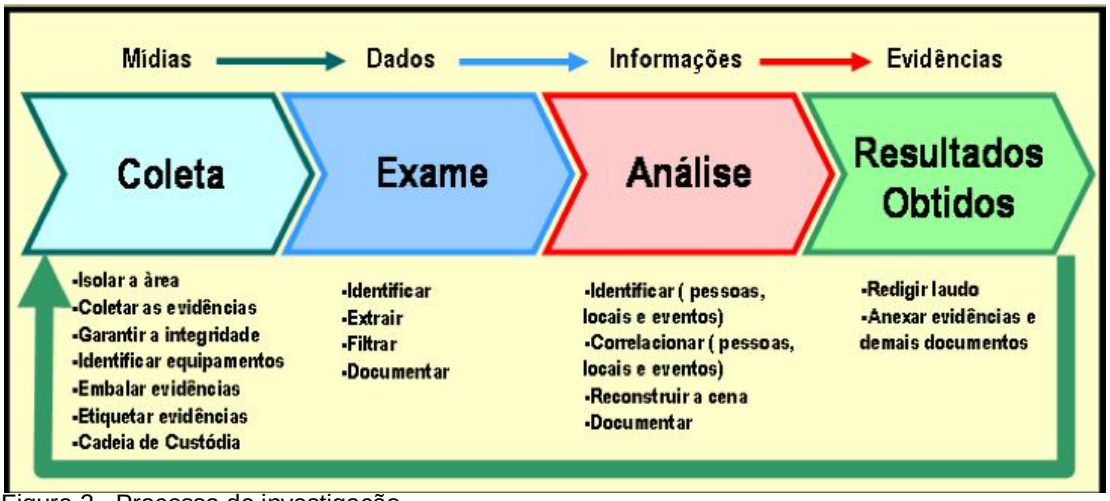

Figura 2 - Processo de investigação.
Fonte: Pereira, (2010).

Para a tarefa de investigação a perícia forense em informática conta com diversas ferramentas que auxiliam na busca e padronização de evidências. E que são capazes de atender a todas as etapas de um processo de perícia.

2.2.3 Ferramentas Forense Digital

Existem aqueles softwares reconhecidos mundialmente por órgãos policiais e/ou periciais, como Encase e o FTK. Porém o custo desses softwares é muito alto. Em contrapartida existem softwares livre, incluindo distribuições Linux específicas para forense digital, com centenas de softwares para este fim (Pereira, 2010).

2.2.3.1 FDTK

O FDTK (Forense Digital *ToolKit*) - UbuntuBr, é um projeto livre que objetiva produzir e manter uma distribuição para coleta e análise de dados em Perícias de Forense Computacional. Na Figura 3 é possível visualizar algumas ferramentas utilizadas para o exame dos dados coletados, e a tela principal da ferramenta.

Figura 3 - Menus FDTK-UbuntuBr V.3.
Fonte: Neukamp (2008).

2.2.3.2 BackTrack

BackTrack, tem como foco testes de seguranças e testes de invasão. A Figura 4 apresenta a tela principal do Live-Cd BackTrack em sua versão 4.0. Em destaque o seu menu mostra um conjunto reduzido de ferramentas de forense digital, fato este justificável pois o foco desta distribuição é realizar teste de invasão, área na qual este disponibiliza um conjunto maior de ferramentas.

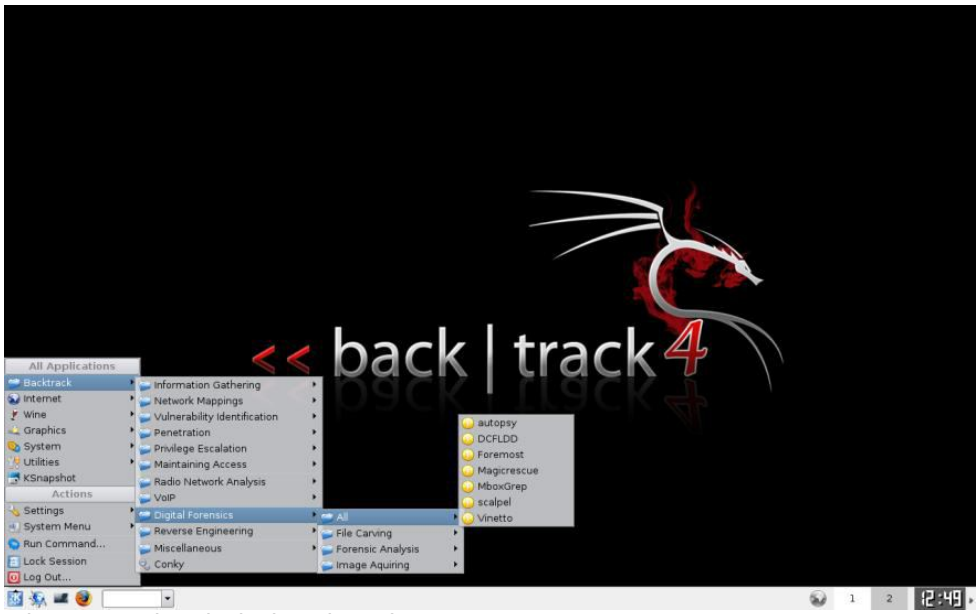

Figura 4 - Tela Principal BackTrack.
Fonte: Rover (200-?).

2.2.3.3 Helix

Trata-se de uma distribuição dedicada à investigação ou ciência forense em informática. Não monta *swap* e não toca no HD. Na Figura 5 é exibida a imagem da área de trabalho do Live-Cd Helix na versão 3.0, e em destaque encontra-se a entrada do seu menu que contém algumas de suas ferramentas de perícia digital.

Figura 5 - Área de trabalho do Live-Cd Helix V. 3.0.
Fonte: Rover (200-?).

2.2.3.4 PeriBr

A PeriBr, contém várias ferramentas de forense. Desenvolvido como trabalho de pós-graduação em perícia digital da Universidade Católica de Brasília. A Figura 6 demonstra a tela principal da PeriBr em sua versão 1.0.

Figura 6 - Tela principal PeriBr em sua versão 1.0.
Fonte: Rover (200-?).

São necessárias constantes atualizações por parte dos peritos, afinal na medida em que a tecnologia evolui os bandidos também mudam a forma de cometer o crime. Os sistemas são mutantes, a cada dia surgem novas versões, vírus são lançados diariamente, consequentemente têm-se variâncias de golpes e fraudes. O perito forense computacional não pode se estagnar, deve se atualizar todos os dias em relação às técnicas dos criminosos digitais (MILAGRE, 2011).

Na maioria das vezes são técnicas destinadas à segurança da informação, quando utilizadas de forma ilícita são classificadas como técnicas Anti-forense.

2.2.4 Conceito Anti-forense

“Anti-forense são métodos de remoção, ocultação e subversão de evidências com o objetivo de mitigar os resultados de análises forenses computacionais” (HENRIQUE, 2006, p. 4).

> Alguns autores defendem que técnicas que “embaralham” ou “ocultam” a informação, tem por objetivo puramente malicioso, buscando burlar técnicas forenses para se esconder e camuflar seus atos. Outros autores defendem que esta técnica objetiva aprimorar técnicas de segurança, e consequentemente de computação forense, obrigando investigadores a criar novos procedimentos de análise em um crime digital (BARRETO, 2009, p. 02).

Existem várias maneiras de se proteger eletronicamente, usando técnicas de segurança como a criptografia uma das mais utilizadas atualmente, mas não é a única. Outras técnicas também podem ser usadas, mas neste trabalho serão focadas apenas duas: Criptografia e Esteganografia.

2.3 Criptografia

Criptografia é a ciência que estuda as formas de se escrever uma mensagem em código.

“A palavra criptografia é de origem grega e significa “escrita secreta”. Entretanto, hoje em dia, o termo criptografia refere-se à ciência e à arte da transformação de mensagens, tornando-as seguras e imunes a ataques.” (FOROUZAN, 2004).

De acordo com Evaristo (1999), podemos entender a criptografia como sendo a ação de reescrever um texto de modo que apenas as pessoas autorizadas pelo autor do texto sejam capazes de compreendê-lo.

A criptografia esconde o conteúdo de uma mensagem, tornando-a incompreensível para pessoas não autorizadas, mas a existência da mensagem é conhecida. Considerada como a ciência e a arte de escrever mensagens em forma

cifrada ou em código, é um dos principais mecanismos de segurança que se pode usar para proteger dos riscos associados ao uso da Internet.

> Na computação, as técnicas mais conhecidas envolvem o conceito de chaves, as chamadas chaves criptográficas. Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação (ALECRIM, c2009).

Existem duas técnicas de criptografia a criptografia convencional, ou simétrica, e a criptografia por chave pública, ou assimétrica, ambas envolvem o conceito de chaves, as chamadas chaves criptográficas.

2.3.1 Criptografia de Chave Simétrica

Criptografia de chave simétrica é um tipo de chave mais simples, onde o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação (ALECRIM, c2009).

A Figura 7 ilustra o processo de criptografia de chave simétrica.

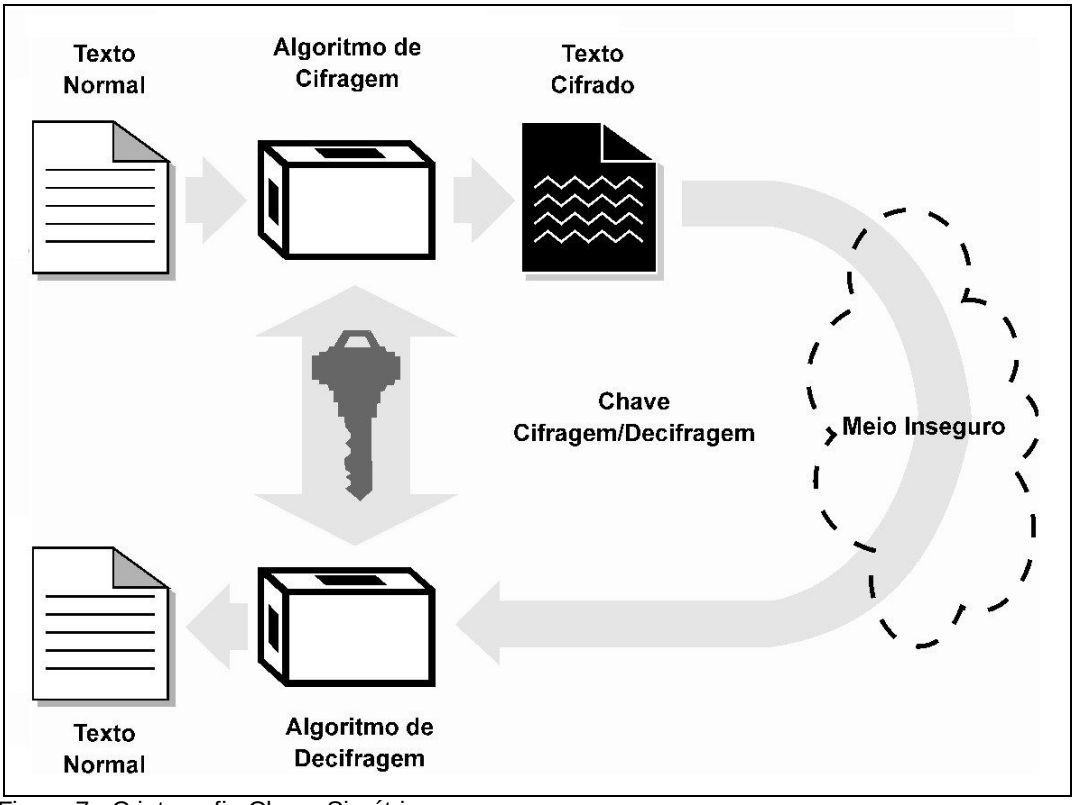

Figura 7 - Criptografia Chave Simétrica
Fonte: Kobuszewski, (2004).

Segundo Forouzan (2004, p. 695):

> Um algoritmo de chave simétrica possui duas desvantagens. A cada par de usuários deverem estar associados uma única chave. Isto significa que se *N* pessoas no mundo quiserem usar este método, serão necessárias *N*(*N* - 1)/2 chaves simétricas. Por exemplo, para que 1 milhão de pessoas possam se comunicar são necessárias 500 bilhões de chaves simétricas. A distribuição das chaves entre duas partes pode ser difícil.

Existem vários algoritmos que usam chaves simétricas, como o DES, o IDEA, o RC e o BLOWFISH. A Figura 8 descreve as principais características de cada um.

Algoritmo	**Tamanho da Chave**	**Descrição**
DES (Data Encryption Standard)	64 *bits*	Criado em 1977, sendo muito usado desde então. Foi adotado pelo *National Bureau of Standards, atualmente conhecido como National Institute of Standards and Technology*. Basicamente seu funcionamento consiste na criptografia de blocos de 64 *bits* de entrada com uma chave de 56 bits, gerando blocos de 64 *bits* como saída. Utiliza o Algoritmo de Feistel.
DES Triplo	112 *bits*	Alternativa do DES original, com variação de três diferentes chaves. O DES é aplicado três vezes, com a mesma chave ou com chaves diferentes.
IDEA (International Data Encryption Algorithm)	128 *bits*	Criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo de cifra de bloco que tem uma estrutura semelhante ao DES. Sua implementação em *software* é mais fácil do que a implementação deste último. Como uma cifra de bloco, também é simétrica. O algoritmo foi concebido como um substituto para o *Data Encryption Standard* (DES). O algoritmo é usado tanto para a cifragem quanto para a decifração.
RC (Rivest Ciphers) RC2, RC4 e RC5	Tamanho variável	Todas as suas versões são algoritmos simétricos. O RC2 caracteriza-se por blocos de entrada de 64 *bits*, contudo podem ser usadas chaves com vários tamanhos. Já o RC4 não é uma técnica de blocos, mas sim de fluxo de entrada de *bytes* e saída de *bytes* cifrados ou decifrados conforme o caso. Esta é uma técnica atualmente muito usada, por um lado porque funciona em fluxo continuo e por outro lado porque é bastante rápida. Por fim o RC5 é uma técnica de cifragem em bloco, ele caracteriza-se por uma grande flexibilidade e possibilidade de parametrização.
BLOWFISH	32 a 448 *bits*	A criptografia é feita através de uma função com 16 interações. A cifragem do texto é feita em blocos de 64 ou 128 bits, nos quais os bits não são tratados separadamente, mas em grupos de 32 bits. A fim de aumentar sua eficiência, foi escolhido usar na confecção deste algoritmo funções simples para os microprocessadores, tais como XOR, adição e multiplicação modular.

Figura 8 - Algoritmos Simétricos.
Fonte: Jasper, (2009). Adaptado pelo autor.

2.3.2 Criptografia de Chave Assimétrica

O método de criptografia assimétrica ou criptografia de chave pública trabalha de forma bem mais segura que a criptografia simétrica, mas perde em desempenho. O método de chave pública utiliza um par de chaves, uma chave para criptografar (chave pública) e outra para descriptografar (chave privada), além de utilizar algoritmos bem mais complexos (PONCE, 2012). A Figura 9 ilustra o processo de chave assimétrica.

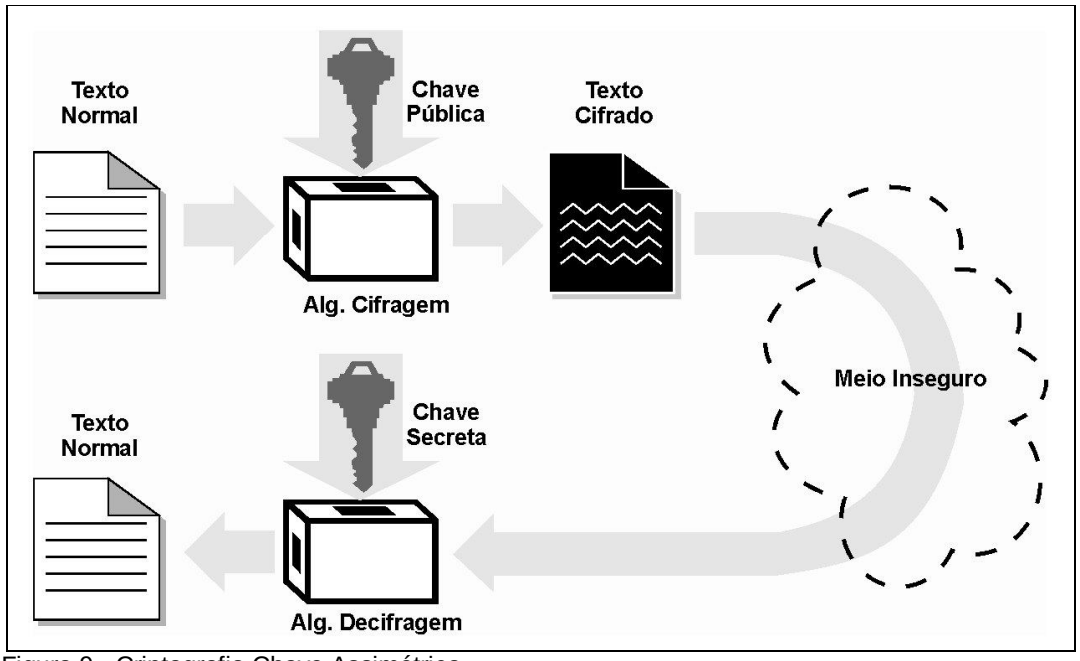

Figura 9 - Criptografia Chave Assimétrica.
Fonte: Kobuszewski, (2004).

> A chave pública tem a vantagem sobre a chave secreta no sentido de viabilizar a comunicação segura entre pessoas comuns. Com a chave pública também acaba o problema da distribuição de chaves existente na criptografia por chave secreta, pois não há necessidade do compartilhamento de uma mesma chave, nem de um pré-acordo entre as partes interessadas. Com isto o nível de segurança é maior (KOBUSZEWSKI, 2004, p. 19).

De acordo com Oliveira (2012), uma desvantagem do sistema de chave pública é a complexidade empregada no desenvolvimento dos algoritmos, que devem ser capazes de reconhecer as duas chaves e relacionar as mesmas no momento oportuno, o que acarreta num grande poder de processamento computacional.

Dois dos principais algoritmos de chave pública são apresentados na Figura 10.

Algoritmo	Descrição
RSA (Rivest, Shamir and Adleman)	Criado em 1977 por *Ron Rivest, Adi Shamir e Len Adleman* nos laboratórios do MIT (*Massachusetts Institute of Technology*), O pioneiro das chaves públicas é o padrão atual para criptografia de chave assimétrica. Nele, números primos são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor. Para, descobrir os dois primeiros números a partir do terceiro (através de uma fatoração) é muito trabalhoso. Se dois números primos grandes forem usados na multiplicação, será praticamente inviável descobri-lo, exigindo muito processamento, tornando essa tarefa praticamente inviável. Basicamente, a chave privada no RSA são os números multiplicados e a chave pública é o valor obtido.
El Gamal e DSS	Criado em 1984 por Taher ElGamal, esse algoritmo utiliza o “logaritmo discreto” para se tornar seguro tendo em vista o nível de dificuldade da equação, sendo muito utilizado em assinaturas digitais. O algoritmo consiste na criação de um código a partir de uma chave privada, que autentica um documento de modo que qualquer tentativa de modificação é detectada, além de verificar o remetente com um “RG digital”.

Figura 10 - Algoritmos Assimétricos.
Fonte: Jasper, (2009). Adaptado pelo Autor.

Embora muito eficaz o uso da criptografia acaba chamando atenção de curiosos, tendo em vista que ao notar que ali existe uma mensagem criptografada (incompreensível), pode-se deduzir que o conteúdo da mesma é importante ou suspeito, e incriminante por si só, como por exemplo em países onde o uso de criptografia é ilegal. Para resolver esse problema é possível utilizar uma técnica chamada Esteganografia, que inclusive é um ramo particular da criptografia, que consiste em fazer com que uma informação seja camuflada, e essa passará despercebida por um usuário que não tem conhecimento da mesma (JASPER, 2009).

É comum o uso combinado de técnicas de esteganografia e criptografia para garantir maior segurança da mensagem a ser ocultada, como será mostrado nos capítulos seguintes. Dessa forma, ao se ocultar uma mensagem previamente criptografada requer que um atacante, para revelar integralmente a mensagem, descubra sua existência e decifre seu significado, ambos ocultos por técnicas distintas (KOBUSZEWSKI, 2004).

2.4 Esteganografia

Segundo Coelho e Bento (2004, p. 15), “esteganografia é uma palavra de origem grega, onde Stegano significa escondido ou secreto e Grafia: escrita ou desenho”.

De acordo com Petri (2004, p.07), “esteganografia é a arte de esconder mensagens e informações por meio de métodos, tendo como objetivo a comunicação em segredo”.

Não se deve confundir criptografia com esteganografia, pois o primeiro esconde o conteúdo de uma mensagem tornando-a ilegível, mas a existência da mensagem é conhecida, provê privacidade, pois oculta o significado da mensagem, já o segundo esconde a existência da mensagem (provê sigilo), ocultando o fato de que a mensagem existe. Uma mensagem oculta através de técnicas esteganográficas não atrai atenção a si mesma, ao transmissor ou ao receptor (COUTINHO, 2008).

> Os dois métodos (criptografia e esteganografia) podem ser combinados para aumento da segurança. Por exemplo, pode-se criptografar uma mensagem e em seguida, utilizar a técnica de esteganografia, trocando-se os bits menos significativos de uma imagem digitalizada pelos bits da mensagem criptografada, e então transmitir a imagem. Se a imagem for interceptada, o adversário primeiro precisará descobrir a mensagem dentre os bits da imagem, e, após isso, poderá tentar decriptografá-la (KOBUSZEWSKI, 2004, p. 24).

Um exemplo básico de técnica moderna de esteganografia é a alteração do *bit* menos significativo de cada *pixel* de uma imagem colorida, de forma a que ele

corresponda a um *bit* da mensagem a ser ocultada. Essa técnica, apesar de não ser ideal pouco afeta o resultado final de visualização da imagem (OLIVEIRA, M. 2007).

A Figura 11 ilustra o processo de como é ocultado o arquivo em uma imagem digital.

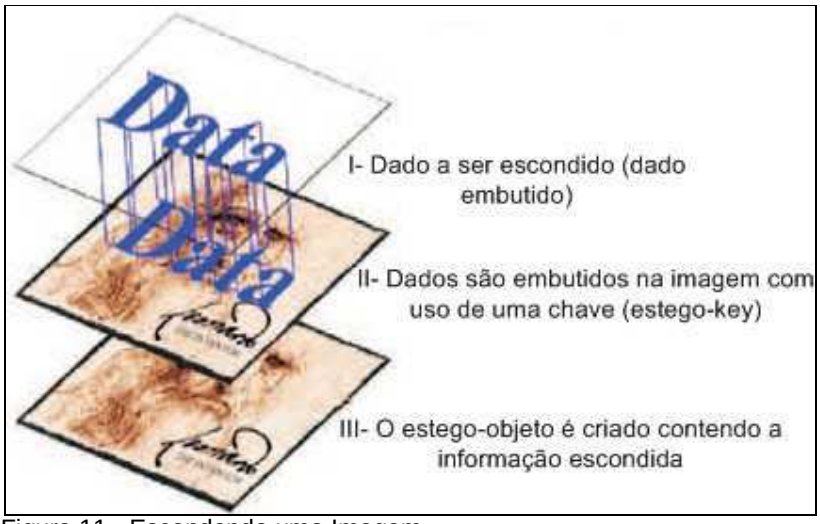

Figura 11 - Escondendo uma Imagem.
Fonte: Julio; Brazil; Albuquerque, (2007).

> O objeto de mídia utilizado para inserção de material oculto recebe a nomenclatura de Objeto de Cobertura. Já o objeto contendo a mensagem oculta recebe o nome de Estego Objeto (*stego object*). Por exemplo se for inserida uma mensagem texto (ASCII) em um documento texto, este receberá o nome de Estego Texto (*StegoText*). Se for inserido um texto no interior de uma imagem esta receberá o nome Estego Imagem (*StegoImagem*) (CARVALHO, 2008, p. 06).

2.4.1 Aspectos Históricos

A esteganografia é uma arte antiga. Suas origens remontam à antiguidade. O primeiro registro conhecido sobre utilização de esteganografia está no livro História de Herótodo, por volta do ano 440 a.C. Onde para enviar uma mensagem secreta foi escolhido um escravo considerado mais fiel entre os demais, lhe raspam a cabeça e tatua uma mensagem em seu couro cabeludo, quando o cabelo do escravo cresceu o suficiente foi enviada a mensagem (COELHO; BENTO, 2004).

Johannes Trithemius, em sua trilogia, descreve ainda o código “Ave Maria”. Tabelas associam letras a certas palavras que, se substituídas na ordem correta, resultam numa mensagem codificada que aparenta ser uma inocente oração. Isso é realizado utilizando-se tabelas com palavras de diferentes classes gramaticais, formando assim sentenças que obedecem a gramática de uma linguagem (COUTINHO, 2008).

Ainda em "História" de Heródoto, consta que na Grécia antiga o meio de escrita era texto em tabletes duplos cobertos de cera. Os tabletes pareciam estar em branco e sem uso, por isso passavam pela inspeção e a mensagem chegava ao seu destino sem ser interceptada por terceiros (COELHO; BENTO, 2004).

Tintas invisíveis também foram muito usadas em esteganografia nos tempos mais modernos e são utilizadas até hoje.

Segundo Petri (2004), as tintas invisíveis começaram a ser utilizadas na Segunda Guerra Mundial. As mensagens escritas por esse tipo de tinta só poderiam ser lidas se o papel fosse aquecido. Outra utilização era escrever a mensagem com tinta invisível sobre um papel, cortá-lo em alguns pedaços e depois rejuntá-los no destinatário.

Outra forma utilizada eram as cifras nulas (mensagens não criptografadas) pelos alemães para esconder mensagens secretas. As cifras nulas, que geralmente pareciam ser mensagens inocentes sobre acontecimentos ordinários, não gerariam suspeitas, não sendo então interceptadas. A disposição do documento também costumava revelar informação. Modulando a posição de linhas e palavras, mensagens poderiam ser marcadas e identificadas. Também na mesma época, surgiram os chamados micro pontos, pois com o advento da fotografia, as

mensagens eram fotografadas e reduzidas ao tamanho de um ponto, para então serem enviadas. A invenção alemã do micro ponto foi considerada pelo Diretor do FBI, J. Edgar Hoover, como a "obra-prima da espionagem inimiga" (COELHO; BENTO, 2004).

Novas tecnologias que armazenavam mais informação em meios nada suspeitos foram desenvolvidas, a detecção de mensagens também foi melhorada. Em termos contemporâneos, a esteganografia evoluiu numa estratégia digital com intuito de esconder um arquivo em algum dos meios multimídia, tais como arquivos de imagem, de áudio ou de vídeo.

2.4.2 Utilização

Como muitas ferramentas de segurança, a esteganografia pode ser usada para uma variedade de razões, algumas boas, outras nem tanto. As finalidades legítimas podem incluir imagens de marca d'água por motivo de proteção de direitos autorais.

Com o crescente aumento da pirataria e de *sites* na Internet onde se pode baixar filmes, músicas e vídeos, esta técnica tem se mostrado uma aliada na proteção dos direitos autorais (JULIO; BRAZIL; ALBUQUERQUE, 2007).

As marcas d'água digitais são similares à esteganografia no que tange à ocultação de dados, os quais parecem ser parte do arquivo original e não são facilmente detectáveis por qualquer pessoa (COELHO; BENTO, 2004). Finalmente, a esteganografia pode ser usada para manter a confidencialidade da informação valiosa, para proteger os dados de possíveis sabotagens, roubo, ou apenas visualização desautorizada. Além disso, pode ser utilizada para a divulgação de mensagens sem o conhecimento da existência dessas mensagens por parte de outros interessados. Um exemplo é a inserção de mensagem de texto em uma figura em formato GIF ou BMP, usando o programa S-tools, disponível para Windows e distribuído livremente.

2.4.3 Requisitos para Sistemas Esteganográficos

De acordo com Julio, Brazil e Albuquerque (2007), existem três requisitos importantes que devem ser satisfeitos para qualquer sistema esteganográfico ser considerado adequado:

a) **Segurança** - Em termos de praticidade, um sistema pode ser considerado seguro, ou esteganograficamente forte, se não for possível descobrir a presença de stego-conteúdo usando qualquer meio acessível.
b) **Carga Útil** - Diferentemente de marca d'água, que precisa embutir somente uma quantia pequena de informações de direitos autorais, a esteganografia é direcionada à comunicação escondida e, portanto normalmente exige capacidade de inclusão suficiente. Os requisitos de segurança e carga útil são frequentemente contraditórios, dependendo da necessidade, um compromisso deve ser buscado.
c) **Robustez** - embora robustez contra ataques não seja uma prioridade importante, como em marcas d'água, ter a capacidade de resistir à compressão é certamente desejável, pois a maioria das imagens JPEG coloridas são comprimidas antes de serem colocadas on-line.

2.4.4 Processo da Esteganografia

O dado embutido (*embedded data*) é a mensagem que se deseja enviar em sigilo. Este dado geralmente fica escondido em uma mensagem aparentemente inocente, chamada de recipiente ou de objeto cobertura (*container ou cover-object*), produzindo um *estego-objeto* (*stego-object*) ou estego-recipiente (*stego-carrier*), ou seja, um arquivo com uma mensagem embutida. Uma estego-*key* ou simplesmente chave é utilizada para controlar o processo de esconder, assim como, para restringir detecção e/ou recuperação do dado embutido, somente para quem a conhece, ou conheça parte dela conseguirá recuperar a mensagem oculta (COELHO; BENTO, 2004). A Figura 12 apresenta de forma resumida como funciona o processo de esteganografia.

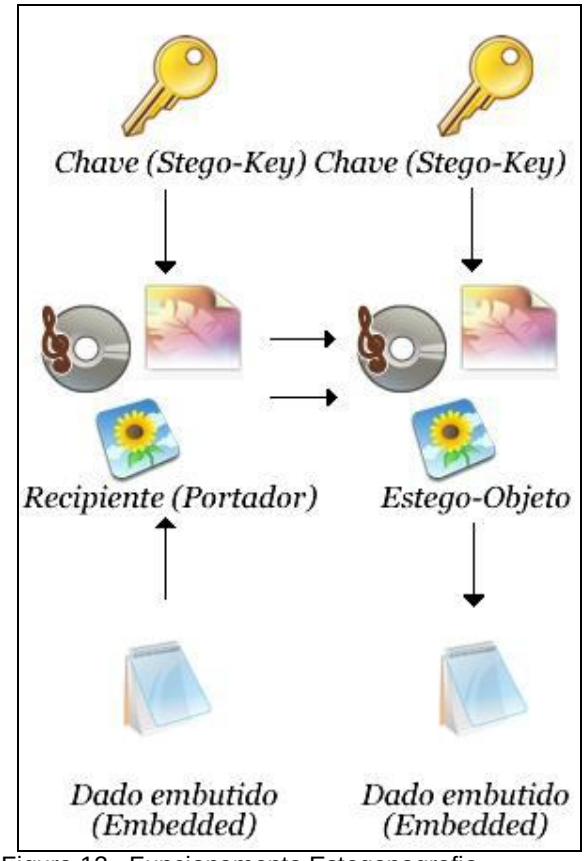

Figura 12 - Funcionamento Esteganografia
Fonte: Jasper, (2009).

2.5 Técnicas de Esteganografia

Técnicas de esteganografia podem ser empregadas em diversos meios, digitais ou não. Nesta etapa será mostrada uma visão geral das técnicas mais comuns e utilizadas atualmente.

2.5.1 Esteganografia em Textos

Métodos modernos de esteganografia incluem cifradores nulos e micro pontos.

De acordo com Julio; Brazil; Albuquerque, (2007, p. 58):

> Cifradores nulos são mensagens nas quais certas letras devem ser usadas para formar a mensagem e todas as outras palavras ou letras são consideradas nulas. Para o uso do cifrador nulo, ambos os lados da comunicação devem usar o mesmo protocolo de uso das letras que formam a mensagem.

Um exemplo do uso de esteganografia utilizando o método cifradores nulos é visto na seguinte mensagem, enviada por um espião alemão durante a Segunda Guerra:

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

Retirando a segunda letra de cada palavra, pode-se ler a mensagem de fato a ser transmitida: "*Pershing sails from NY June 1*" (KOBUSZEWSKI, 2004).

Este é apenas um exemplo trivial, que fica na fronteira entre esteganografia e criptografia. Com a utilização de um programa de computador, é possível criar implementações mais sofisticadas utilizando fórmulas com valor binário ou ASCII dos caracteres.

Atualmente, novas técnicas de esteganografia são produzidas para serem utilizadas nos novos meios de comunicação, a seguir são abordadas algumas técnicas aplicadas em alguns tipos de mídias.

2.5.2 Esteganografia em Imagens

O uso de esteganografia em *software* tem um grande potencial, pois pode esconder dados em uma infinidade de mídias.

LSB (*Least Significant Bit*) são baseadas na modificação dos *bit*s menos significativos de cada *pixel* da imagem, para ocultar a mensagem. Em uma implementação básica, estes *pixels* substituem o plano LSB inteiro com o stego-dado.

Pixel (*Picture Element*) é a menor unidade de uma imagem digital a qual é possível atribuir uma cor. Quanto mais *pixels*, maior a resolução que a imagem terá. Cada *pixel* é formado por um conjunto de três elementos: verde, vermelho e azul (*red - green - blue*) – RGB. Um *pixel* pode ser representado por uma quantidade variável de *bits*, chamada “profundidade”: 2, 4, 8, 16, 24, 32, 64, entre outras.

[**R**] [**G**] [**B**] = *PIXEL*.

[0 – 255] [0 – 255] [0 – 255] = *PIXEL*.

Se a intensidade de cada elemento variar de 0 a 255 podemos ter 256*256*256 = 16.777.216 de cores para cada *pixel*. (DIAS e PAI, 2007).

Para esconder uma mensagem em uma imagem de 24 *bits*, sendo que em cada *pixel* possui três *bytes* (RGB), utilizando a técnica de inserção no *bit* menos significativo, pode-se armazenar 3 *bits* em cada *pixel*, utilizando 1 *bit* de cada *byte* desse *pixel*, sendo assim, cada *byte* da mensagem a ser ocultada irá ocupar 8 *bytes* da imagem (JASCONE, 2003). A Figura 13 ilustra um exemplo de *pixel* de uma imagem:

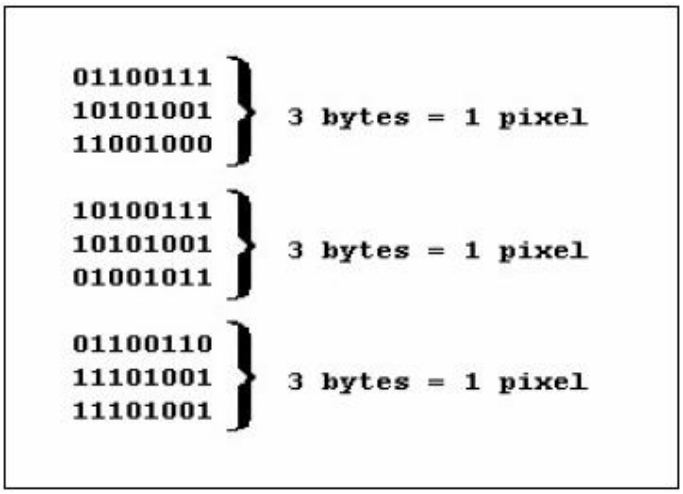

Figura 13 - Exemplo de pixels de uma imagem.
Fonte: Volpe (2007).

Supondo que o desejável seja armazenar a letra “A” nesta imagem. A letra “A” é o código 65 da tabela ASCII e seu valor binário é equivalente ao número: 0 1 0 0 0 0 0 1. Armazenando esse valor binário, *bit* a *bit*, no corpo da imagem, utilizando o *bit* menos significativo de cada *byte* do *pixel*, a imagem resultante seria equivalente a Figura 14 (JASCONE, 2003).

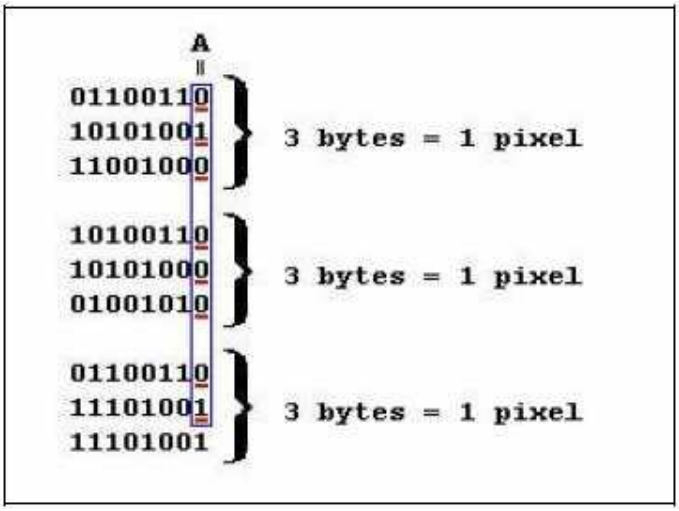

Figura 14 - Exemplo de uso do método LSB.
Fonte: Volpe, (2007).

Os *bits* sublinhados são aqueles que foram alterados, causando uma alteração imperceptível para o olho humano na cor do *pixel.* Esses valores agrupados formam o *byte* que representa a letra “A” (JASCONE, 2003).

Com esquemas mais sofisticados os locais de inclusão são selecionados, dependendo de características da visão humana, até uma pequena distorção é aceitável.

Segundo Rocha (2003), uma possibilidade para esses sistemas mais sofisticados 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.

Em geral, a técnica baseada na modificação dos *bit*s menos significativos, é suscetível a processamento de imagem, especialmente 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, que correspondem à mensagem oculta, têm uma chance menor de serem selecionados (Rocha, 2003).

O filtro passa baixa (*low-pass filters*), é outro método que também causa perda dos dados escondidos utilizando técnicas LSB, pois consistem em fazer pequenas alterações no objeto de cobertura, invalidando assim a mensagem oculta.

“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.” (ROCHA, 2003, p. 18).

Filtragem e mascaramento - Ao contrário da inserção no canal LSB, as técnicas de filtragem e mascaramento trabalham com modificações nos *bits* mais significativos das imagens. Técnicas de filtragem e mascaramento são restritas a imagens em tons de cinza. Isto se deve ao fato de que modificações em *bits* mais significativos de imagens em cores geram muitos artefatos tornando as informações mais propensas à detecção. Estas técnicas são semelhantes à marca d’água visível em que valores de *pixel* em áreas mascaradas são aumentados ou diminuídos por

porcentagem. Reduzindo o incremento por um certo grau faz a marca invisível (JULIO; BRAZIL; ALBUQUERQUE, 2007, p. 59). Uma das vantagens dessa técnica é que devido ao fato da marca d'água ser integrada na imagem ela pode ser aplicada em imagens que passam por métodos de compressão.

Algoritmos e Transformações – Técnicas de esteganografia baseadas em transformações conseguem tirar proveito de um dos principais problemas da inserção no canal LSB que é a compressão.

Os dados são embutidos no domínio de transformação, escondidos em áreas mais robustas, espalhadas através da imagem inteira, fornecendo melhor resistência contra processamento de sinal.

De forma geral, estas técnicas baseadas em algoritmos e transformações aplicam uma determinada transformação em blocos de 8x8 *pixels* na imagem. Em cada bloco, devem ser selecionados os coeficientes que são redundantes ou de menor importância. Posteriormente, estes coeficientes são utilizados para atribuir a mensagem a ser escondida em um processo em que cada coeficiente é substituído por um valor pré-determinado para o *bit* 0 ou 1 (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Para melhor entendimento do funcionamento desta técnica, são apresentados alguns exemplos de imagens usando a transformada de cosseno discreta (DCT – *Discrete Cosine Transform*), que é muito utilizada nas compressões dos padrões JPEG e MPEG.

A transformada de cosseno discreta (DCT) é uma transformada matemática, muito utilizada em processamento digital de imagens e compressão de dados. O valor da função da DCT de um vetor p de *pixels* de comprimento n é apresentado na Equação 1, (Julio; Brazil; Albuquerque, 2007).

$$G_f = \frac{1}{2} C_f \sum_{t=0}^{n-1} p_t \cos\left(\frac{(2t+1)f\pi}{2n}\right), \qquad (1)$$

$$onde:\ C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0 \\ 1 & f > 0 \end{cases} \text{para } f = 0, 1, \ldots, n-1.$$

A Figura 15 apresenta alguns exemplos de imagens transformadas usando DCT (de tamanho 8x8 *pixels*), quantizadas com a tabela recomendada pelo padrão JPEG. Note que as imagens onde as transições de tons são mais suaves proporcionam uma melhor recomposição da imagem.

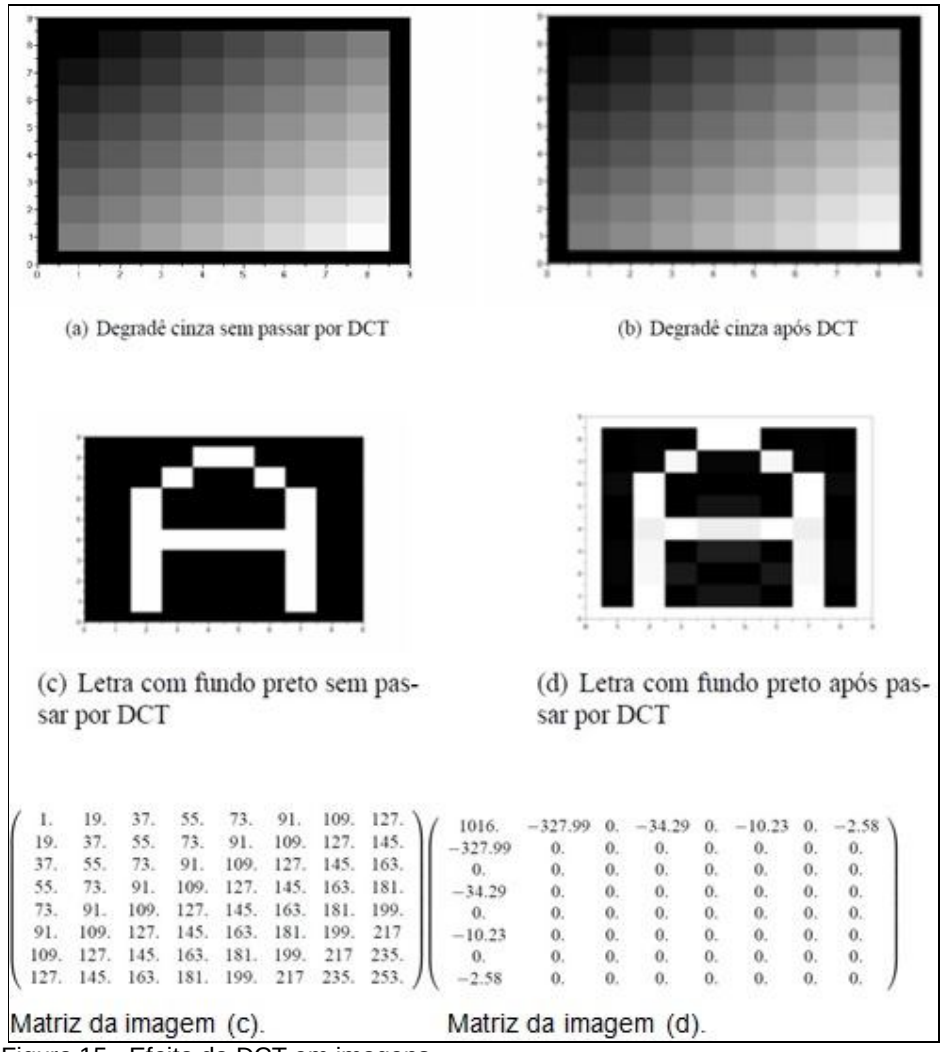

Figura 15 - Efeito da DCT em imagens.
Fonte: Julio; Brazil; Albuquerque, (2007).

A matriz da imagem (c) possui vários valores distintos, não alcançando bons resultados apenas com a eliminação das repetições.

Já a matriz (d), que é resultado após passar por DCT, tem vários valores zerados, que podem ser eliminados na compressão por alguma técnica de remoção de repetições.

O passo seguinte é aplicar a quantização, onde as posições zeradas aumentam, e os valores restantes são todos relativamente pequenos, aumentando assim o potencial de compressão. A Figura 16 apresenta a matriz de quantização.

$$\begin{pmatrix} 63. & -30. & 0. & -2. & 0. & 0. & 0. & 0. \\ -27. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \\ -2. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \\ 0. & 0. & 0. & 0. & 0. & 0. & 0. & 0. \end{pmatrix}$$

Figura 16 - Matriz de quantização.
Fonte: Julio; Brazil; Albuquerque, (2007).

O objetivo na compressão é reduzir a quantidade de dados redundantes. Por exemplo: BBBBBByyy ⟶ 6B3y.

A recuperação dos dados transformados pode ser feita com a operação inversa, chamada de IDCT (*Inverse Discrete Cosine Transform*), que é dada pela fórmula apresentada na Equação 2 (Julio; Brazil; Albuquerque, 2007).

$$p_{xy} = \frac{1}{4} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \cos\left(\frac{(2x+1)i\pi}{2n}\right) \cos\left(\frac{(2y+1)j\pi}{2n}\right). \qquad (2)$$

Após a decodificação da matriz quantizada, usando IDCT, observa-se Na Figura 17, a seguinte matriz:

$$\begin{pmatrix} 4. & 18. & 39. & 57. & 74. & 93. & 113. & 128. \\ 17. & 32. & 52. & 71. & 88. & 106. & 127. & 141. \\ 37. & 52. & 72. & 91. & 107 & 126. & 146. & 161. \\ 56. & 70. & 91. & 109. & 126. & 144. & 165. & 179. \\ 73. & 87. & 108. & 126. & 143. & 161. & 182. & 196. \\ 91. & 106 & 126. & 145. & 161. & 180. & 200. & 215 \\ 111. & 125. & 146. & 164. & 181. & 200. & 220 & 235. \\ 124. & 139. & 159. & 178. & 195. & 213. & 234. & 248. \end{pmatrix}$$

Figura 17 - Matriz após decodificação IDCT.
Fonte: Julio; Brazil; Albuquerque, (2007).

Quando comparado as matrizes, pode-se notar a diferença de valores, a Figura 18 apresenta a comparação entre a matriz original, matriz após reconstrução da compressão, matriz Erro e a diferença de valores entre elas.

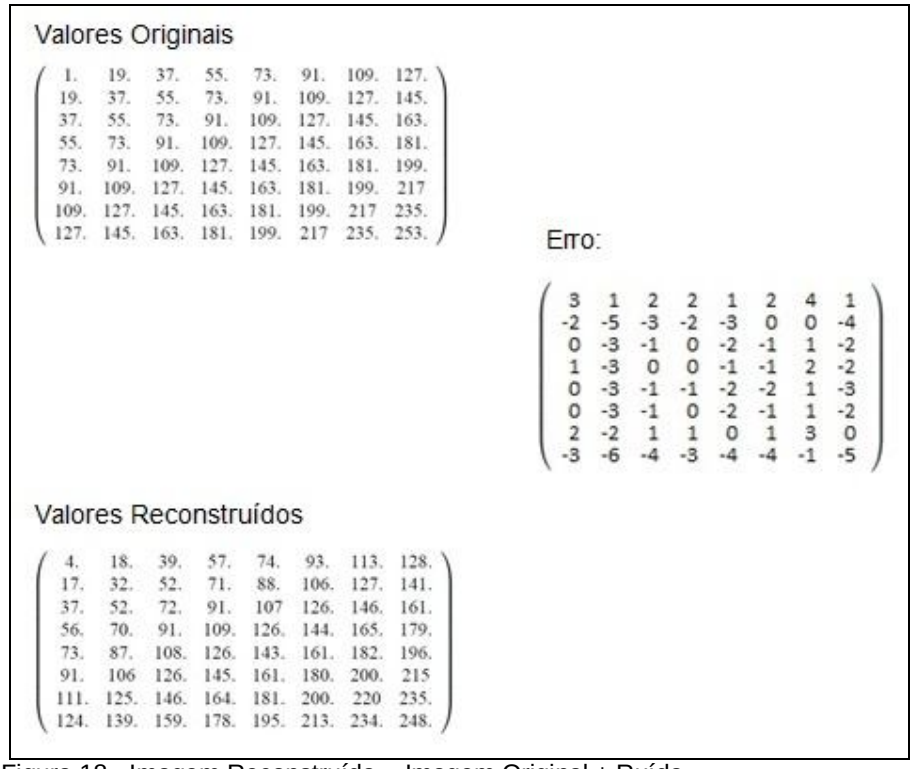

Figura 18 - Imagem Reconstruída = Imagem Original + Ruído.
Fonte: Julio; Brazil; Albuquerque, (2007). Adaptado pelo Autor.

Esses valores de erro são ruídos que a imagem reconstruída ganhou por causa do processo de compressão, significando uma perda de qualidade irreversível, no entanto a percepção ao olho humano é pequena e as técnicas de algoritmos e transformações aproveitam esses valores para inserir o dado oculto.

Técnicas de Espalhamento de Espectro – a informação a ser ocultada é separada em partes e alocada em quantidades que podem ser frações da imagem de cobertura. Basicamente a informação é espalhada nos *pixels* de uma imagem ou em partes de arquivos de áudio.

> Duas técnicas distintas são empregadas com energia eletromagnética gerada numa determinada largura de banda e domínio de freqüência, são elas: seqüência direta e salto de freqüência. No método de seqüência direta, o fluxo de informação é

> dividido em pedaços que são alocados a diferentes canais de freqüência num espectro. Salto de freqüência é uma técnica que divide um espectro em quantas freqüências de *broadcast* forem possíveis, e os dados são transmitidos através dessas frequências (JASPER 2009, p. 62).

2.5.3 Esteganografia em Áudio

Esconder imagens em sinais de áudio é algo desafiante, pois o sistema auditivo humano (SAH) pode trabalhar em uma faixa muito grande de freqüências.

De acordo com Julio; Brazil e Albuquerque (2007, p. 69),

> O SAH pode captar até um bilhão de potências diferentes de sinais (altura) e até mil frequências de sinais distintas. A sensitividade a ruído também é muito apurada. Uma perturbação em um arquivo de som pode ser detectada tão baixa quanto uma em 10 mihões de partes ou 80 dB em um ambiente comum. Apesar de ser tão poderoso para captar sinais e frequências, o SAH não consegue fazer diferenciação de tudo que recebe. Sendo assim, sons mais altos tendem a mascarar sons mais baixos. Além disso, o SAH não consegue perceber um sinal em fase absoluta, somente em fases relativas. Também existem algumas distorções do ambiente muito comum que são simplesmente ignoradas pelo ouvido na maioria dos casos.

De forma resumida Petri (2004), explica que onde os dados são inseridos em sinal próprio gerando um eco. Os dados são ocultados através da variação de três parâmetros de eco: amplitude inicial, taxa de deterioração e o atraso. Em algum ponto, a audição humana não pode distinguir entre o som original e o eco, onde o sinal do eco é ouvido meramente como ressonância.

As técnicas de esteganografia exploram muitas destas “vulnerabilidades” do ouvido humano, porém sempre têm que levar em conta a extrema sensibilidade do SAH.

2.5.4 Esteganografia em Vídeo

A esteganografia em vídeos digitais possibilita o ocultamento de um grande volume de informações quando comparada a técnicas em imagens. Contudo essa tarefa não é fácil quando aplicada a vídeos comprimidos, pois na decodificação das

informações, o processo de inserção das mensagens ocultas pode adicionar ruído dificultando a perfeita recuperação das mesmas.

> Para criação de uma técnica de esteganografia em vídeos digitais comprimidos é importante ressaltar que além da presença da compressão espacial temos a presença de compressão temporal em muitos padrões. A compressão temporal tem o papel de analisar quadros parecidos do vídeo, realizar relacionamentos entre quadros e codificar apenas partes necessárias dos quadros. Ou seja, é um sistema de compressão com perdas e os dados descomprimidos não são idênticos aos dados originais. Quanto maior compressão se quer atingir, maior é a perda de qualidade visual, degradando assim consequentemente as informações ocultas que estavam armazenadas no interior de alguns quadros do vídeo (CARVALHO, 2008, p. 08).

2.6 Esteganálise

"Os estudos e pesquisas que se destinam a revelar a existência de mensagens secretas dentro de um objeto recipiente são denominados esteganálise." (PETRI, 2004, p. 5).

De acordo com os autores Julio, Brazil e Albuquerque (2007, p. 55), "esteganálise é a arte de detectar mensagens escondidas nos mais diversos meios de comunicação".

Existem técnicas de esteganálise que o objetivo é apenas detectar a presença ou ausência de uma informação oculta no objeto analisado, sem focar o conteúdo secreto, essa técnica é classificada como esteganálise passiva. Outras se destinam a extrair uma cópia, às vezes aproximada, da mensagem secreta, essas são classificadas como esteganálise ativa.

Segundo (WAYNER (2002), citado por JASPER (2009 p.65)). "As técnicas de esteganálise possuem algumas limitações. Muitas delas, por exemplo, foram feitas especialmente para determinados algoritmos e *softwares* de esteganografia que já são previamente conhecidos; ou seja, quando essas mesmas técnicas são aplicadas aos resultados de outro algoritmo ou *software*, elas têm grande probabilidade de falhar".

O conhecimento dos seguintes componentes são necessário para que o esteganoanalista possa realizar a análise:

- *Stego-only* (apenas Esteganografia);
- *Known cover* (recipiente conhecido);
- *Known message* (mensagem conhecida);
- *Chosen stego* (escolha da Esteganografia); e
- *Chosen message* (mensagem escolhida).

O ataque *stego-only* somente o estego-objeto (arquivo contendo o dado oculto), está disponível para análise. No ataque *known cover* o recipiente original e o estego-objeto estão disponíveis. O esteganoanalista pode utilizar um ataque *known message* quando a mensagem escondida já foi revelada anteriormente, assim um atacante pode analisar os estego-objetos para futuros ataques. Mesmo com a mensagem, este pode ser um ataque muito difícil e pode ser considerado um ataque *stego-only*. No ataque *chosen stego*, a ferramenta (algoritmo) de esteganografia e o estego-objeto são conhecidos. No ataque *chosen message*, o esteganoanalista gera o estego-objeto que aponta o uso de ferramentas ou algoritmos de esteganografia específicos.

Em ambientes computacionais existem três tipos básicos de ataques de esteganálise:

- **Ataques Visuais** - Consistem em avaliar o arquivo visualmente, em busca de detalhes que revelem algum traço de esteganografia. Mudanças perceptíveis em cores podem endossar a presença de alguma informação oculta.
- **Ataques Estruturais** - Os ataques estruturais dizem respeito a identificar se há mudanças na estrutura dos arquivos que sugerem algum tipo de modificação via algum processo esteganográfico. A técnica de *bit* menos significativo (LSB) pode não ser eficiente em formatos de imagens que possuem uma pequena palheta de cores, pois seria possível detectar as mudanças.
- **Ataques Estatísticos** - São técnicas que se destinam à análise estatística dos dados de um arquivo, medindo a quantidade de redundância de dados ou distorção do mesmo. Em imagens pode-se medir o número de pares de cores próximas, as quais se distinguem no

> máximo de uma unidade em cada uma das componentes vermelho, verde e azul (RGB).

De acordo com Chirigati, Kikuchi e Gomes (2006), as técnicas que obtém melhores resultados são aquelas desenvolvidas especificamente a um determinado algoritmo. Quando se sabe qual *software* foi utilizado para realizar a esteganografia, o esteganalista consegue ter uma melhor análise do processo.

3 Metodologia

Este trabalho foi desenvolvido em duas fases distintas: uma fase de investigação dos aspectos teóricos e uma etapa prática de aplicação das técnicas de esteganografia e análise dos arquivos.

Nessa primeira fase foi realizada a revisão literária sobre a definição de esteganografia, e as diversas técnicas utilizadas na computação atualmente. Em paralelo, foi realizado um estudo na Internet e em outras fontes, dos diversos assuntos relacionados com o escopo do trabalho, envolvendo áreas como Segurança da Informação, Criptografia e Pericia Forense Computacional.

Depois de concluídas estas etapas, foi iniciado a parte prática, que envolve a utilização de duas ferramentas para a ocultação do arquivo. Foram escolhidas priorizando as que apresentavam técnicas diferentes de esteganografia.

Dentro desses critérios, as ferramentas escolhidas para realizar os testes foram: Camouflage e JPHS.

A ferramenta Camouflage é mencionada em diversos artigos da área. A escolha desta ferramenta justifica-se pelos seguintes fatos:

a) A ferramenta é *free*;
b) Possibilita a inserção de criptografia na hora de ocultar a informação, de maneira a deixar o arquivo mais protegido;
c) Solicita a escolha de uma senha, a qual será utilizada na hora de recuperar a informação;
d) Aplica esteganografia em uma variedade de objetos de cobertura;
e) Tem como base de funcionamento a técnica (LSB), que são baseadas na modificação dos *bit*s menos significativos de cada *pixel* (ou de cada cor) da imagem, para ocultar a mensagem. Ferramentas que utilizam a implementação básica (LSB), os *pixels* da mensagem secreta substituem o plano LSB inteiro com o stego-dado.

Já a ferramenta JPHS (versão do Windows, JPHSWIN.exe), foi escolhida pelos seguintes fatos:

a) Também é uma ferramenta *free*;
b) Foi desenvolvida para ser usada com arquivos JPEG como base e compressão *lossy* (compressão com perdas de dados). Ferramentas de esteganografia que trabalham com compressão *lossy* se baseiam na técnica de Algoritmos e Transformações;
c) O programa utiliza criptografia na hora de ocultar a informação;
d) O usuário é obrigado a fornecer uma *pass* frase e a mesma será solicitada na hora de extrair a mensagem oculta;
e) O aplicativo analisa a imagem de cobertura e diz qual o tamanho máximo que o arquivo de entrada (arquivo a ser ocultado), deve ter para que o processo seja seguro;
f) O programa distribui o arquivo oculto na imagem JPEG de modo que ambos os efeitos visuais e estatísticos são minimizados.

As aplicações de esteganografia e as análises foram feitas na plataforma Windows 7, com o uso de um notebook HP Pavilion dm4, processador Intel Core i7-2620M CPU@ 2.70GHz, memória RAM 6 GB, SO 64 Bits. Porém para rodar o Backtrack e o Camouflage, foi utilizado o VirtualBox (Máquina Virtual), versão 4.2.16 r86992.

Para a realização das análises foi acessado os valores hexadecimais do arquivo original e do arquivo esteganografado, através do Back Track, distribuição Linux, focado em testes de segurança e testes de invasão, muito apreciada por hackers e analistas de segurança. O objetivo é encontrar os valores que não correspondem ao arquivo original e verificar de que maneira esses valores foram distribuídos nos hexadecimais das imagens com esteganografia, de acordo com cada técnica.

Intencionalmente utilizou - se a mesma imagem como arquivo de cobertura nas duas ferramentas de esteganografia, com a intenção de facilitar a análise da manipulação no hexadecimal do arquivo.

4 Resultados

Essa sessão consiste na realização de testes práticos sobre algumas ferramentas esteganográficas existentes. Esses testes têm como principal objetivo demonstrar os resultados das principais técnicas apresentadas, mostrando o antes e depois do ocultamento da informação dentro da imagem, sendo que, posteriormente os resultados serão analisados comparando os valores hexadecimais das imagens.

Para realização dos testes foi escolhida uma imagem de 8 *bits* no formato JPEG compatível com as duas ferramentas de esteganografia.

Os softwares utilizados para os testes foram escolhidos com o principal critério de utilizarem técnicas diferentes de esteganografia.

Os testes foram divididos em duas etapas, uma sobre arquivos do tipo imagem digital e outra na comparação dos valores hexadecimais dessas imagens antes de aplicar a esteganografia e após aplicar, sendo possível verificar a disposição do arquivo oculto na estrutura da imagem de acordo com cada técnica.

4.1 Testes em Imagens

O primeiro teste foi feito com a ferramenta JPHS, que aceita como base somente imagens no formato JPEG.

4.1.1 Testes usando a ferramenta JPHS

A Figura 19 representa a imagem original JPG.

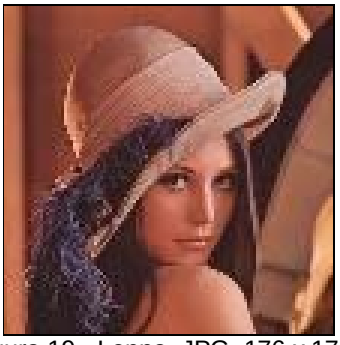

Figura 19 - Lenna, JPG, 176 x 176 *pixels*, 121 Kb, RGB, 8 bits.
Fonte: http://140.115.156.251/vclab/teacher/DIP2005Spring.htm

Com a imagem da Figura 19 poderia ocultar arquivos de, no máximo, 1 kb (aproximadamente 25% da imagem original), sem que a qualidade da mesma fosse comprometida. No caso, foi ocultado um arquivo do tipo .TXT de 1 Kb, gerando a Figura 20.

Figura 20 - Lenna, após a inserção da informação.

A imagem gerada, a olho nu, é idêntica à original, sendo o processo de ocultação um sucesso, não transparecendo que a imagem gerada foi modificada internamente. Valores hexadecimais da imagem original e da imagem com mascaramento são representados pela Figura 19 e Figura 20 respectivamente, através deles é possível notar que há diferença entre as imagens.

Para acessar os valores hexadecimais foi utilizado o BrackTrack versão 5-R3. Backtrack é um sistema operacional Linux baseado no Ubuntu, pode ser iniciado

diretamente pelo CD (sem necessidade de instalar em disco), mídia removível (*pen drive*), máquinas virtuais ou direto no disco rígido. Esta distribuição acompanha em torno de 300 ferramentas com o objetivo de testar a segurança do sistema e auxiliar na criação de scripts contra invasões. A ferramenta utilizada no BackTrack para acessar os valores hexadecimais foi o Hexedit.

Na Figura 21 são apresentados os valores hexadecimais do primeiro setor da imagem original.

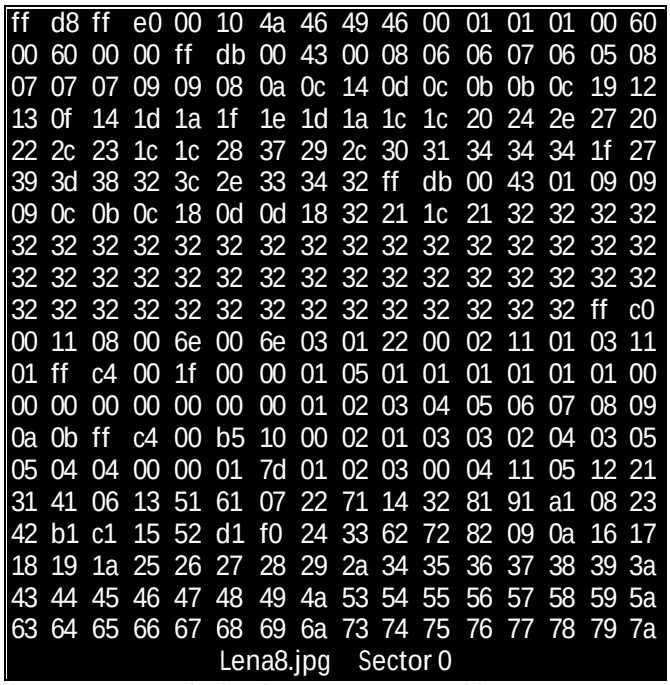

Figura 21 - Hexadecimal setor 0, Lenna 8 bits, JPG.

O primeiro setor de hexadecimal contém o cabeçalho da imagem original, dados como, assinatura do arquivo, tamanho, nome, quantidade de cores, etc. No total são 7 setores de valor hexadecimal, que são reduzidos após o processo de compressão, na Figura 22 é possível observar as alterações referente a esteganografia logo no primeiro setor de hexadecimal da imagem com mascaramento.

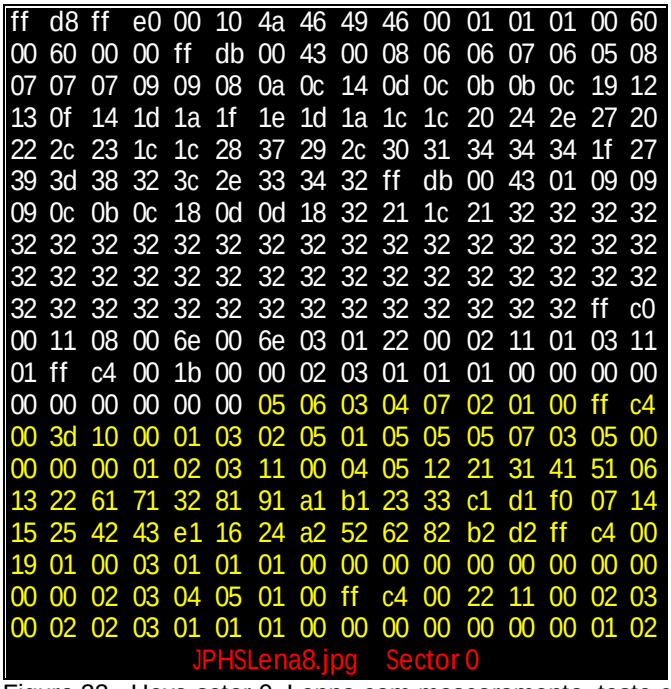

Figura 22 - Hexa setor 0, Lenna com mascaramento, teste com JPHS.

Na técnica aplicada pela ferramenta JPHS, os hexadecimais são alterados em todos os setores que passam para 6 após o processo de compressão. O que se pode perceber é que o cabeçalho da imagem original é preservado e os valores referente ao arquivo oculto são distribuídos sem criar dados repetitivos.

De acordo com Kessler (2004), o JP *Hide*-e-*Seek* (JPHS) desenvolvido por Allan Latham foi concebido para ser usado com arquivos JPEG e compressão *lossy*. O JPHS utiliza os *bits* menos significativos dos coeficientes “gerados” pela transformada do cosseno discreta, técnica de redução de redundância, utilizada pelo algoritmo JPEG. Estes coeficientes são utilizados para atribuir a mensagem a ser escondida em um processo em que cada coeficiente é substituído por um valor pré-determinado para o bit 0 ou 1. O algoritmo de criptografia que a ferramenta utiliza para aumentar a segurança do arquivo oculto é o *Blowfish*.

Nas Figuras 23 e 24 são apresentados os últimos setores da imagem original e da imagem com mascaramento, para que seja possível a comparação.

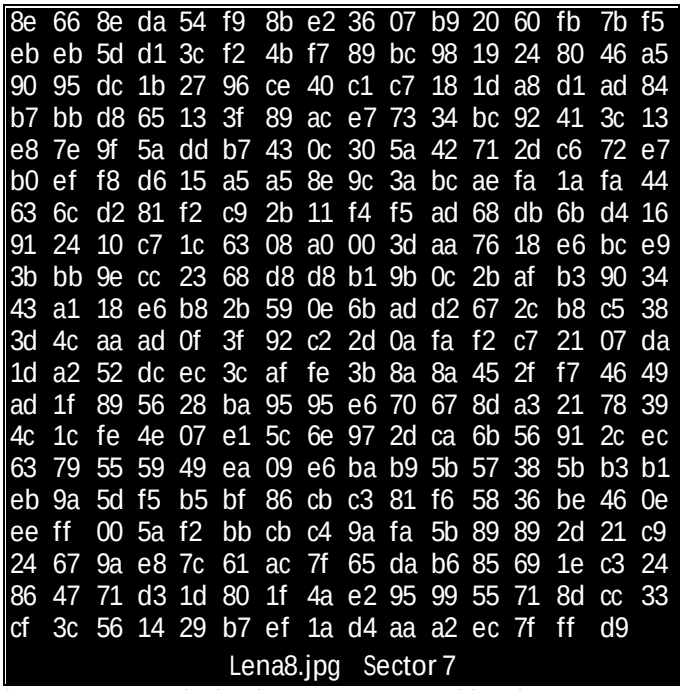

Figura 23 - Hexadecimal setor 7, Lenna 8 bits, .jpg.

Os valores são alterados à partir da décima segunda linha conforme a Figura 22, motivo que se justifica pela técnica de compressão que ao separar os valores significativos e desprezar os redundantes obrigatoriamente os valores são alterados. A técnica de algoritmo e transformação se aproveita dessas alterações para minimizar a suspeita de esteganografia. O programa distribui o arquivo oculto na imagem JPEG de modo que ambos os efeitos visuais e estatísticos são minimizados.

A Figura 24 apresenta o ultimo setor de hexadecimal da imagem com mascaramento.

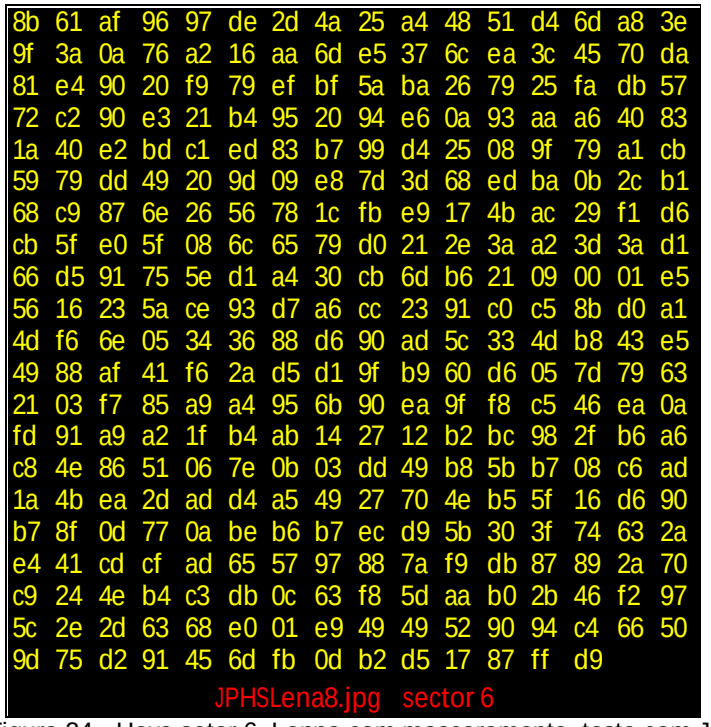

Figura 24 - Hexa setor 6, Lenna com mascaramento, teste com JPHS.

Um detalhe que é interessante e também dificulta detectar a presença de esteganografia, é que a assinatura final do formato JPEG também é preservada.

A ferramenta JPHS é de fácil operação, tem interface amigável, além de ser gratuito. Ela faz a utilização de criptografia na hora de ocultar a informação e solicita a escolha de uma senha, que será usada na hora de recuperar a informação.

4.1.2 Testes usando a ferramenta Camouflage

O segundo teste foi feito com a ferramenta Camouflage. Camoufalge se destaca por aceitar diversas extensões de arquivo como base, para aplicar a esteganografia. Para este teste foi escolhido arquivo do tipo JPEG. A Figura 25 representa a imagem original.

Figura 25 - Lenna,.JPG, 176 x 176 *pixels*, 121 Kb, RGB, 8 bits.
Fonte: http://140.115.156.251/vclab/teacher/DIP2005Spring.htm

Na imagem de número 25 foi ocultado um arquivo TXT de 1 kb. Como o objetivo neste trabalho não é a aparência da imagem e sim como é alterada a estrutura da mesma, não houve preocupação em relação ao tamanho do arquivo a ser ocultado.

A Figura 26 representa a imagem com mascaramento.

Figura 26 - Lenna após a inserção da informação, Camouflage.

A Figura 25 parece idêntica a olho nu à Figura 26, mas com uma diferença, esta contém um arquivo TXT, mascarado entre seus bytes. No método aplicado pela ferramenta Camouflage os valores hexadecimais que correspondem à imagem original não são alterados. Porém tanto o tamanho da imagem, como os valores de hexadecimais são aumentados, de 7 setores passam para 8 na imagem com o arquivo oculto. Os hexadecimais da imagem com mascaramento são representados pela Figura 27.

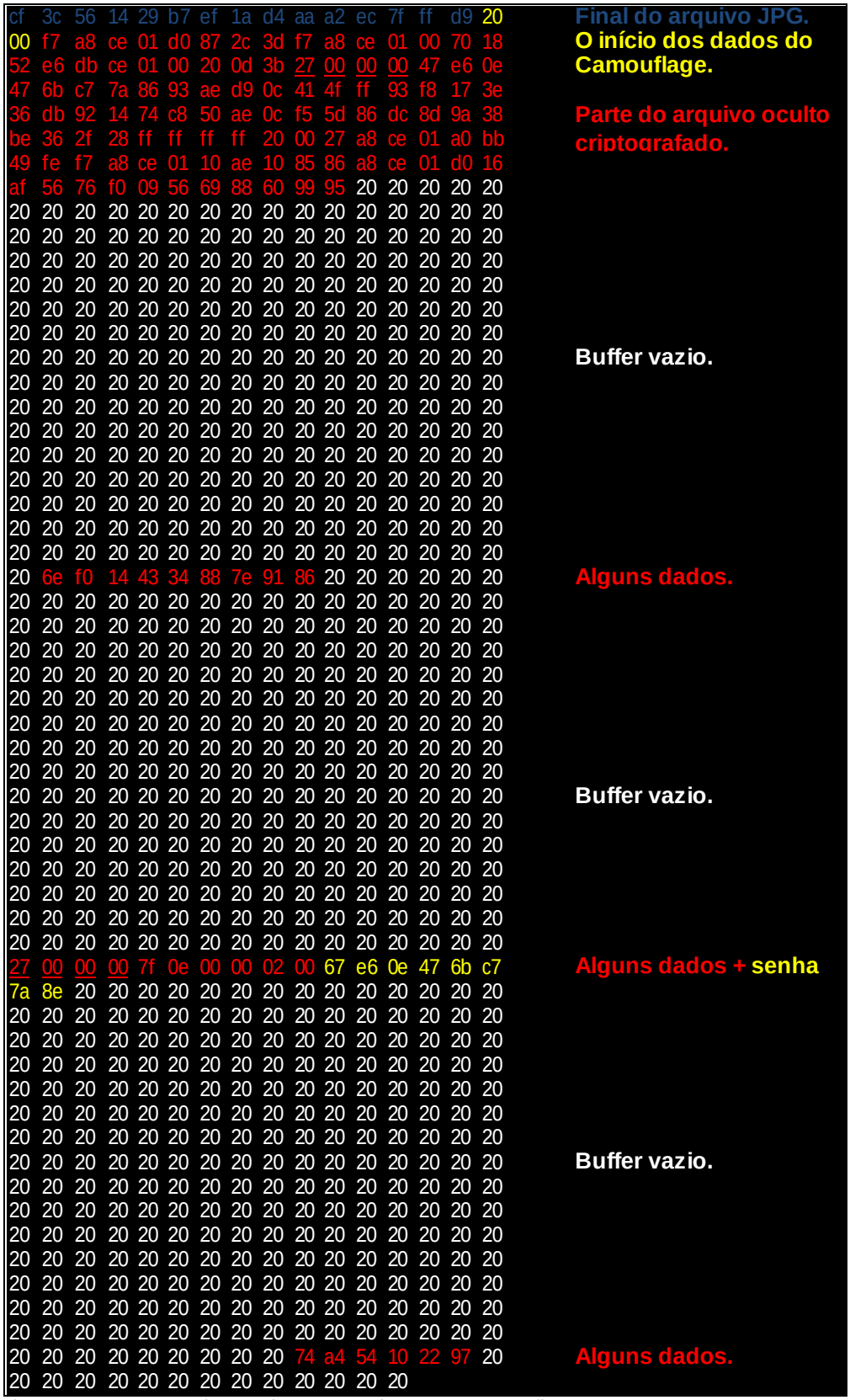

Figura 27 - Hexa arquivo oculto com senha, teste Camouflage.

A primeira coisa que chama a atenção ao comparar a imagem original com a imagem com mascaramento pelo Camouflage é o grande bloco de dados no final do arquivo, logo após o FF D9, “fim do arquivo JPG”, assinatura.

O bloco começa com 20 00, e então provavelmente o cabeçalho, dados como o tamanho do arquivo oculto que aparece sublinhado que é de 27 em decimal, ou 1B em hexadecimal, criptografados e em seguida o primeiro bloco de número “20”, que equivale ao número 32 em decimal, código ASCII para o espaço. Os *buffers* são provavelmente para armazenar sequências ASCII. Os blocos de espaço são “divididos”, por duas sequências de dados criptografados, onde em uma delas se encontra a senha que foi utilizada na hora de ocultar o arquivo, e por fim a assinatura do Camouflage. A Figura 28 apresenta o hexadecimal equivalente à senha utilizada na hora de ocultar o arquivo .txt.

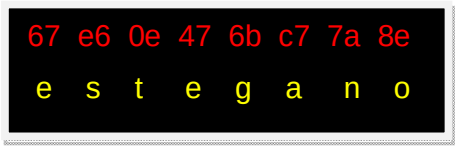

Figura 28 - Senha Camouflage.

Outro detalhe que é interessante, mesmo na imagem contendo o arquivo oculto sem a senha, o primeiro bloco de números 20 não muda, isso mostra que a criptografia não depende da senha. A Figura 29 demonstra o ultimo bloco de números 20, arquivo oculto sem senha.

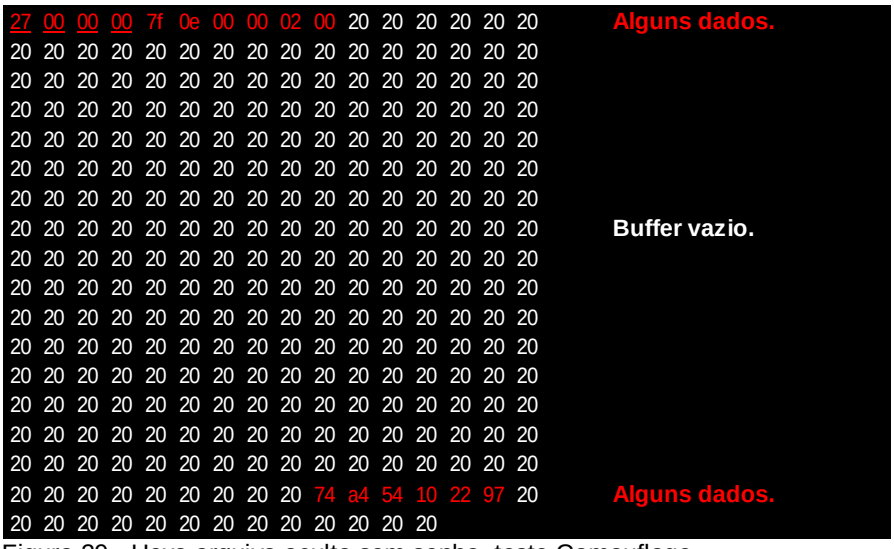

Figura 29 - Hexa arquivo oculto sem senha, teste Camouflage.

Há poucos softwares de esteganografia que esconde dados no final de arquivos, porque é um sistema extremamente fraco e detectável. A ferramenta Camouflage apesar de ter um grande diferencial ao aceitar vários formatos de arquivo como base, e também de a imagem com esteganografia não sofrer grandes modificações quando analisada a olho nu, se torna uma ferramenta fraca quando analisado a estrutura de seus arquivos esteganografados por ficar evidente a presença de valores que não correspondem ao arquivo de cobertura, que neste teste foi utilizado .JPG.

4.2 Comparação JPHS e Camouflage

A Figura 30 apresenta a tabela de comparação entre a ferramenta JPHS e Camouflage, destacando suas principais características.

Ferramentas Esteganografia									
Nome	**Free**	**Criptografia**	**Senha**	**Imagem de Cobertura**	**Formato Arquivo Oculto**	**Técnica**	**Opção somente Leitura**	**Tamanho Arquivo Oculto**	**Segurança da Informação**
JPHS	OK	OK	OK	.JPG	.DOC; .TXT; MPEG-4; MP3; .GIF; .JPG; .PNG, .WMV	Algoritmos Tranformações LSB Aleatoriamente		Limitado	FORTE
Camouflage	OK	OK	c/ senha, s/ senha	.DOC; .TXT; MPEG-4; MP3; .GIF; .JPG; .PNG, .WMV	.DOC, .TXT, MPEG-4 MP3; .GIF; .JPG; .PNG, .WMV	LSB	OK	s/ Limite	FRACO

Figura 30 - Comparação JPHS e Camouflage.
Fonte: Autor.

Através da tabela é possível notar que as ferramentas em analise possuem somente duas características iguais. Porém a técnica é a principal diferença entre elas.

4.3 Teste Esteganálise

Com a intenção de complementar a parte prática desse trabalho, utilizou-se uma ferramenta de esteganálise, que faz parte das ferramentas reunidas no BackTrack.

De acordo com Popolin (2011), Stegdetect (2007) é uma ferramenta *open source* de linha de comando usada para esteganografia, sendo utilizada para verificar se existem informações escondidas em imagens .JPG. Foi desenvolvida pelo mesmo autor do Outguess (Niels Povos). Este software se propõe a detectar conteúdo esteganográfico gerado pelos softwares Jsteg, JPHS, Invisible Secrets,

versões mais antigas do Outguess, F5, AppendX e Camouflage. A versão mais atual do StegDetect suporta análise discriminante linear (LDA) para detectar qualquer estego sistema. A Figura 31 apresenta a analise nas imagens utilizadas nos testes, através da ferramenta Stegdetect.

Figura 31 - Stegdetect analisando as imagens utilizadas nos testes.

A ferramenta mostra que em uma das imagens, existem indícios de que foi usado o programa *Jphide* para ocultação de um arquivo. E acusa também que a imagem esteganografada pelo Camouflage possui dados redundantes. A imagem original, utilizada nos testes não acusa presença de esteganografia, aponta como negativo os indícios.

5 Trabalhos Futuros

Como possíveis trabalhos futuros, pode-se apontar:

- Esteganografar imagem com menor qualidade ou seja com menos valor de *bits*.
- Explorar a ferramenta Stegdetect, a técnica análise discriminante linear, que afirma detectar qualquer estego sistema.
- Aprofundar a analise na ferramenta JPHS, para seja possível mostrar a presença de esteganografia no hexadecimal da imagem.
- Utilizar métricas para medir similaridade entre a imagem original e esteganografada, pode também mostrar o quanto a técnica pode ser segura para “esconder” informações.

5.1 Considerações Finais

Neste trabalho foram apresentados não só conceitos sobre Esteganografia como também conceitos de assuntos que sofrem impacto com o uso da esteganografia nos meios digitais. Além disso, na parte prática deste trabalho foi apresentadas duas ferramentas de esteganografia que utilizam de diferentes métodos para ocultação de dados em imagens digitais.

Em termos de pesquisa histórica, foi encontrado muito conteúdo curioso e motivador, principalmente na rede mundial de computadores, mas que teve de ser filtrado, resumido e direcionado já que a intenção desse trabalho não era apenas essa. Porém, fica o registro de que muito já foi criado pelo homem com o intuito de esconder mensagens, e manter a privacidade.

A esteganografia usa de muita criatividade na sua aplicação, uma fonte que podemos considerar inesgotável e que nos leva a crer que novas técnicas podem ser criadas, alteradas, combinadas. Isso torna o trabalho de um perito digital mais difícil de ser implementado, porém, desafiador. Em arquivos textos, onde, na sua maioria, são aproveitados aqueles espaços existentes entre linhas e caracteres, esse trabalho não parece ser tão complicado para um programa de computador. O difícil é descobrir onde monitorar uma imagem digital, dentro da quantidade enorme de dados que a compõem, levando em conta que nos dias atuais esse tipo de arquivo é disponibilizado para diversos fins e diversas áreas.

O objetivo na parte pratica deste trabalho não era simplesmente esconder um arquivo, mas fazer isso de tal forma que fosse possível analisar a estrutura das imagens contendo o arquivo oculto, mostrar a manipulação nas imagens. Para isso foi usado uma imagem visual típica, uma taxa de inserção baixa e a comparação e analise nos valores hexadecimais das imagens.

No que diz respeito à alteração nas imagens a olho nu, os resultados obtidos foram satisfatórios, ficando a imagem original e a estego-imagem muito semelhantes.

Quanto à eficiência entre os métodos, o segundo método torna-se menos aplicável se comparado ao primeiro, pois este apesar de modificar os valores hexadecimais não acrescenta valores repetitivos, o que torna o método aplicável a dados que requerem alto nível de segurança e discrição, de modo a dificultar a

detecção de mensagens. Já o segundo método preserva os valores hexadecimais da imagem original, porém o arquivo oculto é anexado no final do arquivo de cobertura, onde podem ser observados valores repetitivos, descaracterizando o formato original da imagem o que torna evidente o uso de esteganografia.

Levando em consideração que em uma investigação se tem em mãos somente a imagem e a suspeita de esteganografia, o método utilizado pela ferramenta JPHS tornará o trabalho do perito bem mais complexo. Já no método utilizado pela ferramenta Camouflage o uso de esteganografia fica evidente e a recuperação do arquivo oculto também é facilitado.

É importante salientar que já existe uma ferramenta de esteganálise (StegDetect), desenvolvida para detectar a esteganografia nas ferramentas utilizadas na parte prática desse trabalho. Em termos de segurança para quem possui conhecimento na área, as duas ferramentas, JPHS e Camouflage se tornam vulneráveis, e não é aconselhado o uso de nenhuma delas, tendo em vista que em uma pericia não passara despercebida a presença do arquivo oculto. Com relação as técnicas, sem sombra de duvidas, a transformação e algoritmo, com inserção dos bits aleatoriamente se torna mais aplicável.

6 Referências

ALECRIM, E. Criptografia**. Infowester.com,** c2009. Disponível em: <http://www.infowester.com/criptografia.php>. Acesso em: 8 Març. 2013.

AMOROSO, D. **O que é autenticação?** Disponível em: <http://www.tecmundo.com.br/seguranca/1971-o-que-e-autenticacao-.htm>. Acesso em: 04 jul. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos: referências: elaboração. Rio de Janeiro, 2006.

BARRETO, G. L. Utilização de técnicas anti-forenses para garantir a confidencialidade, **ebookbrowse.com,** c2009. Disponível em: <http://ebookbrowse.com/tcc-gustavo-luis-barreto-pdf-d93628314>. Acesso em: 06 Maio 2013.

BRASIL PROFISSÕES. Perito Criminal. Disponível em: <http://www.brasilprofissoes.com.br/profissoes/publicas/concursos-carreiras-publicas/perito-criminal#.UdF-f_nVCSo>. Acesso em: 01 jul. 2013.

CARVALHO, D. F. **Esteganografia em vídeos comprimidos MPEG-4**, 2008. 69 f. Tese (Mestre em Ciência de Computação e Matemática Computacional) - USP, São Carlos, São Paulo, 2008.

CHIRIGATI F. S., KIKUCHI R. S., GOMES T. L. **Esteganálise**. 2006. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/esteganalise.html>. Acesso em: 29 Abr. 2013.

COELHO L. C. M.; BENTO R. J. Ferramentas de Esteganografia e seu uso na INFOWAR. In: Conferência Internacional de Perícias em Crimes Cibernéticos, 1ª., 2004, Brasília. **Anais eletrônicos...** Brasília: Departamento de Polícia Federal, 2004. p. 14-22. Disponível em: < http://angel.acmesecurity.org/~adriano/papers/anais-iccyber-dpf-2004.pdf >. Acesso em: 14 Març. 2013.

CONSELHO DA JUSTIÇA FEDERAL (CJF), **O que é Assinatura Digital,** (2012). Disponível em: <http://www.jf.jus.br/cjf/tecnologia-da-informacao/identidade-digital/o-que-e-assinatura-digital> Acesso em 19 de Ab. de 2013.

COSTA, M. A. S. L. **Computação Forense**, Jun. 2005. 107p. Apostila.

COUTINHO, P. S. **Esteganografia**. Disponível em:

<http://www.gta.ufrj.br/grad/08_1/estegano/index.html>. Acesso em: 02 jul. 2013.

DIAS, C. R., PAI T. B. D. **Fundamentos de Processamento de Imagens:** Esteganografia em Diversos meios Digitais. Disponível em: <http://www.inf.ufrgs.br/~crdias/projeto_final_relatorio.htm >. Acesso em: 29 Maio 2013.

EVARISTO, J. **Introdução à Álgebra com aplicações à Ciência da Computação.** Maceió: Edufal ED., 1999. Disponível em: <http://books.google.com.br/books?id=YXMGrSnB8AAC&printsec=frontcover#v=onepage&q&f=false>. Acesso em: 14 Març. 2013.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI.** Rio de Janeiro: Brasport, 2008. Disponível em: <http://books.google.com.br/books?id=IvLVUdfv158C&pg=PA142&dq=seguran%C3%A7a+da+informa%C3%A7%C3%A3o&hl=pt-BR&sa=X&ei=i-bJUf_6H-uz0QGmtYDwCQ&ved=0CDcQ6AEwAA#v=onepage&q=seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o&f=false> Acesso em: 25 Jun. 2013.

FOROUZAN, B. A. **Comunicação de dados e Redes de Computadores.** São Paulo: Artmed S.A. ED., 2004. Disponível em: <http://books.google.com.br/books?id=C9ZN-jYKHpMC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 27 Març. 2013.

FREITAS, A. R. **Perícia Forense aplicada à Informática**. Disponível em: <http://www.guiatecnico.com.br/gt/?p=162>. Acesso em: 29 Abr. 2013.

HENRIQUE, W. G. **Anti Forensics:** Dificultando Análises Forenses Computacionais, 2006. Disponível em: <http://www.intruders.com.br/>. Acesso em: 01 de Jul. 2013.

INFO ESCOLA. Perito Judicial. Disponível em: <http://www.infoescola.com/profissoes/perito-judicial/>. Acesso em: 01 jul. 2013.

IZQUIERDO, V. A. **Afinal o que é Segurança da Informação?** (c2007), disponível em: <http://www.relacionamentodigital.com/afinal-o-que-e-seguranca-da-informacao>. Acesso em 19 Abr. 2013.

JASCONE, F. L. T. **Protótipo de Software para Ocultar texto Criptografado em Imagens Digitais.** Blumenau, 2003. Disponível em:

<http://www.inf.furb.br/~pericas/orientacoes/Esteganografia2003.pdf>. Acesso em 21 de Nov. 2013.

JASPER, N. A. **História, Técnicas e Classificação de Algoritmos esteganográficos**, 2009. 85 f. Monografia (Tecnólogo em Processamento de Dados) - Faculdade de Tecnologia de São Paulo, São Paulo, 2009.

JULIO, E. P., BRAZIL, W. G., ALBUQUERQUE C. V. N., Esteganografia e suas Aplicações. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 7, 2007, Rio de Janeiro. **Anais eletrônicos**... Rio de Janeiro: UFF, 2007. p. 54-102. Disponível em: <http://sbseg2007.nce.ufrj.br/minicurso.htm> Acesso em 24 de Abr. de 2013.

KESSLER, G. C. **An Overview of Steganography for the Computer Forensics Examiner.** Disponível em: <http://garykessler.net/library/fsc_stego.html> Acesso em: 08 Set. 2013.

KOBUSZEWSKI, A. **Protótipo para Ocultação de Textos.** 2004. 50 f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) - Universidade Regional de Blumenau. Centro de Ciências Exatas e Naturais, Santa Catarina, 2004.

MICROSOFT. **Visão geral sobre os protocolos de autenticação**. Disponível em: <http://technet.microsoft.com/pt-br/library/cc739177(v=ws.10).aspx>. Acesso em: 13 Maio 2013.

MILAGRE, J. A. **Combate a Crimes Virtuais.** Disponível em: <http://josemilagre.com.br/blog/>. Acesso em: 11 Jul. 2013.

NORTON Cybercrime Report**. Now-static.norton.com,** c2012. Disponível em: <http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf>. Acesso em: 13 Maio 2013.

NIC BR. **Práticas de Segurança para Administradores de Redes Internet.** NBSO. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf>. Acesso em: 14 Març. 2013.

OLIVEIRA, M. **Esteganografia**. Disponível em: <http://www.inf.ufrgs.br/~crdias/projeto_final_projeto.htm>. Acesso em: 02 jul. 2013.

OLIVEIRA, R. R. **Criptografia simétrica e assimétrica:** os principais algoritmos de cifragem. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. Acesso em: 05 de Abr. de 2013.

PEREIRA, E. D. V. Investigação Digital: conceitos, ferramentas e estudos de caso. **Infobrasil.inf.br,** c2010. Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao%20Digital.pdf>. Acesso em: 02 Maio 2013.

PEREIRA, M. R. T., SILVA, E. G. Esteganografia: Análise de Técnicas Aplicadas a Segurança da Informação. In: Congresso de Pesquisa Científica: Inovação, Meio Ambiente, Ética e Políticas Públicas, 3º, 2013, Marília. **Resumos**... Marília: Fundação de Ensino “Eurípides Soares da Rocha”, 1967. p. 191.

PETRI, M. **Esteganografia**. 2004. 56 f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Sociedade Educacional de Santa Catarina, Instituto Superior Tupy, Joinville, 2004.

PONCE, D. L. C. Criptografia de Dados no SQL Server – Simétrica e Assimétrica. **Imasters,** 2012. Disponível em: <http://imasters.com.br/artigo/21391/sql-server/criptografia-de-dados-no-sql-server-simetrica-e-assimetrica/> Acesso em: 20 Nov. 2013.

POPOLIN J. G. **Análise de Ferramentas para Computação Forense em Sistemas NTFS**. 2011. 65 f. Monografia Ciência da Computação (Como parte das exigências do curso de Pós – Graduação) - Universidade Federal de Lavras Minas Gerais, 2011.

QUEIROZ, C. e VARGAS R. **Investigação e Perícia Forense Computacional,** Rio de Janeiro: Brasport ED., 2010.

ROCHA, A. R. **Desenvolvimento de um Software para Segurança Digital Utilizando Esteganografia.** 2003. 30 f. Pré-projeto (apresentado ao Dep. de Ciência da Computação, como parte das exigências da disciplina Projeto orientado I.) - Universidade Federal de Lavras, Lavras, Minas gerais, 2003.

ROVER A. J. **Forense Computacional,** (200-?). Disponível em: <https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao> Acesso em: 02 Maio 2013.

SSH – **Funcionamento de Algoritmos Criptográficos**. Disponível em: <http://www.gta.ufrj.br/~natalia/SSH/blowfish.html> Acesso em: 08 Set. 2013.

SPANGHERO, M.; MARQUES, F.; CERVANTES, M. **Segurança da Informação**. Disponível em: <http://www.slideshare.net/121050876/seminario-seguranca-da-informacao>. Acesso em: 04 jul. 2013.

SILVA, N. **Segurança da Informação (TI).** Disponível em: <http://www.administradores.com.br/artigos/tecnologia/seguranca-da-informacao-ti/23933/> Acesso em: 14 Març. 2013.

VARGAS, R. Perícia Forense Computacional e metodologias para obtenção de evidênvias. **Imasters.com.br,** c2007. Disponível em: <http://imasters.com.br/artigo/6225/>. Acesso em: 02 Maio 2013.

VOLPE, L. D. **Aplicação de Esteganografia em Arquivos JPG**, 2007. 60 f. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) - Universidade do Oeste Paulista, Presidente Prudente, São Paulo, 2007.

ESTEGANOGRAFIA: ANÁLISE DE TÉCNICAS APLICADAS A SEGURANÇA DA INFORMAÇÃO

Maria Rosiane T. Pereira[1], Elvio G. Silva, Henrique P. Martins, Patricia B. Ribeiro

[1]Centro de Ciências Exatas e Sociais Aplicadas – Universidade Sagrado Coração
Bauru – SP – Brasil

mariarosiane.tp@gmail.com, egilberto@uol.com.br, henmartins@gmail.com, patriciabellin@yahoo.com.br

Abstract. *Information security is being increasingly discussed and highly relevant to Information Technology. Experts seek to develop techniques to ensure the security of Internet users. Among several existing techniques Digital Steganography, known as "hidden writing", is gaining place because of its effectiveness, and the presenting of threats by its illegitimate use. The purpose of this paper deals with practice steganographic tools tests, which use different methods of concealment, thus enabling the comparison through analysis of the files in hexadecimal values.*

Resumo. *A segurança da informação vem sendo cada vez mais discutida e de grande relevância para a Tecnologia da Informação. Especialistas buscam desenvolver técnicas para garantir a segurança de usuários na Internet. Dentre as diversas técnicas existentes a Esteganografia Digital, conhecida como "escrita oculta", vem ganhando espaço por conta de sua eficácia, e por apresentar ameaça pelo seu uso ilegítimo. A proposta deste trabalho aborda testes práticos com ferramentas esteganográficas, as quais se utilizam de diferentes métodos de ocultação, possibilitando assim a comparação através de análise feita nos valores hexadecimais dos arquivos.*

1. Introdução

Com o avanço da tecnologia, a troca de informações aumentou estrondosamente e a Internet se tornou o meio de comunicação mais utilizado. Inicialmente não se previa esse crescimento tão rápido, muito menos que pudessem aparecer pessoas especializadas em roubar informações e utilizá-las com o objetivo terroristas cometendo atentados contra as nações e os seres humanos.

Para não serem descobertas, essas pessoas, se aproveitam de técnicas de segurança da informação, desenvolvidas para o meio digital. Atualmente, uma técnica que consiste no ocultamento de informações e está sendo muito utilizada é a Esteganografia. A Esteganografia utiliza textos, imagens, sons e vídeos para esconder informações de forma que as mesmas passem despercebidas aos olhos humanos.

Diante disso, os crimes na Internet se tornaram um desafio para as autoridades e são poucos os trabalhos sobre o assunto no Brasil assim sendo é crescente a necessidade de novas pesquisas nessa linha, considerando que a utilização de computadores em atividades criminosas é cada vez mais comum.

2. Objetivos

2.1 Objetivo Geral

Explorar técnicas de Esteganografia Digital. Colaborando assim com usuários que tenham interesse nessa área, e também com o perito forense computacional, que tem por necessidade conhecer e explorar as diversas técnicas desenvolvidas para a segurança digital, que por seu uso ilegítimo são consideradas técnicas anti-forenses, obrigando investigadores a criar novos procedimentos de análise em um crime digital.

2.2 Objetivos Específicos

- Estudar métodos de Esteganografia e Perícia Forense Digital;
- Analisar softwares que utilizem diferentes técnicas de Esteganografia;
- Identificar a presença de esteganografia através da análise do hexadecimal das imagens, através de uma ferramenta de Perícia Forense Digital;
- Evidenciar pontos fortes e fragilidades de cada técnica.

3. Justificativa

Atualmente a Criptografia está sendo utilizada como critério de segurança no âmbito computacional.

Já a uso da Esteganografia vem desde antes de Cristo, e suas técnicas conseguem suprir um ponto que a criptografia não consegue: a ocultação da mensagem, um ponto crucial para a segurança da informação.

Técnicas de segurança digital podem ser usadas por razões ilegítimas, no caso da Esteganografia, por exemplo, roubar dados e esconder em um arquivo e emiti-los para fora por meio de um inocente *e-mail*, é uma forma de cometer um crime sem levantar suspeitas.

No entanto, é difícil encontrar material que explore as diversas técnicas existentes de uma maneira que seja possível à classificação de cada uma delas dentro dos critérios de segurança da informação.

4. Revisão da Literatura

4.1. Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido [ABNT - NBR ISO/IEC, 2006, p. 02].

De acordo com Izquierdo (2007), a segurança da informação digital deve focar não somente o setor de informática, rede e assemelhados, como também garantir que as informações em qualquer formato: mídias eletrônicas, papel e até mesmo conversações pessoais ou por telefone, estejam protegidas contra o acesso por pessoas não autorizadas, estejam sempre disponíveis quando necessárias, e que sejam confiáveis, ou

seja, não tenham sido corrompidas ou adulteradas por atos de pessoas mal intencionadas.

4.2. Computação Forense

Computação Forense é a ciência que trata do exame, análise e investigação de um incidente computacional, ou seja, que envolvam a computação como meio, sob a ótica forense, sendo ela civil ou penal. Na criminalística a Computação Forense trata o incidente computacional na esfera penal, determinando causas, meios, autoria e consequências [COSTA, 2005].

O profissional responsável pela perícia forense é classificado como perito, para a área computacional é denominado perito computacional.

4.2.1. Perito Forense Computacional

O perito forense computacional tem que juntar competências das mais variadas áreas do conhecimento para atuar especificamente em um único campo (Queiroz e Vargas, 2010). Para iniciar o procedimento de perícia em um equipamento, existem duas metodologias possíveis de serem adotadas: a) Live Forensics e b) Post Mortem Forensics, sendo que uma delas deve ser escolhida pelo perito.

De acordo com Pereira (2010, p. 3): a Live Forensics se caracteriza pela investigação do equipamento ainda em funcionamento, esse método é o único que permite a aquisição de informações voláteis. Já a Post Mortem Forensics, é caracterizada pela análise realizada após o desligamento do equipamento. Após ser definido qual método será utilizado, é iniciado o processo de investigação, que consiste na coleta, exame e análise dos resultados obtidos. Para a tarefa de investigação a perícia forense em informática conta com diversas ferramentas que auxiliam na busca e padronização de evidências.

4.2.2. Ferramentas Forense Computacional

Se tratando de software, existem aqueles reconhecidos mundialmente por órgãos policiais e/ou periciais, como o Encase e o FTK. Porém o custo desses softwares é muito alto. Em contrapartida existem softwares livre, incluindo distribuições Linux específicas para forense digital, com centenas de softwares para este fim. Alguns exemplos são: Helix, FDTK, PeriBR, entre outras. Existem também diversos softwares simples, cada um com seu objetivo restrito e específico. O BackTrack por exemplo foi usado para atingir os objetivos desse trabalho, é uma distribuição Linux tem como foco testes de seguranças e testes de invasão.

4.3. Criptografia

A palavra criptografia é de origem grega e significa “escrita secreta”. Entretanto, hoje em dia, o termo criptografia refere-se à ciência e à arte da transformação de mensagens, tornando-as seguras e imunes a ataques [FOROUZAN, 2004].

Existem duas técnicas de criptografia a criptografia convencional, ou simétrica, e a criptografia por chave pública, ou assimétrica, ambas envolvem o conceito de chaves, as chamadas chaves criptográficas.

Criptografia de chave simétrica é um tipo de chave mais simples, onde o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação [ALECRIM, c2009].

O método de criptografia assimétrica ou criptografia de chave pública trabalha de forma bem mais segura que a criptografia simétrica, mas perde em desempenho. O método de chave pública utiliza um par de chaves, uma chave para criptografar (chave pública) e outra para descriptografar (chave privada), além de utilizar algoritmos bem mais complexos [PONCE, 2012].

4.4. Esteganografia

Esteganografia é uma palavra de origem grega, onde Stegano significa escondido ou secreto e Grafia: escrita ou desenho [COELHO; BENTO, 2004].

Um exemplo básico de técnica moderna de esteganografia é a alteração do *bit* menos significativo de cada *pixel* de uma imagem colorida, de forma a que ele corresponda a um *bit* da mensagem a ser ocultada. Essa técnica, apesar de não ser ideal pouco afeta o resultado final de visualização da imagem (OLIVEIRA, M. 2007). Essa técnica é denominada LSB (*Least Significant Bit*) modificação dos *bit*s menos significativos de cada *pixel* da imagem, e pode ser melhorada se escolhido aleatoriamente os *bits* para não causar redundância nos valores.

Outra técnica ainda em imagens é filtragem e mascaramento ao contrário da inserção no canal LSB, as técnicas de filtragem e mascaramento trabalham com modificações nos *bits* mais significativos em imagens tons de cinza, porque essa técnica não é eficaz em imagens coloridas [JASCONE, 2003].

Outro método também em imagens é o de algoritmos e transformações, conseguem tirar proveito de um dos principais problemas da inserção no canal LSB que é a compressão. De forma geral, estas técnicas baseadas em algoritmos e transformações aplicam uma determinada transformação em blocos de 8x8 *pixels* na imagem, um exemplo são compressões dos padrões JPEG que utiliza a transformada de cosseno discreta (DCT), [JULIO; BRAZIL; ALBUQUERQUE, 2007].

Método de esteganografia em arquivos de áudio, os dados são inseridos em sinal próprio gerando um eco. Os dados são ocultados através da variação de três parâmetros de eco: amplitude inicial, taxa de deterioração e o atraso. Em algum ponto, a audição humana não pode distinguir entre o som original e o eco, onde o sinal do eco é ouvido meramente como ressonância [PETRI, 2004].

Petri (2004), também explica que os estudos e pesquisas que se destinam a revelar a existência de mensagens secretas dentro de um objeto recipiente são denominados esteganálise.

5. Metodologia

Este trabalho foi desenvolvido em duas fases distintas: uma fase de investigação dos aspectos teóricos e uma etapa prática de aplicação das técnicas de esteganografia e análise dos arquivos.

Nessa primeira fase foi realizada a revisão literária sobre a definição de esteganografia, e as diversas técnicas utilizadas na computação atualmente. Em paralelo, foi realizado um estudo na Internet e em outras fontes, dos diversos assuntos relacionados com o escopo do trabalho, envolvendo áreas como Segurança da Informação, Criptografia e Pericia Forense Computacional.

Depois de concluídas estas etapas, foi iniciado a parte prática, que envolve a utilização de duas ferramentas para a ocultação do arquivo, escolhidas priorizando as que apresentavam técnicas diferentes de esteganografia. Dentro desses critérios, as ferramentas escolhidas para realizar os testes foram Camouflage e JPHS.

A escolha da ferramenta Camouflage justifica-se pelo fato de ser muito utilizada atualmente, pois possibilita a ocultação de vários formatos de arquivo, em vários formatos de arquivo de cobertura. É uma ferramenta extremamente flexível, além de ser free, criptografar o arquivo oculto e principalmente utilizar a técnica LSB básica.

Já a ferramenta JPHS foi escolhida por ter sido desenvolvida para ser usada com arquivos JPEG como base e compressão *lossy* (compressão com perdas de dados). Ferramentas de esteganografia que trabalham com compressão *lossy* se baseiam na técnica de Algoritmos e Transformações. Também é uma ferramenta free, utiliza criptografia na hora de ocultar o arquivo.

Para a realização das análises foi acessado os valores hexadecimais do arquivo original e do arquivo esteganografado, através do Back Track, distribuição Linux, focado em testes de segurança e testes de invasão, muito apreciada por hackers e analistas de segurança. O objetivo é encontrar os valores que não correspondem ao arquivo original e verificar de que maneira esses valores foram distribuídos nos hexadecimais das imagens com esteganografia, de acordo com cada técnica.

Intencionalmente utilizou - se a mesma imagem como arquivo de cobertura nas duas ferramentas de esteganografia, com a intenção de facilitar a análise da manipulação no hexadecimal do arquivo. O formato utilizado foi JPEG.A Figura 1 representa a imagem original, utiliza como arquivo de cobertura nos testes.

Figura 1. Lena, .JPG, 110 x 110 *pixels*, 4 Kb, 8 bits.
Fonte: http://140.115.156.251/vclab/teacher/DIP2005Spring.htm

A imagem representada pela Figura 1, é uma imagem .JPG de 8 *bits* que serviu para ocultar, um arquivo TXT de 1 Kb, como o objetivo neste trabalho não é a aparência da imagem e sim como é alterada a estrutura da mesma, não houve preocupação em

relação ao tamanho do arquivo a ser ocultado, nem ao tamanho e qualidade do arquivo de cobertura.

6. Resultados

6.1. Testes usando a ferramenta JPHS

A Figura 2 apresenta a imagem com a esteganografia aplicada pela ferramenta JPHS.

Figura 2. Lena, após a inserção da informação, com JPHS.

A imagem gerada, a olho nu, é idêntica à original, sendo o processo de ocultação um sucesso, não transparecendo que a imagem foi modificada internamente. Porém na imagem representada pela Figura 3, que corresponde aos valores hexadecimais da imagem com esteganografia é possível verificar a diferença.

ff	d8	ff	e0	00	10	4a	46	49	46	00	01	01	01	00	60
00	60	00	00	ff	db	00	43	00	08	06	06	07	06	05	08
07	07	07	09	09	08	0a	0c	14	0d	0c	0b	0b	0c	19	12
13	0f	14	1d	1a	1f	1e	1d	1a	1c	1c	20	24	2e	27	20
22	2c	23	1c	1c	28	37	29	2c	30	31	34	34	34	1f	27
39	3d	38	32	3c	2e	33	34	32	ff	db	00	43	01	09	09
09	0c	0b	0c	18	0d	0d	18	32	21	1c	21	32	32	32	32
32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32	32	32	32	32	32	32	ff	c0
00	11	08	00	6e	00	6e	03	01	22	00	02	11	01	03	11
01	ff	c4	00	1b	00	00	02	03	01	01	01	00	00	00	00
00	00	00	00	00	00	05	06	03	04	07	02	01	00	ff	c4
00	3d	10	00	01	03	02	05	01	05	05	05	07	03	05	00
00	00	00	01	02	03	11	00	04	05	12	21	31	41	51	06
13	22	61	71	32	81	91	a1	b1	23	33	c1	d1	f0	07	14
15	25	42	43	e1	16	24	a2	52	62	82	b2	d2	ff	c4	00
19	01	00	03	01	01	01	00	00	00	00	00	00	00	00	00
00	00	02	03	04	05	01	00	ff	c4	00	22	11	00	02	03
00	02	02	03	01	01	01	00	00	00	00	00	00	00	01	02
JPHSLena8.jpg Sector 0															

Figura 3. setor 0, Lena com mascaramento, teste com JPHS.

Na técnica aplicada pela ferramenta JPHS, os hexadecimais são alterados em todos os setores que passam para 6 após o processo de compressão. O que se pode perceber é que o cabeçalho da imagem original é preservado e os valores referente ao arquivo oculto são distribuídos aleatoriamente sem criar dados repetitivos.

Um detalhe que é interessante e também dificulta a detectar presença de esteganografia, é que a assinatura final do formato JPEG também é preservada.

A ferramenta JPHS é de fácil operação, tem interface amigável, além de ser gratuito. Ela faz a utilização de criptografia na hora de ocultar a informação e solicita a escolha de uma senha, que será usada na hora de recuperar a informação.

O programa distribui o arquivo oculto na imagem JPEG de modo que ambos os efeitos visuais e estatísticos são minimizados.

6.2. Testes usando a ferramenta Camouflage

O segundo teste foi feito com a ferramenta Camouflage. Camoufalge se destaca por aceitar diversas extensões de arquivo como base, para aplicar a esteganografia. Para este teste foi escolhido arquivo do tipo .JPEG (Figura 1). A Figura 4 apresenta a imagem já com o arquivo oculto.

Figura 4. Lena após a inserção da informação, Camouflage.

Na imagem de número 4 foi ocultado um arquivo .TXT de 1 kb. A Figura 4 parece idêntica a olho nu à Figura 1, mas com uma diferença, esta contém um arquivo .TXT, mascarado entre seus bytes. No método aplicado pela ferramenta Camouflage os valores hexadecimais que correspondem à imagem original não são alterados. Porém tanto o tamanho da imagem, como os valores de hexadecimais são aumentados, de 7 setores passam para 8 na imagem com o arquivo oculto. Os hexadecimais da imagem com mascaramento são representados pela Figura 5.

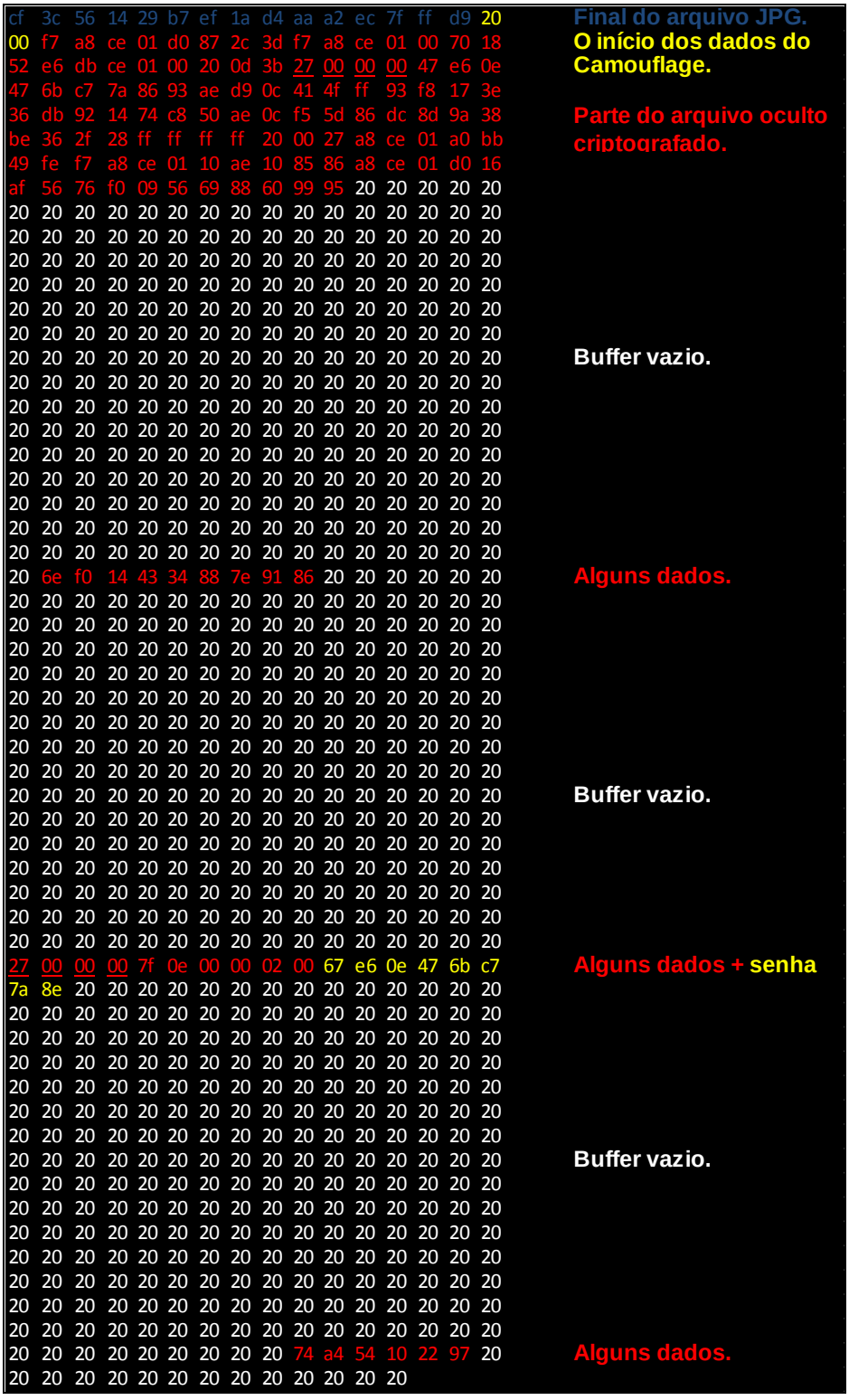

Figura 5. Hexa arquivo oculto com senha, teste Camouflage.

A primeira coisa que chama a atenção ao comparar a imagem original com a imagem com mascaramento pelo Camouflage é o grande bloco de dados no final do arquivo, logo após o FF D9, “fim do arquivo JPG”, assinatura.

O bloco começa com 20 00, e então provavelmente o cabeçalho, dados como o tamanho do arquivo oculto que aparece sublinhado que é de 27 em decimal, ou 1B em hexadecimal, criptografados e em seguida o primeiro bloco de número "20", que equivale ao número 32 em decimal, código ASCII para o espaço. Os *buffers* são provavelmente para armazenar sequências ASCII. Os blocos de espaço são "divididos", por duas sequências de dados criptografados, onde em uma delas se encontra a senha que foi utilizada na hora de ocultar o arquivo, e por fim a assinatura do Camouflage.

Há poucos softwares de esteganografia que esconde dados no final de arquivos, porque é um sistema extremamente fraco e detectável. A ferramenta Camouflage apesar de ter um grande diferencial ao aceitar vários formatos de arquivo como base, e também de a imagem com esteganografia não sofrer grandes modificações quando analisada a olho nu, se torna uma ferramenta fraca quando analisado a estrutura de seus arquivos esteganografados por ficar evidente a presença de valores que não correspondem ao arquivo de cobertura, que neste teste foi utilizado .JPG.

7. Conclusão

O objetivo na parte pratica deste trabalho não era simplesmente esconder um arquivo, mas fazer isso de tal forma que fosse possível analisar a estrutura das imagens contendo o arquivo oculto, mostrar a manipulação nas imagens. Para isso foi usado uma imagem visual típica, uma taxa de inserção baixa e a comparação e analise nos valores hexadecimais das imagens. No que diz respeito à alteração nas imagens a olho nu, os resultados obtidos foram satisfatórios, ficando a imagem original e a estego-imagem muito semelhantes.

Quanto à eficiência entre os métodos, o segundo método torna-se menos aplicável se comparado ao primeiro, pois este apesar de modificar os valores hexadecimais não acrescenta valores repetitivos, o que torna o método aplicável a dados que requerem alto nível de segurança e discrição, de modo a dificultar a detecção de mensagens. Já o segundo método preserva os valores hexadecimais da imagem original, porém o arquivo oculto é anexado no final do arquivo de cobertura, onde podem ser observados valores repetitivos, descaracterizando o formato original da imagem o que torna evidente o uso de esteganografia.

Levando em consideração que em uma investigação se tem em mãos somente a imagem e a suspeita de esteganografia, o método utilizado pela ferramenta JPHS tornará o trabalho do perito bem mais complexo. Já no método utilizado pela ferramenta Camouflage o uso de esteganografia fica evidente e a recuperação do arquivo oculto também é facilitado.

8. Referências

Alecrim, E. (c2009) "Criptografia", Infowester.com Disponível em: http://www.infowester.com/criptografia.php, 8 Març. 2013.

Associação Brasileira de Normas Técnicas, (2006) NBR ISO/IEC 27001: "Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação " — Requisitos: referências: elaboração. Rio de Janeiro.

Coelho L. C. M.; Bento R. J. “Ferramentas de Esteganografia e seu uso na INFOWAR”, In: Conferência Internacional de Perícias em Crimes Cibernéticos, 1ª., 2004, Brasília. Anais eletrônicos... Brasília: Departamento de Polícia Federal, 2004. p. 14-22. Disponível em: http://angel.acmesecurity.org/~adriano/papers/anais-iccyber-dpf-2004.pdf , 14 Març. 2013.

Costa, M. A. S. L. (Jun. 2005) “Computação Forense”, 107p. Apostila.

Forouzan, B. A. (2004) “Comunicação de dados e Redes de Computadores”, São Paulo: Artmed S.A. ED., Disponível em: http://books.google.com.br/books?id=C9ZN-jYKHpMC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false, 27 Març. 2013.

Izquierdo, V. A. (c2007) “Afinal o que é Segurança da Informação?”, Disponível em: http://www.relacionamentodigital.com/afinal-o-que-e-seguranca-da-informacao, 19 Abr. 2013.

Jascone, F. L. T. (2003) “Protótipo de Software para Ocultar texto Criptografado em Imagens Digitais”, Blumenau, Disponível em: http://www.inf.furb.br/~pericas/orientacoes/Esteganografia2003.pdf, 21 de Nov. 2013.

Julio, E. P., Brazil, W. G., Albuquerque C. V. N. “Esteganografia e suas Aplicações”, In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 7, 2007, Rio de Janeiro. Anais eletrônicos... Rio de Janeiro: UFF, 2007. p. 54-102. Disponível em: http://sbseg2007.nce.ufrj.br/minicurso.htm, 24 de Abr. de 2013.

Milagre, J. A. Combate a Crimes Virtuais. Disponível em: http://josemilagre.com.br/blog/, 11 Jul. 2013.

Oliveira, M. “Esteganografia”, Disponível em: http://www.inf.ufrgs.br/~crdias/projeto_final_projeto.htm, 02 jul. 2013.

Pereira, E. D. V. (c2010) “Investigação Digital: conceitos, ferramentas e estudos de caso” Infobrasil.inf.br, Disponível em: http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao%20Digital.pdf, 02 Maio 2013.

Petri, M. “Esteganografia”, (2004). 56 f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Sociedade Educacional de Santa Catarina, Instituto Superior Tupy, Joinville, 2004.

Ponce, D. L. C. **(**2012) “Criptografia de Dados no SQL Server – Simétrica e Assimétrica”, Imasters, Disponível em: http://imasters.com.br/artigo/21391/sql-server/criptografia-de-dados-no-sql-server-simetrica-e-assimetrica/, 20 Nov. 2013.

Queiroz, C. e Vargas R. (2010) “Investigação e Perícia Forense Computacional”, Brasport ED., Rio de Janeiro.