UNIVERSIDADE SAGRADO CORAÇÃO

MURILO JOSÉ MARQUI BOTURA

TECNICAS DE ESTEGANOGRAFIA: UM COMPARATIVO ENTRE AS FERRAMENTAS STEGDETECT, HIDE AND REVEAL e SILENTEYE

BAURU
2014

MURILO JOSÉ MARQUI BOTURA

TECNICAS DE ESTEGANOGRAFIA: UM COMPARATIVO ENTRE AS FERRAMENTAS STEGDETECT, HIDE AND REVEAL e SILENTEYE

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

BAURU
2014

Botura, Murilo José Marqui.

B7519t

Técnicas de esteganografia: um comparativo entre as ferramentas Stegdetect, Hide and Reveal e SilentEye / Murilo José Marqui Botura -- 2014.

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. Esteganografia. 2. Segurança da Informação. 3. Stegdetect. 4. Hide and Reveal. 5. SilentEye. I. Silva, Elvio Gilberto da. II. Título.

MURILO JOSE MARQUI BOTURA

TECNICAS DE ESTEGANOGRAFIA: UM COMPARATIVO ENTRE AS FERRAMENTAS STEGDETECT, HIDE AND REVEAL e SILENTEYE

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração 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. Me. Patrick Pedreira Silva
Universidade Sagrado Coração

_____
Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

Bauru, 10 de Dezembro de 2014.

Dedico este trabalho à minha família e amigos, pelo apoio e incentivo de todos durante o desenvolver deste trabalho. Obrigado pela paciência e ajuda nos momentos necessários, todos fazem parte dessa conquista.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me dar força e dedicação durante estes quatro anos de estudo e evolução, tanto pessoal quanto profissional.

Agradeço a todos os professores do curso de Ciência da Computação, pela paciência e dedicação em nos passar todos seus conhecimentos, em especial ao Prof. Me. Henrique Pachioni Martins e o Prof. Me Patrick Pedreira pelo suporte e pelas dicas, principalmente o meu orientador Prof. Dr. Elvio Gilberto da Silva, por toda a dedicação e apoio para que fosse possível concluir este trabalho.

Agradeço a todos os meus colegas de curso, especialmente Felipe Almeida Gimenes e Raphael Fernando Paez, onde estivemos juntos desde o início deste curso, pela companhia e por todas as risadas.

Agradeço também a toda minha família, por estar junto comigo em todos os momentos, principalmente pelo apoio e incentivo durante essa jornada, por aguentarem também todo o stress e correria em épocas de provas, inclusive durante o desenvolvimento deste trabalho.

A todos, muitíssimo obrigado, mas não há palavras que possam expressar toda minha gratidão a todos.

“Suba o primeiro degrau com fé. Não é necessário que você veja toda a escada. Apenas dê o primeiro passo.” (Martin Luther King, 1929).

RESUMO

A segurança da informação é um tema de grande importância para a área de tecnologia da informação. Tendo em vista o grande avanço tecnológico, questões como confidencialidade, integridade e privacidade são pontos cruciais que devem ser mantidos aos usuários da Internet, que estão conectados de várias maneiras transmitindo milhares de informações, sejam elas pessoais ou mesmo comerciais, a interceptação dessas mensagens de forma ilegal, poderia gerar graves consequências. A Esteganografia é sinônimo de escrita oculta, que consiste em ocultar algum tipo de informação em arquivos como imagens, vídeos, sons e textos. Esta pode ser equiparada à criptografia, que consiste em transmitir uma informação de maneira segura para o destinatário. O intuito destas técnicas é que a transmissão de informações seja feita de forma segura e que não tenha intervenção de outros usuários. Especialistas da área de segurança digital buscam cada vez mais desenvolver técnicas de segurança digital para combater a grande massa de cibercrimes que também evolui no mundo digital. Este trabalho apresenta um referencial teórico sobre segurança de informação e o uso da esteganografia. A proposta do presente trabalho consiste em testes práticos utilizando três ferramentas de esteganografia para inserir uma mensagem em alguns formatos de imagens pré-definidos, para que seja possível avaliar a eficiência de cada ferramenta, e assim, colaborar com interessados da área de informação digital. Após gerar os resultados, estes foram analisados para que fosse possível identificar qual ferramenta apresentou resultados mais satisfatórios. De acordo com um quadro comparativo que foi elaborado, foi possível determinar que a ferramenta Stegdetect apresentou melhores resultados, já que as imagens geradas após a inserção de uma mensagem, não sofreram alterações na qualidade visual.

Palavras-chave: Esteganografia. Segurança da Informação. Stegdetect. Hide And Reveal. SilentEye.

ABSTRACT

Information security is a topic of great importance to the information technology area. In view of the great technological advancement, issues such as confidentiality, integrity, and privacy are crucial points that must be kept to Internet users, who are connected in many ways passing thousands of information, whether personal or business, the interception of these messages illegally, could generate serious consequences. The steganography is synonymous with hidden writing, which consists of hide some kind of information in files such as images, videos, sounds and texts. This can be equated to cryptography, which consists of transmitting information securely to the recipient. The purpose of these techniques is that the transmission of information will be done safely and without intervention from other users. Digital security specialists seek increasingly developing digital security techniques to combat the large mass of cybercrimes which also evolves in the digital world. This paper presents a theoretical framework on security of information and the use of steganography. The proposal of this work consists of practice tests using three tools of steganography to embed a message in some predefined image formats, so that you can evaluate the efficiency of each tool, and thus collaborate with interested in the area of digital information. After generating the results, they were analyzed to make it possible to identify which tool presented better results. According to a comparative table was prepared, it was determined that the stegdetect tool showed better results, since the images generated after insertion of a message, no changes in visual quality.

Keyword: Steganography. Information Security. Stegdetect. Hide And Reveal. SilentEye.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

SIGLA	SIGNIFICADO
DCT	Discrete Cosine Transform
FDTK	Forensic Digital Toolkit
JPEG	Joint Photographic Experts Group
LSB	Last Significant Bit
NTLM	NT LAN Manager
RLE	Run Lenght Encoding
SSL	Secure Sockets Layer
TLS	Transport Layer Security

SUMARIO

1 INTRODUÇÃO

Atualmente muito se fala sobre o avanço constante da tecnologia, onde a comunicação e a troca de informações se torna cada vez mais prática e acessível a todos os públicos. A internet é um dos meios de comunicação mais utilizados, proporcionando lazer e praticidade aos usuários. Entretanto, além de proporcionar facilidade e conforto na interação entre as pessoas, pode também ocasionar problemas quando a questão são as “falhas de segurança”, as quais estão por todos os lados da rede, até mesmo nos sites mais conhecidos e utilizados por todos.

Pessoas que fazem da internet um meio de realizar crimes, se aproveitam de pequenas falhas em sistemas para invadir e roubar informações de usuários para fins autolucrativos. Cibercrimes, definição dada para práticas criminosas utilizando por exemplo, a internet, se tornaram uma causa preocupante para empresas, usuários e até mesmo o governo, sendo necessária a criação de métodos cada vez mais seguros para transferir informações. (CRIME..., c2008).

Pode-se citar a criptografia[1] como uma das técnicas de transferência de informação para outra pessoa de maneira segura, sem que haja intervenção de terceiros. Por mais que seja uma técnica confiável, ela ainda pode chamar a atenção de curiosos, tendo em vista que é possível perceber que uma mensagem está criptografada pelo simples fato de ali existir um código totalmente ilegível. Neste caso, um especialista pode procurar maneiras de decifrar aquele código para descobrir o que existe por traz daquela mensagem codificada. (GALVAO, JUNIOR, c2007).

Diferentemente da criptografia, a técnica de esteganografia tem como intuito transmitir uma mensagem de forma que possa passar despercebida a olho nu por outros usuários, para isso, utilizam-se textos, imagens, vídeos ou áudio para ocultar dados ou informações. Boatos afirmam que terroristas tenham usado desta técnica para planejar ataques, como o de 11 de Setembro de 2001 nos EUA, e de outros crimes de grandes proporções, que necessitavam de maior planejamento e sigilo durante as comunicações. (PEREIRA, 2013).

Toda essa evolução tecnológica está cada vez mais ao alcance de todos, indiferente de classes sociais, basta você se sentar em uma mesa de um

[1] Criptografia: codificação de mensagens em códigos para que sejam transmitidas de forma segura.

restaurante e reparar que grande parte das pessoas ali presentes estão mexendo em seus smartphones, tablets, dentre outros aparelhos, onde isso permite que as pessoas estejam conectadas e cientes do que está acontecendo em todo o mundo em tempo real.

Tanta praticidade também requer cuidado, os internautas devem se atentar ao realizarem cadastros e compras online, transações bancarias, etc., ter a consciência para identificar se um site é confiável ou não, para que assim, suas informações se mantenham seguras e não corram o risco de cair nas mãos de criminosos.

Por se tratar de um tema amplo, é crescente a necessidade de novas pesquisas e investimentos nessa linha, considerando que a utilização dos meios tecnológicos para atividades criminosas se torna cada vez mais comum.

Com base nesse contexto, o presente trabalho tem como intuito contribuir com interessados na área de segurança, como por exemplo peritos forenses, ou até mesmo estudantes das áreas de tecnologia da informação, técnicas de inserção, análise e detecção de dados e informações em imagens, bem como, estabelecer comparativos de ferramentas de esteganografia, que possam ser úteis para futuros trabalhos, e também para o uso do perito forense, que tem por necessidade conhecer e explorar as diversas técnicas existentes de análise de informações digitais, que a princípio foram desenvolvidas com o objetivo de manter a integridade e a segurança da informação.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Aplicar a esteganografia utilizando as ferramentas Stegdetect, Hide and Reveal e SilentEye, apresentando suas técnicas de inserção, análise e detecção de dados e informações em imagens.

2.2 OBJETIVOS ESPECÍFICOS

a) levantar referencial teórico sobre métodos de esteganografia e perícia forense digital;
b) aplicar e analisar métodos de esteganografia utilizando as ferramentas Stegdetect, Hide and Reveal e SilentEye;
c) comparar o desempenho dos métodos aplicados com base nas ferramentas propostas;
d) verificar a integridade e a segurança dos dados que foram inseridos nos arquivos;
e) apresentar os resultados e comparativos, apontando as funcionalidades e qualidades das ferramentas utilizadas.

3 REVISÃO DA LITERATURA

3.1 EVOLUÇÃO DA INTERNET

A internet se transformou num dos meios de comunicação mais utilizados no mundo, visto que, independentemente das diferenças financeiras entre países e pessoas, a internet tem se tornado cada vez mais uma necessidade e não apenas diversão.

Tendo em vista sua criação, durante a Segunda Guerra Mundial, onde seu objetivo era o rastreamento de informações, para que assim, fosse possível localizar e eliminar pontos considerados como inimigos com maior precisão. Em meados de 1969, quando a internet foi criada nos Estados Unidos, interligava laboratórios de pesquisas do Departamento de Defesa Norte-Americano, no auge da Guerra Fria. Posteriormente, o termo Internet foi criado e durante cerca de duas décadas, ela ficou restrita ao ambiente acadêmico e cientifico, e aos poucos foi sendo ampliada a outros países. (TAIT, 2007).

Ainda, segundo o autor citado, em 1987 a internet foi liberada para uso comercial, porém se tornou mais conhecida a partir da criação da Web, em 1991, quando servia para conectar laboratórios e instituições acadêmicas sendo capaz de exibir documentos científicos de forma simples e fácil de ser acessada. No Brasil, em 1994 entraram em funcionamento os primeiros servidores web, com acessos discados e fins comerciais.

A tecnologia está em constante evolução para proporcionar aos usuários maior agilidade, praticidade e segurança na transferência de informações, visto que a internet faz parte da rotina de trabalho, estudo e da vida das pessoas.

Técnicas de cibercrimes existem desde os primórdios da criação da internet, onde crackers[2] se aproveitaram de falhas de segurança existentes para acessar dados e informações de acessos privilegiados.

Devido a esta constante evolução tecnológica, se tornou necessário criar métodos confiáveis de segurança, através dos quais seja possível confiar dados pessoais a uma rede, podendo transitar por vários lugares antes de chegar ao seu destinatário final.

[2] Crackers são pessoas que utilizam do seu conhecimento na área de informática para quebrar códigos de segurança com fins criminosos.

3.2 SISTEMAS DE INFORMAÇÃO

Pode-se definir a informação como um conjunto organizado de dados, capaz de constituir uma mensagem sobre um fenômeno ou evento. A informação permite resolver problemas e tomar decisões, e seu uso racional é a base do conhecimento. O conceito de informação no sentido de conhecimento, caracteriza a sociedade como uma sociedade da informação, tendo em vista que a informação é uma condição básica para o desenvolvimento econômico. (CAPURRO; HJORLAND, 2007).

Segundo Laudon e Laudon (2007), um sistema de informação pode ser definido como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações, de maneira que seja possível auxiliar na coordenação e controle de uma organização.

Os sistemas de informações possuem informações sobre pessoas, locais e informações relevantes para aqueles que necessitam desses dados. (LAUDON; LAUDON, 2007).

3.3 SEGURANÇA DA INFORMAÇÃO

Atualmente, a comunicação está ao alcance de todos graças ao grande avanço da tecnologia. A informação é a base de tudo, pois é a maneira que temos de nos comunicar, e passar as outras pessoas o que sentimos, pensamos e no que acreditamos.

Existem várias maneiras de transmitirmos informações e atualmente, a internet vem tomando a frente de revistas, jornais, televisão, entre outros meios de comunicação, devido a sua acessibilidade, pois pode-se acessar onde quer que esteja, e a qualquer horário do dia, sem precisar aguardar ao próximo telejornal para se informar sobre o que ocorreu a um determinado tempo atrás. Essa é a vantagem da internet, comunicação rápida e prática 24 horas por dia, e com informação disponível até mesmo no exato momento do ocorrido. (KOLLING, [20--]).

De acordo com Kolling ([20--]), quando se fala sobre segurança da informação, nos referimos a segurança daquilo que estamos transmitindo pela internet, ou por qualquer outro meio de comunicação. Sabe-se que hoje a internet é

uma das principais vias de acesso as informações. O autor supracitado destaca que entretanto é preciso respeitar três características básicas de segurança:

a) Confidencialidade: diz respeito sobre a entrega da informação ao seu exato destinatário, para evitar que outras pessoas que não tenham autorização consigam acesso ao que foi transmitido;
b) Integridade: entregar a informação original do remetente ao destinatário, sem que tenham ocorrido alterações durante a transmissão dos dados, e também impedir que o documento seja apagado por usuários sem permissão;
c) Disponibilidade: as informações devem estar disponíveis para que as entidades autorizadas acessem a qualquer momento quando solicitadas.

Para que esta proteção exista dentro de uma empresa ou organização, é necessário adotar políticas de segurança, impondo regras para que fique clara a importância de uma informação, desde o momento que é criada, transferida e entregue ao seu destinatário final.

Já é possível realizar basicamente tudo por meio da internet, as transações comerciais são apenas uma das possibilidades, pois podem englobar grandes quantias de valores financeiros de uma forma mais rápida e pratica, não precisando encarar filas, ou mesmo ter de esperar o gerente do banco para realizá-la. Toda essa praticidade faz também com que o ambiente se torne propício ao surgimento e crescimento de crimes digitais.

3.3.1 Assinatura digital

De acordo com Carvalho (20[--]), a assinatura digital têm como intuito conservar a segurança, integridade e procedência de um documento, sendo assim, visa garantir que um documento não foi modificado durante a transição entre emissor/receptor, e se o usuário que está recebendo o documento realmente é quem deveria receber.

Para se obter uma assinatura digital, é preciso que o usuário solicite uma chave privada perante a uma entidade autorizada pelo Instituto Nacional de Tecnologia da Informação, essa chave é composta por um conjunto criptografado de bits que são usados para habilitar apenas algumas pessoas a emitir e receber dados. Obtendo uma chave privada, o usuário poderá emitir dados com sua

identidade própria, se for uma chave pública, o usuário poderá acessar os dados recebidos e repassá-los a outros usuários, porém ainda constará a identificação, e o emitente original do documento, garantindo ao verdadeiro emissor a responsabilidade por ele. (CARVALHO, [20--]).

Para repassar a informação de maneira segura, é necessária a intervenção de um hash[3], que é responsável por criptografar e gerar uma identidade única para os dados usados. Posterior a isso, é emitido um certificado para que seja estabelecida uma comunicação entre os usuários, desde que ao menos um possua uma chave privada (simétrica), e o restante tenham a chave pública (assimétrica). (GAZZARRINI, 2012).

Ainda de acordo com o autor citado anteriormente, cada browser identifica os problemas de jeitos diferentes, conferindo os certificados dos sites acessados a todo o momento. Caso ocorra alguma falha durante a verificação de algum site, aparecerá um aviso perguntando se o usuário quer ou não continuar aquela conexão, se tornando responsabilidade do próprio usuário caso aconteça algum problema no decorrer da operação. A Figura 1 ilustra os meios de verificação do certificado SSL pelo navegador Chrome, onde o mesmo consiste em um protocolo que fornece uma conexão encriptada entre o computador e a página da web, de maneira que impeça que usuários terceiros interfiram durante a transição de informações.

[3] Uma sequência única de letras e números são calculadas e atribuídas a um arquivo ou pasta que serão compartilhados.

Figura 1 - Certificado de Autenticação.

Ícone	Significado
	**O site não está usando SSL.** A maioria dos sites não precisa usar SSL porque não lida com informações confidenciais. Evite digitar informações confidenciais, como nomes de usuário e senhas, na página.
	**O Google Chrome estabeleceu uma conexão segura com o site.** Caso você seja solicitado a fazer login no site ou inserir informações confidenciais na página, procure esse ícone e certifique-se de que a URL possui o domínio correto. Se o site utilizar um certificado EV-SSL (Extended Validation SSL), o nome da organização também aparecera em verde ao lado do ícone.
	**O site usa SSL, mas o Google Chrome detectou conteúdo não seguro de alto risco na página ou problemas com o certificado do site.** Não digite informações confidenciais nessa página. Um certificado invalido ou outros problemas sérios com https podem indicar que alguém está tentando adulterar sua conexão com o site.
	**O site usa SSL, mas o Google Chrome detectou conteúdo não seguro na página.** Tenha cuidado caso você esteja digitando informações confidenciais nessa página. Conteúdo não seguro pode oferecer uma brecha para que alguém modifique a aparência da página.

Fonte: Gazzarrini (2012).
Nota: Adaptado pelo autor.

3.3.2 Protocolo de Autenticação

A autenticação é a forma que um processo confirma a identificação de um usuário ou ferramenta. Os protocolos de autenticação têm por função validar se uma página da web ou programa é seguro, validar usuários e senhas para acessar algum tipo de conta, além de autenticar certificados e assinaturas digitais. A Figura 2 descreve alguns protocolos de autenticação, bem como suas definições. (MICROSOFT, 2005).

Figura 2 - Protocolos de Autenticação.

Protocolos de Autenticação	Descrição
Autenticação Kaberos V5	Um protocolo usado com uma senha ou um cartão inteligente para logon interativo. É também o método padrão de autenticação de rede para serviços.
Autenticação SSL/TLS	Um protocolo usado quando um usuário tenta acessar um servidor web 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.

Fonte: Visão... (2005).

É visível que o surgimento de novas tecnologias que melhoram e facilitam o uso de computadores e técnicas computacionais é diário, porém, todo esse avanço também causa o aumento de novos meios de invadir contas de usuários com intuitos maliciosos, para isso, se torna cada vez mais necessário investir em meios de segurança para proteger a transmissão de dados e informações.

3.4 CRIPTOGRAFIA

A palavra Criptografia é de origem grega e tem por significado “escrita secreta”, que se refere à arte de transformar mensagens em códigos, em um conjunto de informações ilegíveis impossíveis de serem decifrados. O conceito visa que apenas quem tenha a chave de decriptação consiga transformar as informações em dados legíveis novamente, impossibilitando usuários que não possuam a chave de decriptação consigam ter acesso a essas informações, de maneira a transmitir informações de forma segura e impedir que haja modificações durante a transmissão dos dados, garantindo sua integridade. (PEREIRA, 2013).

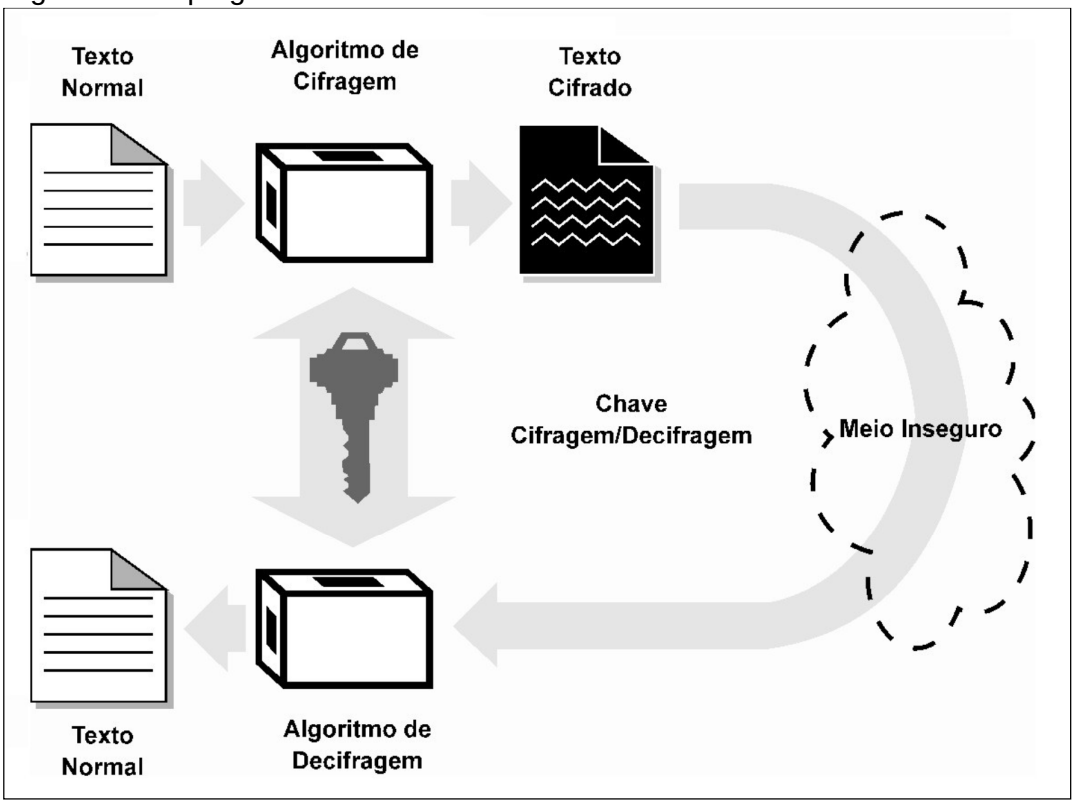
Segundo a autora citada anteriormente, a criptografia é capaz de transformar o conteúdo de uma mensagem em algo incompreensível, mas não invisível, deixando o usuário ciente de que existe alguma mensagem importante por traz de todos aqueles códigos. Hoje é possível falar sobre duas técnicas de criptografia, a convencional, ou simétrica, e a criptografia por chave pública, ou assimétrica, sendo que as duas técnicas envolvem o conceito de chaves criptográficas.

3.4.1 Criptografia de Chave Simétrica

A criptografia simétrica é a técnica mais antiga e conhecida, utiliza a mesma chave para criptografar e para descriptografar as informações, o que faz com que o processo seja realizado mais rapidamente. (OLIVEIRA, 2007).

A Figura 3 ilustra o funcionamento da técnica de criptografia por chave simétrica, que consiste em receber a informação, criptografá-la a partir da chave criptográfica, transmitir a informação para o destinatário, onde a mesma chave criptográfica utilizada anteriormente será utilizada para decodificar o texto.

Figura 3 – Criptografia de Chave Simétrica.



Fonte: Trinta, Macedo. (1998).

Conforme pode-se observar na imagem anterior, um texto normal antes de ser transmitido passa pelo algoritmo de cifragem, responsável por criptografar a mensagem. O texto cifrado é gerado e transmitido, e quando o destinatário o recebe, o mesmo algoritmo é utilizado para decifrar o texto e converte-lo para o texto normal novamente.

Sua simplicidade torna essa técnica vantajosa, por apresentar maior facilidade e rapidez na execução do processo, tendo em vista que quanto mais simples for o algoritmo, maior será sua velocidade de processamento e maior facilidade de implementação.

A principal desvantagem desta técnica é utilizar-se da mesma chave para criptografar quanto para descriptografar. Faz-se necessário que a chave de ciframento seja compartilhada previamente entre o emissor e o receptor dos dados, podendo a transmissão ser interceptada fazendo com que usuários maliciosos tenham acesso as informações restritas. (OLIVEIRA, 2007).

A Figura 4 apresenta os principais algoritmos de criptografia de chave simétrica, esta que não garante os princípios de autenticidade e não-repudiação.

Figura 4 - Principais algoritmos de chave simétrica.

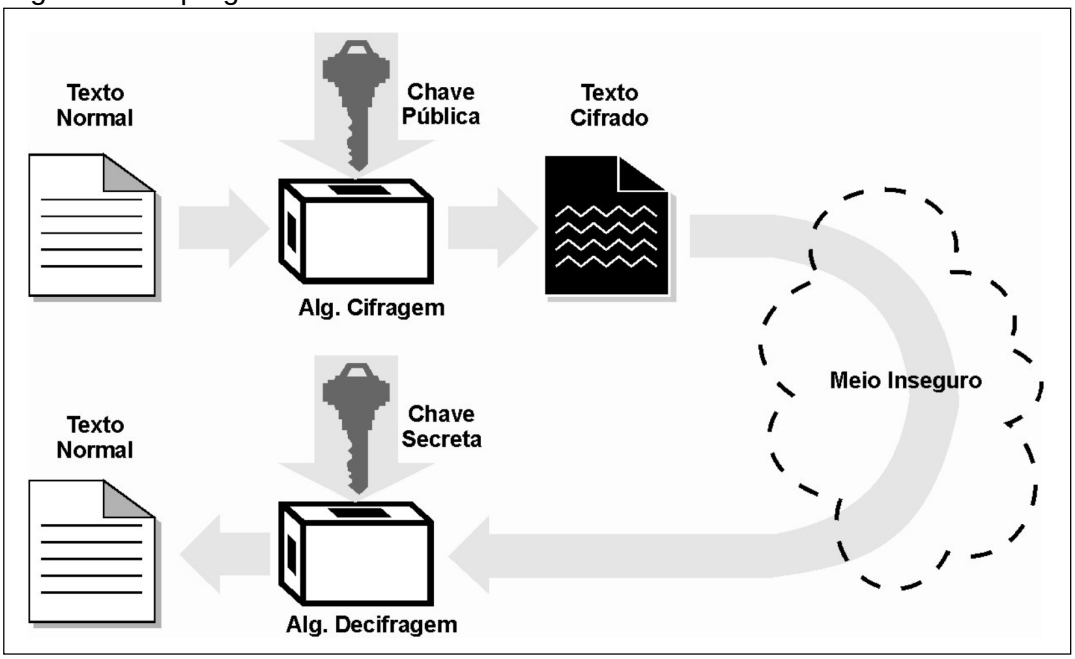
Algoritmo	Tamanho da Chave	Descrição
DES (Data Encryption Standard)	64 bits	Criado em 1977, sendo muito usado desde então. Foi adotado pelo National Bureau of Standards, atualmente conhecido como National Institute of Standards and Technology. Basicamente seu funcionamento consiste na criptografia de 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.

Fonte: Oliveira, (2007).
Nota: Adaptado pelo autor.

3.4.2 Criptografia de Chave Assimétrica

A técnica de criptografia assimétrica, ou de chave pública, é um método mais seguro de criptografia, onde se é utilizado um par de chaves, uma chave para criptografar (chave pública) e uma chave privada para descriptografar. Por se tratar de um algoritmo mais complexo, faz com que ele perca desempenho em relação a agilidade. A Figura 5 ilustra como se aplica essa técnica, onde diferentemente da técnica anterior, não se utiliza da mesma chave criptográfica para criptografar e descriptografar uma informação ou mensagem. Tanto o emissor quanto o receptor possuem chaves diferentes, mas capazes de se comunicar a ponto de decifrar os códigos contidos na mensagem. (OLIVEIRA, 2007).

Figura 5 - Criptografia de chave assimétrica.



Fonte: Trinta, Macedo. (1998).

Neste processo, um texto normal passa por um algoritmo de cifragem composto por uma chave pública, com isso, um texto cifrado é grado e transmitido ao destinatário, que por sua vez utiliza uma chave secreta para decifrar o texto e entrega-lo de forma legível.

A vantagem de se utilizar a criptografia assimétrica é de permitir a qualquer usuário transmitir uma informação utilizando a chave pública do seu receptor. Devido a chave pública ser amplamente disponível, não há a necessidade do envio de

chaves como é feito na técnica simétrica. A segurança e a integridade da informação estarão garantidas, desde que a chave privada esteja segura e apenas em posse do seu respectivo receptor. (PEREIRA, 2013).

Sua desvantagem engloba a questão de ser um algoritmo mais complexo e de difícil implementação, bem como sua perda de agilidade no momento de se descriptografar a mensagem. A Figura 6 mostra os principais algoritmos que se utilizam da chave assimétrica, onde a complexidade desses algoritmos devem ser capazes de reconhecer a dupla de chaves compostas e ser capaz de relaciona-las no momento oportuno. (OLIVEIRA, 2007).

Figura 6 - Principais algoritmos de chave assimétrica.

Algoritmo	Descrição
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como fatoração. Gerar a chave pública envolve multiplicar dois primos grandes. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes.
ElGamal	O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas, que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos

	de chave pública mais seguros, com chaves de menor tamanho.

Fonte: Oliveira, (2012).
Nota: Adaptada pelo autor.

A técnica de criptografia é muito eficiente para transferir informações entre um emissor e um receptor sem a intervenção de um usuário não permitido. Por mais que seja uma técnica segura, a criptografia pode chamar a atenção das pessoas, vendo que ali pode existir uma informação importante, porém existem países onde o uso da mesma é ilegal. Em função disso, se fez necessário desenvolver outros meios de transmitir mensagens de forma segura e que possa passar despercebida pelos usuários. A Esteganografia utiliza da técnica de camuflar uma informação dentro de uma imagem, áudio ou mesmo vídeo, de forma que possa passar pelos olhos de qualquer pessoa sem ao menos perceber se tem algo a mais nela. (PISA, 2013).

A criptografia é uma técnica muito eficiente e utilizada em basicamente tudo na Internet, porem a existência da mesma é muito perceptível fazendo com que usuários maliciosos procurem métodos de decifrar a mensagem, para isso foi criada outra técnica, a Esteganografia, que visa esconder informações de forma que passe despercebido pelos usuários.

3.5 ESTEGANOGRAFIA

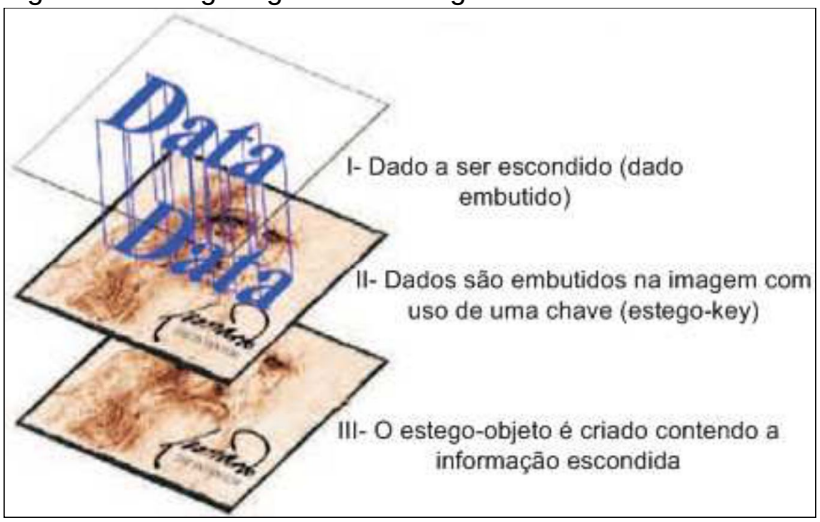
A palavra Esteganografia é de origem grega onde Stegano significa esconder e Grafia significa escrita ou desenho. (PETRI, 2014).

Segundo Petri (2004), pode-se dizer que a Esteganografia é a arte de ocultar mensagens e informações utilizando técnicas com o objetivo de se comunicar em segredo, diferentemente da criptografia, que possibilita privacidade durante a transferência de uma informação, porém de uma forma que torna visível sua presença, já a esteganografia possibilita sigilo, transmitindo uma informação de forma que sua presença não seja percebida.

Uma de suas técnicas utilizadas é a alteração do bit menos significativo de um pixel dentro de uma imagem colorida, correspondendo a um bit da mensagem que será ocultada. (CHIRIGATI; KIKUCHI; GOMES, c2006).

A Figura 7 ilustra o funcionamento da técnica de esteganografia em uma imagem.

Figura 7 - Esteganografia em Imagem.



Fonte: Julio; Brazil; Albuquerque, (2013).

Conforme pode ser observado na Figura 7:

a) o dado embutido ou embedded data é a informação que será inserida em algum arquivo de maneira que possa ser transferida de forma sigilosa.
b) a mensagem de cobertura ou cover-message é o arquivo que servirá de esconderijo, o dado que será embutido. Este arquivo pode ser de áudio (cover-audio), arquivo de texto (cover-text) ou mesmo uma imagem (cover-image).
c) stego-key é uma chave que pode ser usada ao inserir os dados na mensagem de cobertura.
d) stego-object é o resultado final da mensagem de cobertura já possuindo a mensagem que será transmitida de forma secreta.

3.5.1 Histórico da esteganografia

Muitas das técnicas de esteganografia já são conhecidas a milhares de anos. Os gregos usavam pedaços de madeira cobertos com cera para se comunicarem, as informações eram escritas sobre a cera e quando não eram mais necessárias bastava derreter a cera. Para se comunicarem de forma sigilosa sem que outras pessoas conseguissem enxergar as informações ali contidas, as mensagens eram escritas nas madeiras e encobertas com cera, de forma que não fosse possível identificar uma mensagem ali presente.

Outro método que era utilizado por volta de 440 a.C. criado pelo General Histiaeus, que consistia em raspar a cabeça de um escravo que era considerado de confiança e tatuar uma mensagem no seu couro cabeludo e, quando o cabelo estivesse grande de forma que a mensagem que foi tatuada não fosse perceptível, o escravo era encaminhado ao seu destinatário para que a mensagem pudesse ser entregue de forma segura e sigilosa. (PETRI, 2004).

A técnica Astrogal, criada por Enéas e utilizada na Grécia Antiga, era uma madeira composta por vários furos, onde cada furo representava uma letra do alfabeto. Nestes furos eram passados barbantes, de forma que fosse possível gerar uma mensagem, e para ser decodificada, bastava o destinatário acompanhar as ligações feitas pelos furos. (CHIRIGATI; KIKUCHI; GOMES, c2006).

O termo “esteganografia” ficou conhecido quando o monge Johannes Trithemius publicou uma série de livros sobre o tema, no século XV, onde detalhavam várias técnicas de como transmitir uma mensagem de forma que não fosse perceptível, porém, quando publicado, foi muito criticado e apontado como um livro que falava de magias e espíritos. (JULIO; BRAZIL; ALBUQUERQUE, 2007).

A Figura 8 destaca a trilogia escrita por Trithemius, este que naquela época foi conhecido como mago e alquimista, e por sua vez foi muito criticado por suas publicações e interesses pela ciência oculta, e chegou a ter seus livros proibidos pela Inquisição de serem divulgados. (GONZALES, c2005).

Figura 8 - Trilogia escrita por Trithemius.

Fonte: Google imagens (2014).
Nota: Adaptada pelo autor.

Durante a segunda Guerra Mundial, um tipo de tinta invisível foi desenvolvida, e para que se tornasse visível era preciso que o papel que continha a mensagem fosse aquecido. Nessa mesma época, foi desenvolvida a técnica chamada de micro pontos, onde as mensagens eram fotografadas e reduzidas para o tamanho de um ponto para que posteriormente fossem enviadas. (PETRI, 2004).

Métodos mais modernos de esteganografia envolvem cifradores nulos, que são mensagens onde certas letras devem ser utilizadas para formar a real mensagem que foi encaminhada, já as outras palavras ou letras são desconsideradas, sendo assim, nulas. Para essa técnica funcionar corretamente, tanto o emissor quanto o receptor da mensagem devem usar a mesma forma de interpretar o texto para formar a mensagem, como por exemplo, utilizar a primeira letra de cada palavra, porém apesar dessa técnica ser eficiente, é um pouco trabalhosa, pois o texto em questão deve ter algum sentido, para que não chame a

atenção caso haja intervenção durante a transmissão da mensagem. (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Ainda segundo os autores citados anteriormente, além destes, outros tipos de técnicas foram criados com o intuito de serem utilizadas em novos meios de comunicação. A Marca D'Água, por exemplo, muito utilizada hoje em dia por artistas e músicos para proteger suas obras contra a pirataria.

3.5.2 Utilização

A esteganografia é uma técnica que vem crescendo com o tempo, porém sua finalidade nem sempre pode ser vista com boas intenções.

De acordo com Pereira (2013), a marca d'agua, por exemplo, é de grande interesse comercial, tendo em vista que hoje a pirataria cresceu muito, então para garantir a integridade e a legalidade do produto, as produtoras ou empresas inserem sua marca para fins de comprovação e até mesmo de garantia de qualidade e proteção autoral.

A esteganografia pode ser utilizada para a comunicação de forma sigilosa, de maneira que seja possível impedir que a informação seja acessada por usuários que não possuam permissão, ou até mesmo planejar crimes, de forma que as informações cheguem ao destinatário certo e de maneira sutil, onde caso sejam deflagrados, não seja possível identificar nada de errado na mensagem ou na imagem. (PEREIRA, 2013).

3.5.3 Requisitos para sistemas esteganográficos

Segundo Júlio, Brazil e Albuquerque (2007), para um software de esteganografia ser considerado de qualidade, deve proceder de acordo a três requisitos existentes, descritos a seguir:

1. **Segurança:** a ferramenta deve ser segura a fim de não levantar suspeita de usuários durante a transferência do arquivo, de forma que o conteúdo oculto permaneça imperceptível e mantenha sua integridade até chegar ao seu destinatário.

2. **Carga Útil:** diferentemente da marca d'agua, que consiste em inserir uma pequena quantia de informações para garantir os direitos autorais, o intuito da esteganografia é a comunicação de forma sigilosa, e para isso é necessário uma capacidade maior de inclusão, de forma que seja possível inserir toda a informação desejada.
3. **Robustez:** consiste na capacidade de resistência durante a compressão de uma imagem, já que grande parte das imagens JPEG coloridas são comprimidas antes de serem dispostas online.

3.5.4 Métodos de Esteganografia

A esteganografia não precisa ser necessariamente aplicada de forma digital, conforme visto anteriormente, técnicas como: tatuar o couro cabeludo de um escravo, técnicas de escrita, dentre outras também são consideradas como formas de ocultar alguma mensagem.

3.5.4.1 Esteganografia em Textos

O método de esteganografia em textos consiste em esconder uma mensagem dentro de um texto, lembrando que este texto deve ter sentido para que não chame a atenção de outros leitores caso haja intervenção de outra pessoa que não seja o seu destinatário final.

Chamados de cifradores nulos, a técnica consiste em uma mensagem onde certas letras são usadas para formar a real mensagem, com isso, o restante das letras ou palavras é descartado, ou seja, consideradas como nulas (JULIO; BRAZIL; ALBUQUERQUE, 2013).

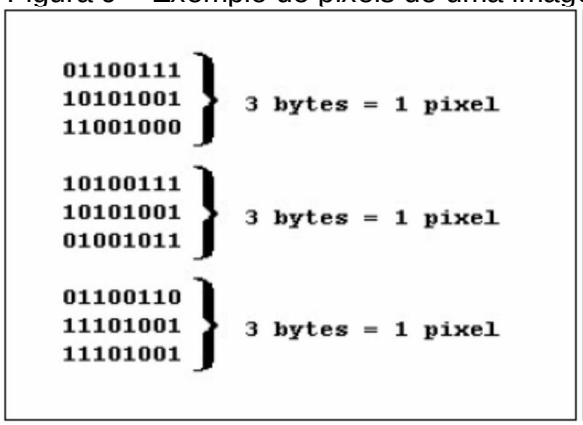
É necessário que ambas as partes envolvidas na comunicação utilizem e conheçam o mesmo protocolo de uso das letras, além também de saber interpretar o texto para que seja possível formar a mensagem final, pois pode ser que seja necessário incluir alguma outra letra para formar uma palavra. (PEREIRA, 2013).

3.5.4.2 Esteganografia em Imagens

A técnica **LSB** (Last Significant Bit) baseia-se na modificação dos bits menos significativos da imagem, onde em uma implementação simples, os pixels substituem o plano LSB por completo com o stego-dados. Em um esquema mais complexo, locais de inclusão são adaptativamente selecionados, e dependendo das características da visão humana, uma pequena distorção é aceitável, desde que não chame a atenção das pessoas. (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Para inserir uma mensagem em uma imagem de 24 bits, é possível armazenar 3 bits para cada pixel utilizando a técnica LSB. A Figura 9 ilustra o exemplo dos pixels contidos em uma imagem.

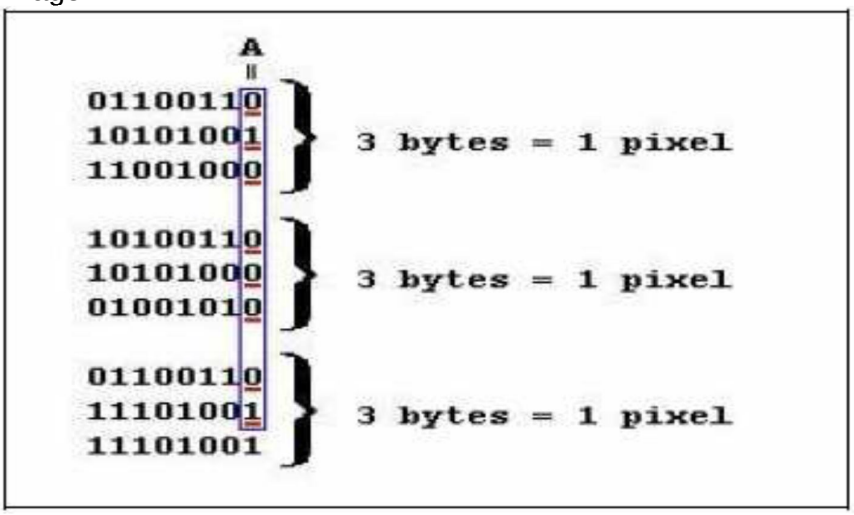
Figura 9 – Exemplo de pixels de uma imagem.



Fonte: Pereira, (2013).

Já a Figura 10, consiste na modificação dos pixels menos significativos da imagem citada anteriormente para a inserção da letra “A” dentro da mesma, sendo o seguinte valor binário: 0 1 0 0 0 0 0 1.

Figura 10 - Utilização da técnica LSB para inserir a letra "A" em uma imagem.



Fonte: Pereira, (2013).

Os bits que foram modificados estão destacados. A técnica causou uma pequena alteração na coloração do pixel, porém imperceptível ao olho humano.

As técnicas de **filtragem e mascaramento** são mais robustas do que na inserção LSB. Nesta técnica as estego-imagens criadas são imunes a compressão e recorte, porém é mais fácil de ser detectada. O inverso da técnica anterior ocorre aqui, onde os bits mais significativos são modificados, as imagens de coberturas precisam ser em tons de cinza pelo motivo da técnica não ser eficaz em imagens coloridas. Isso ocorre pelo fato de que os bits mais significativos, quando modificados, geram maior quantidade de artefatos, o que faz com que as informações se tornem mais fáceis de detecção. (JULIO; BRAZIL; ALBUQUERQUE, 2013).

Segundo Pereira (2013), as técnicas de **algoritmos e transformações** são capazes de tirar proveito dos problemas de inserção no canal LSB, que é a compressão. Para tais fins, pode-se citar a transformada de Fourier discreta, transformada de cosseno discreta e transformada Z.

Os dados inseridos são alocados em áreas mais robustas, sendo espalhadas por toda a imagem, proporcionando maior resistência contra o processamento de sinal. A técnica de inclusão de dados no domínio de transformação é mais usada para casos de marca d’agua robustas. (PEREIRA, 2013).

Baseando-se nestas técnicas, é aplicada uma determinada transformação em blocos de 8x8 pixels nas imagens, onde em cada bloco os coeficientes que são

redundantes, ou de menor importância são selecionados, para que posteriormente estes mesmos coeficientes sejam utilizados na atribuição de imagens a serem escondidas, sendo que neste processo, cada coeficiente é substituído por um valor pré-determinado para os bits 0 ou 1. (JULIO; BRAZIL; ALBUQUERQUE, 2007).

A transformada de cosseno discreta (DCT) consiste em uma fórmula matemática baseada nos cossenos, bastante utilizada em processamentos digitais de imagens e compressão de dados. A Figura 11 apresenta a fórmula utilizada.

Figura 11 - Fórmula DCT.

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

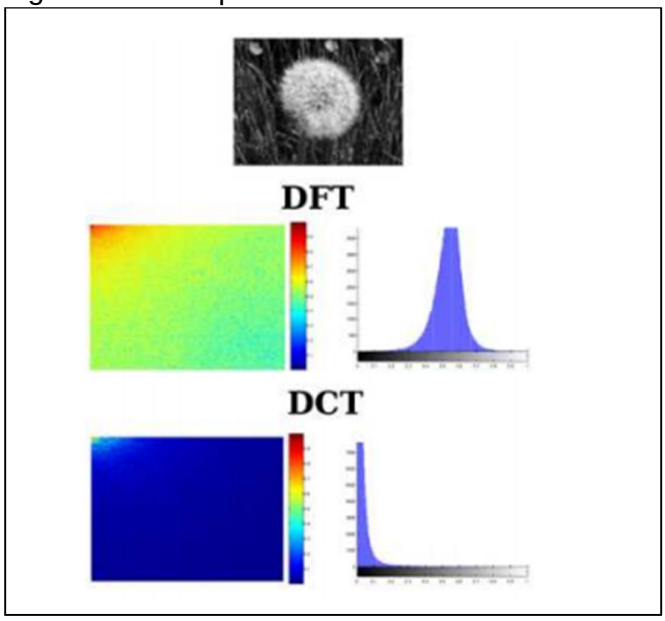
$$C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0 \\ 1 & f > 0 \end{cases} \text{ para } f = 0, 1, \ldots, n-1.$$

Fonte: Júlio; Brazil; Albuquerque (2013).

Ainda segundo os autores citados anteriormente, a matriz da transformada é composta por vetores ortonormais, sendo por sua vez uma matriz de rotação. Durante a compressão de dados, essa transformada é bastante utilizada por ser capaz de transferir a maior parte das informações contidas para os primeiros elementos do vetor, isso otimiza o armazenamento e facilita a quantização dos valores.

A Figura 12 mostra um comparativo entre a transformada de Fourier discreta e a DCT, onde é possível observar o acumulo dos coeficientes que são mais significativos no canto direito superior da imagem, sendo assim, capaz de uma melhor compressão.

Figura 12 - Comparativo entre Transformada Fourier e DCT.

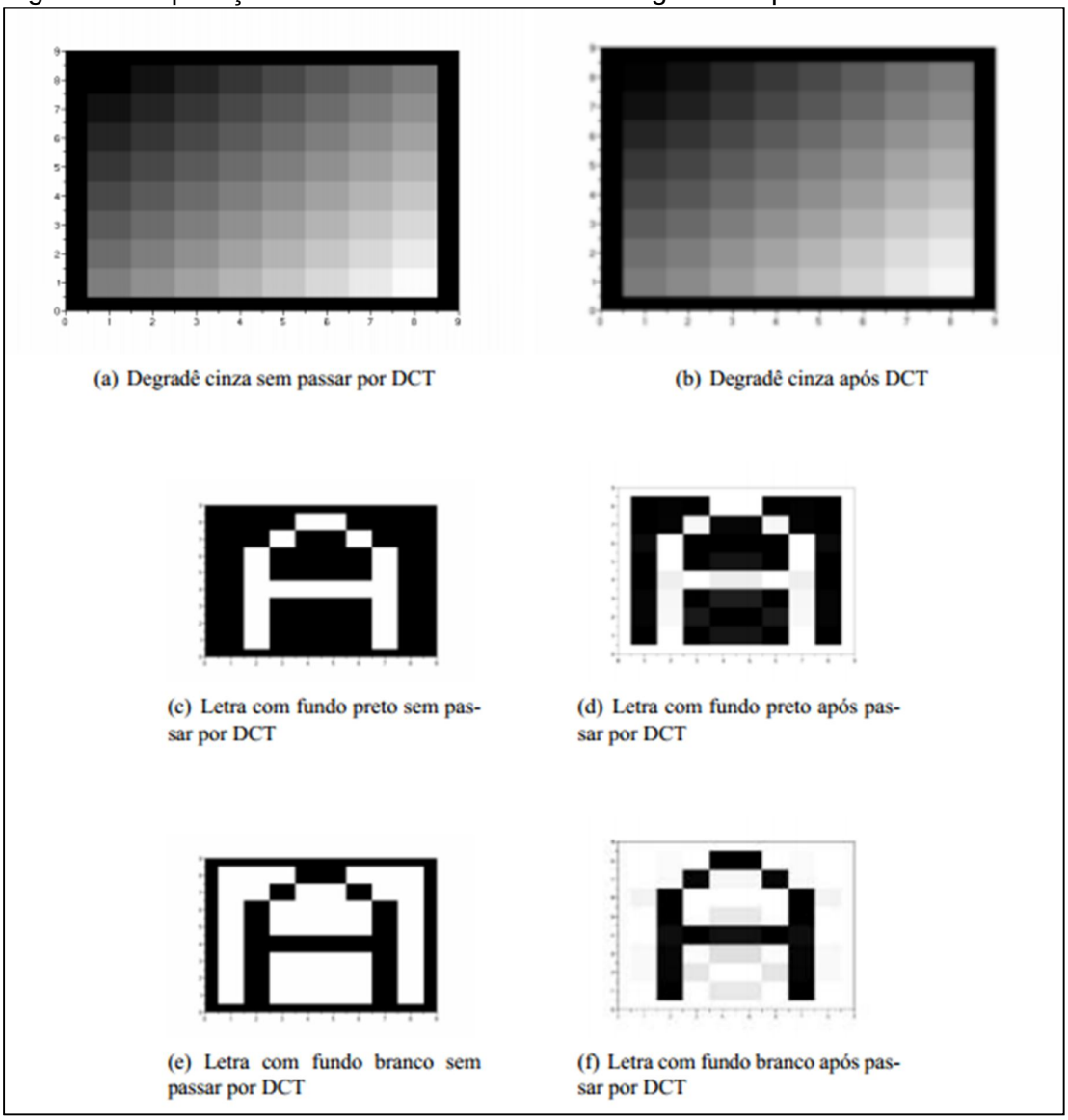


Fonte: Júlio; Brazil; Albuquerque (2013).

No padrão JPEG os coeficientes mais significativos de cada bloco 8x8 são separados dos demais, para que se possa ter maior efeito de compressão, além de comprimidos usando uma combinação de RLE (Run Length Encoding) e codificação de Huffman. Dentro do padrão, também se prevê uma compressão por meio de uma variante das codificações aritméticas, conhecida como codificação QM. (PEREIRA, 2013).

A Figura 13 ilustra exemplos de imagens de tamanho 8x8 pixels transformadas por meio da técnica DCT e quantizadas com a tabela do padrão JPEG e, posteriormente, destransformadas para recompor a imagem descomprimida. É possível perceber na imagem onde as transições de tons são mais suaves, uma melhor recomposição da imagem é proporcionada. (JULIO; BRAZIL; ALBUQUERQUE, 2013; PEREIRA, 2013).

Figura 13 - Aplicação da técnica DCT em uma imagem 8x8 pixels.



Fonte: Júlio; Brazil; Albuquerque (2013).

Já a **técnica de espalhamento de espectro** refere-se a espalhar os dados inseridos ao longo da imagem de cobertura, onde uma stego-key é utilizada para selecionar os canais de frequência. (PEREIRA, 2013).

> Os dados embutidos são primeiramente modulados com pseudo ruído e então a energia é espalhada sobre uma faixa de frequência larga, alcançando somente um nível muito baixo de força de inclusão. Isto é valioso para alcançar a imperceptibilidade (JULIO; BRAZIL; ALBUQUERQUE, 2013, p. 69).

3.5.4.3 Esteganografia em Áudio

A técnica de esteganografia em áudio é uma técnica mais complicada que as outras, tendo em vista que o sistema auditivo humano é capaz de trabalhar em uma alta faixa de frequência, o que faz tornar perceptível até mesmo uma pequena perturbação em um arquivo de áudio. (JULIO; BRAZIL; ALBUQUERQUE, 2007).

Uma das técnicas utilizadas neste método é o de inserir uma informação através de um eco. Para que a informação seja oculta de forma eficaz, variam-se três parâmetros de sinais de eco: a amplitude, taxa de deterioração e o atraso. Esses parâmetros são configurados de forma que fiquem abaixo do limite sensorial do ouvido humano, para que não seja possível distinguir entre o som original e o eco, que pode ser considerado como uma ressonância. (PETRI, 2004).

3.5.4.4 Esteganografia em Vídeo

Um vídeo digital consiste em um conjunto de inúmeras imagens que quando exibidas em uma taxa de 24 a 30 quadros por segundo, dão a impressão de movimento.

Utilizando da técnica para inserir uma informação oculta em um vídeo, é necessário manipular as imagens ali contidas. Isso só é possível pelo fato de que a visão humana não tem a capacidade de percepção de pequenas alterações nas imagens realizadas por meio da introdução de bits relativos a mensagem que será ocultada. A mesma técnica LSB é utilizada para tal fim, onde o bit menos significativo de cada byte da imagem será modificado. (CARVALHO, 2008).

3.5.5 Esteganálise

Segundo Petri (2004), a Esteganálise refere-se a estudos e pesquisas com o intuito de descobrir informações que foram ocultadas de alguma forma, seja em texto, imagem, áudio ou vídeo.

As técnicas de esteganografia possuem falhas como em qualquer outro sistema, e podem ser descobertas por qualquer usuário que tenha interesse em avaliar e examinar detalhadamente algum objeto em busca de informações ali ocultas, pois ao se utilizar da técnica de esteganografia, a qualidade do objeto é

degradada, sendo assim, torna-se possível perceber alguma modificação, e definir parâmetros para que seja possível detectar um objeto modificado. (PETRI, 2004).

Ainda segundo o autor, na técnica de Esteganálise, pode-se considerar três métodos de ataques:

a) Os **ataques aurais** consistem na retirada das partes significativas da imagem, de forma que facilite ao olho humano a busca por falhas contidas na imagem.
b) Nos **ataques estruturais**, a estrutura do arquivo é alterada quando uma mensagem é inserida, devido a isso, com a ajuda de um software é possível analisar a estrutura da imagem com o intuito de descobrir se a mesma foi alterada no momento da inserção dos dados. Tomamos como exemplo os dados inseridos em uma imagem indexada, baseada em paleta de cores, onde a imagem de cobertura tem suas características modificadas, tornando maior as chances de detecção.
c) No **ataque estatístico**, é possível identificar que os padrões dos bits menos significativos revelam a existência de uma mensagem, por meio de uma medição da quantidade de redundância ou distorção dos dados ali contidos.

Ainda segundo o autor supracitado, não há métodos de ataques à esteganografia que sejam universais ou mesmo que correspondam a todos os softwares com esta finalidade. Em um ataque passivo, o intuito é apenas identificar a presença ou ausência de uma informação no arquivo, já no ativo, além de interceptar a mensagem também é possível manipular os dados.

Quando há a suspeita de que existe uma informação oculta em um arquivo, é preciso realizar testes e analisar hipóteses a fim de descobrir uma maneira de extrair as informações. 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. (CHIRIGATI; KIKUCHI; GOMES, 2006 citado por PEREIRA, 2013).

Tendo em vista todo este avanço na tecnologia, que está cada vez mais ao alcance de todos, porém não podemos nos esquecer dos perigos que também acompanham esse avanço, como: pedofilia, conteúdo pornográfico, roubos, fraudes são exemplos do que corre pela rede a todo o momento, com todos esses problemas, foi necessário desenvolver meios e designar pessoas treinadas e

qualificadas para realizar essas investigações, o qual são denominadas de peritos forense computacionais.

3.6 PERÍCIA FORENSE

A perícia pode ser considerada como uma pesquisa onde são exigidos conhecimentos técnicos e/ou científicos, a fim de que o perito esteja capacitado para interpretar e decifrar algum crime. Já a perícia forense, consiste em aplicar métodos científicos para que seja possível identificar, analisar e solucionar um caso por meio das evidências deixadas pelo autor. (SILVA, 2010).

3.6.1 Perícia Forense Computacional

A perícia forense computacional é um método criado para investigar e combater os cibercrimes, onde se utiliza de técnicas especificas para coletar, preservar, analisar e apresentar informações suspeitas contidas em computadores que foram utilizados na elaboração e execução de algum crime digital, e a partir daí buscar evidencias deixadas pelos criminosos a fim de solucionar o caso.

Considerando que a tecnologia evolui mais e mais a cada dia, esta é uma área onde o estudo em busca de melhoramentos deve ser constante, bem como a qualificação da equipe que está envolvida, pois assim, conforme a tecnologia avança, também novos crimes cibernéticos são desenvolvidos, e cada vez mais complexos e difíceis de serem resolvidos. (GONÇALVES et al., 2012).

Uma das formas do perito analisar as provas de um crime consiste em trabalhar com a máquina ainda ligada após a execução do mesmo, de forma a realizar uma imagem dos dados voláteis, preservando o estado inicial do equipamento para que se possa fazer uma análise minuciosa das informações ali contidas. (TOLENTINO; SILVA; MELLO, 2011).

Para se ter uma investigação eficiente, é preciso seguir algumas etapas, onde a **coleta de dados** consiste na captação do equipamento e das informações de maneira em que sua integridade não seja afetada. No **exame dos dados**, é realizada a captação das informações mais relevantes à investigação e separada das demais, dessa forma é possível definir um processo mais especifico para que seja realizada a **análise das informações**, onde o intuito é encontrar dados

importantes que auxiliem na resolução do caso. Na última etapa, a **interpretação dos resultados** consiste em apresentar um laudo técnico contendo todas as informações verídicas dos dados que foram analisados em laboratório. (PEREIRA, 2013).

3.6.2 Softwares de Perícia Forense Digital

Para que seja possível coletar, analisar e evidenciar dados e informações a fim de se chegar a um resultado final plausível, os peritos forenses dependem de ferramentas precisas e eficientes, que possam colaborar com investigações criminais. Em alguns casos é necessário comprar uma licença para utilizá-las, o que gera um alto custo, mas em contrapartida existem softwares de distribuição livre, que também são capazes de auxiliar em uma análise forense.

No presente trabalho, foram utilizadas as ferramentas: Stegdetect contida no Sistema Operacional FDTK, baseado em Linux, e Hide And Reveal e SilentEye, baseados em Windows, que estão descritas a seguir.

3.6.2.1 Stegdetect

Esta é uma ferramenta de código livre, capaz de detectar métodos de esteganografia em imagens de formato **JPG**.

Para isso, o software utiliza a análise de discriminante linear, onde a imagem original é comparada com a alterada. É realizado um cálculo que apresenta as diferenças que existem dentro da imagem. O resultado é armazenado a fim de que possa ser reutilizado em novas análises de imagens. (PROVOS, c2004).

O mesmo pode ser encontrado no sistema operacional FDTK, versão 3.0, este que possui em torno de 100 ferramentas que podem ser utilizadas em uma investigação digital. (NEUKAMP, BOTELHO, c2014).

A Figura 14 apresenta uma tela do sistema FDTK, baseada em plataforma Linux, onde é possível ver algumas de suas ferramentas que podem ser utilizadas em investigações e analises forense.

Figura 14 - Sistema FDTK e suas ferramentas de análise digital.

Fonte: Neukamp, Botelho, (c2014).

3.6.2.2 Hide and Reveal

Segundo Cottin (c2013), é uma ferramenta desenvolvida em Java, o Hide and Reveal é um aplicativo de código livre, que usa a técnica de esteganografia para camuflar informações em uma imagem, no formato **BMP**. Além de oferecer três opções de inserção LSB:

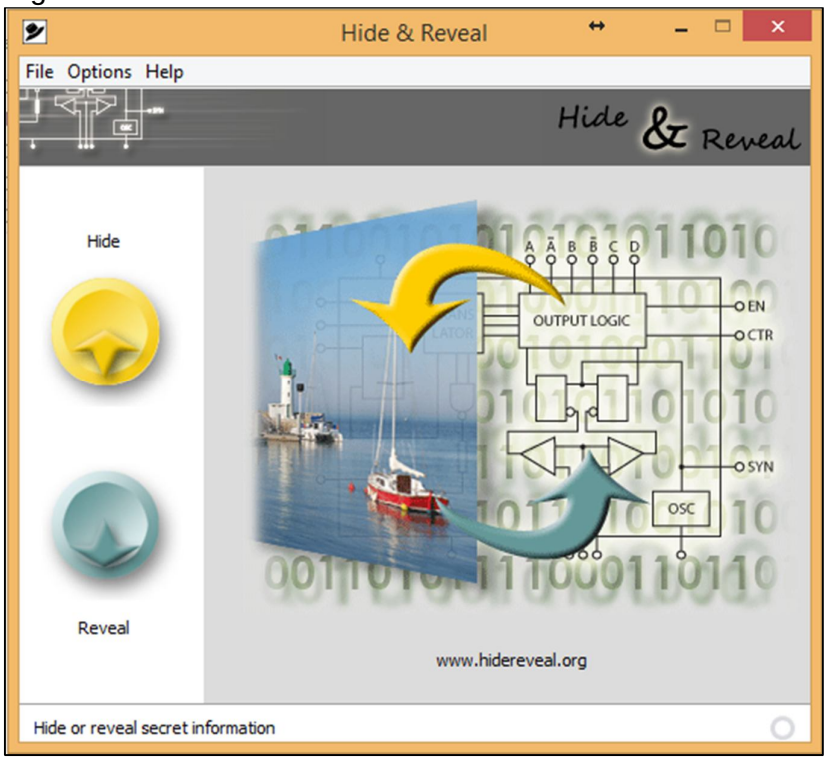
a) Single LSB;

b) Double LSB: Cada bit codificado utiliza 2 pixels de 32 bits;

c) Triple LSB: Cada byte codificado utiliza 1 único pixel.

A Figura 15 ilustra a tela principal da ferramenta Hide And Reveal, uma interface de fácil utilização e entendimento, com as opções de ocultar uma informação ou revelar uma mensagem que pode ter sido inserida em uma imagem.

Figura 15 - Ferramenta Hide And Reveal



Fonte: Hide And Reveal (2014).

3.6.2.3 SilentEye

A ferramenta SilentEye é uma aplicação multiplataforma com uma interface de fácil utilização, sendo capaz de esconder informações em imagens no formato **JPG**, também utilizando a técnica LSB. (CHOREIN, c2010).

A Figura 16 mostra a tela principal da ferramenta SilentEye, que por sua vez, também possui uma interface de fácil entendimento e permite que os dados sejam encriptados antes de esconde-los.

Figura 16 - Ferramenta SilentEye.

Fonte: SilentEye, (2014).

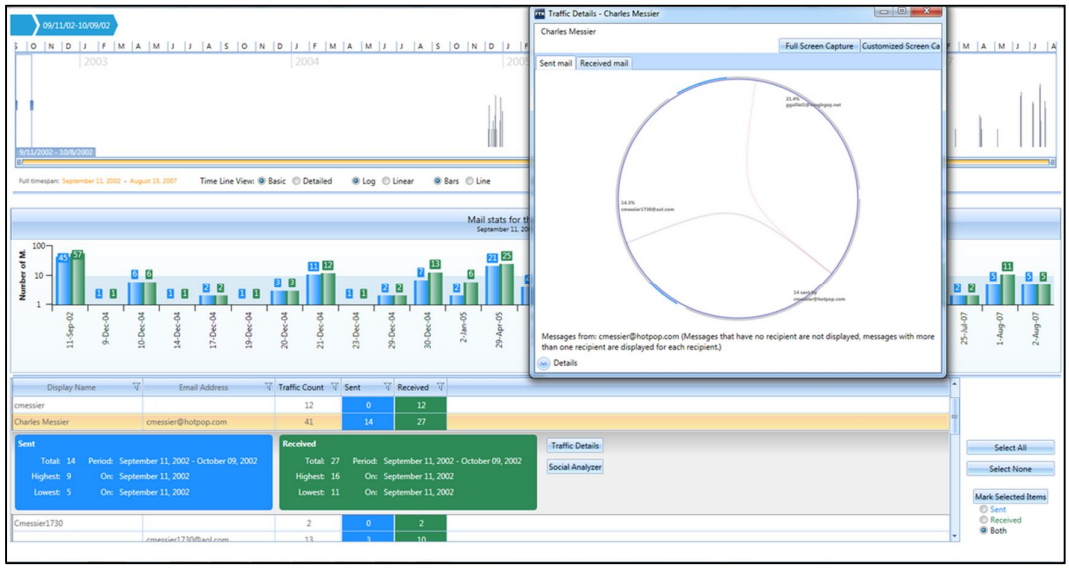
Outras ferramentas de perícia digital estão citadas a seguir.

3.6.2.4 Forensic Toolkit

Este é um software livre desenvolvido pela AccessData, e utilizado para coletar e analisar dados em uma perícia computacional. A ferramenta dispõe de vários recursos que podem ser utilizados para tais fins.

A Figura 17 apresenta uma das ferramentas do Forensic Toolkit, que possibilita visualizar o trafego de dados durante o período desejado, possibilitando, por exemplo, a análise por parte de uma empresa a fim de verificar o consumo de dados de um determinado período.

Figura 17 – Visualização de trafego de dados, disponível na ferramenta Forensic Toolkit.



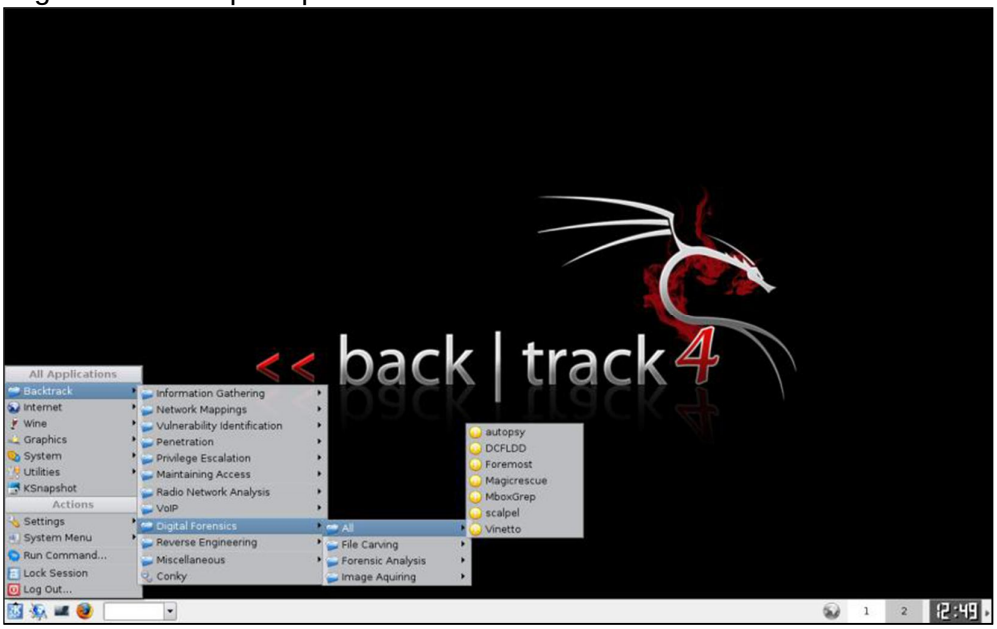
Fonte: AccessData Group, (c2014).

3.6.2.5 BackTrack

Trata-se de uma ferramenta que contem cerca de 300 programas, onde o foco é em testes de segurança e análise de vulnerabilidades. Também é utilizada para encontrar falhas em sistemas e em páginas web. Uma de suas vantagens é a de possuir diversos programas de manipulação de rede, o que torna possível ao usuário simular situações reais de invasão. (GONÇALVES et al. 2013).

Na Figura 18, pode-se ver a tela principal com um conjunto de ferramentas forenses em seu menu do BackTrack na versão 4.0, este baseado em um sistema de livre distribuição que também pode ser utilizado para fins criminais.

Figura 18 - Tela principal do BackTrack.

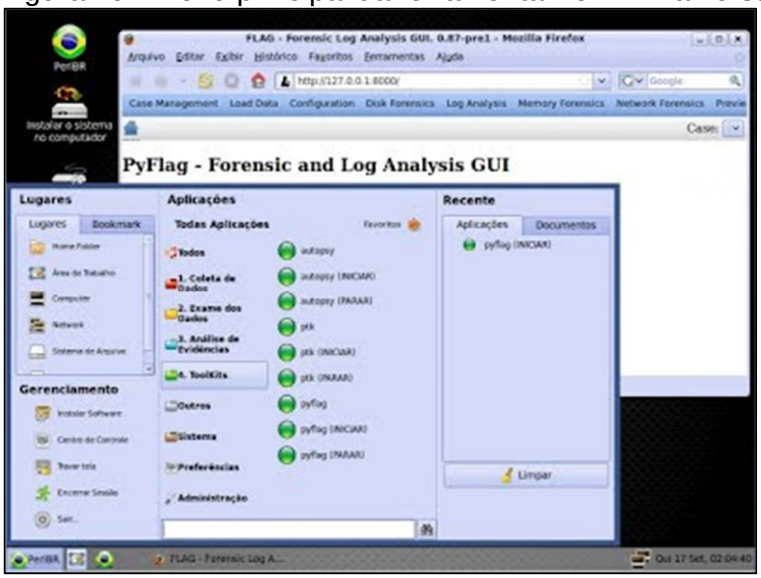


Fonte: Pereira, (2013).

3.6.2.6 PeriBR

É um software brasileiro desenvolvido por alunos de pós-graduação da Universidade Católica de Brasília na área de perícia computacional, baseado no sistema FDTK, possui as ferramentas que torna possível realizar uma investigação digital, pode-se ver na Figura 19 algumas de suas ferramentas que estão disponíveis. (PEREIRA, 2013).

Figura 19 - Menu principal da ferramenta PeriBR na versão 1.0

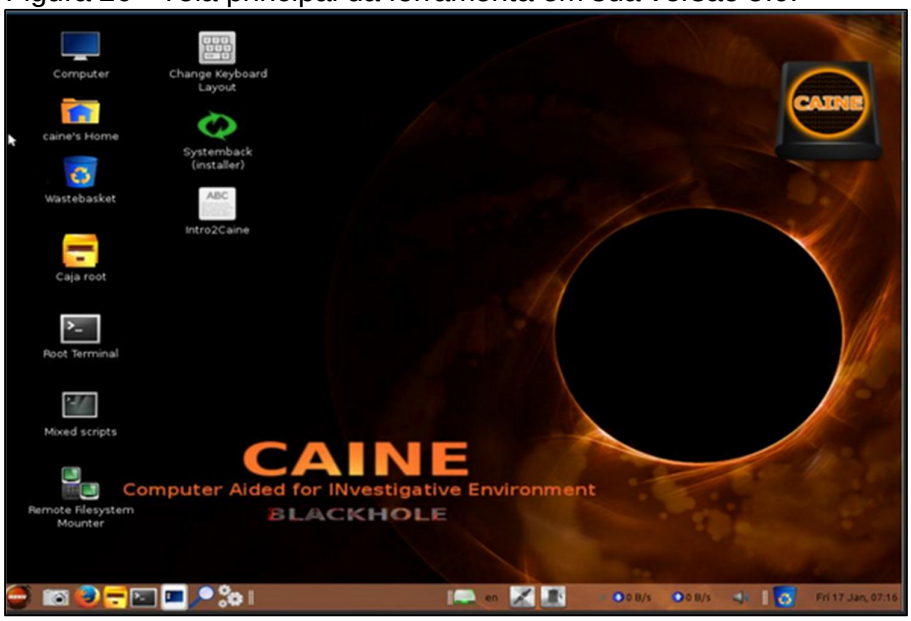


Fonte: Pereira, (2013).

3.6.2.7 Caine

Segundo Gonçalves, Amadio, Gavilan e Santos (2013), o Caine (Computer Aided Investigative Environment) é um software desenvolvido por peritos italianos, onde o objetivo é de criar um ambiente gráfico amigável ao usuário, conforme apresentado na Figura 20 que ilustra a tela principal da ferramenta em sua versão 5.0, de maneira a auxiliar na coleta, exame, analise e interpretação das informações, cumprindo com as etapas da investigação. Uma de suas vantagens é a de criar uma imagem semiautomática do relatório final da análise feita.

Figura 20 - Tela principal da ferramenta em sua versão 5.0.



Fonte: Bassetti, (20[--]).

4 TRABALHOS CORRELATOS

A área de esteganografia ainda tem muito a ser explorada, embora venha sendo tratada e estudada com maior amplitude de uns tempos para cá, tendo em vista a grande evolução tecnológica, bem como seu crescimento no uso para fins criminais.

Por se tratar de um tema amplo e com diversos métodos e técnicas para serem aplicadas, a esteganografia se tornou um desafio para os peritos, sendo necessários desenvolvimento e uso de softwares que atendam suas necessidades de análise, além de raciocínio lógico, para entender e interpretar as informações para que se obtenha um resultado final plausível e mais próximo da verdade.

Hoje é possível encontrar trabalhos e artigos que falam a respeito de métodos e aplicações das técnicas esteganográficas a fim de transmitir uma mensagem secreta a um destinatário, utilizando uma imagem, um vídeo, uma música, ou outro tipo de arquivo, de forma que não chame a atenção durante o tráfego, além de estudos para analisar métodos para interceptar e capturar a mensagem que está sendo transmitida de forma oculta.

Dentro deste contexto pode-se citar o trabalho de conclusão de curso intitulado “Esteganografia: Análise de técnicas aplicadas a segurança da informação”, de autoria de Maria Roseane Teixeira Pereira, que aborda testes práticos com as ferramentas esteganográficas Camouflage e JPHS, onde o objetivo é mostrar o antes e o depois do ocultamento de informação em imagens, e depois analisar os resultados comparando com os valores hexadecimais das imagens.

As ferramentas foram escolhidas por utilizarem diferentes técnicas de esteganografia, ampliando as chances de se obter resultados plausíveis.

Outro trabalho tomado como base é o “Esteganografia”, do autor Marcelo Petri, apresentado ao Instituto Superior Tupy, em Joinville no ano de 2004. Este fala sobre o que é esteganografia e suas funcionalidades, e apresenta ainda algumas técnicas esteganográficas, tomando como princípio o cuidado com a informação.

Dessa forma, este trabalho tem como intuito analisar algumas ferramentas de esteganografia, a fim de coletar resultados relevantes sobre sua eficiência e qualidade durante o processo, e também colaborar com futuros trabalhos e pesquisas sobre o assunto abordado.

5 METODOLOGIA

O presente trabalho foi desenvolvido em duas etapas, onde a primeira etapa foi a busca de informações e aspectos históricos e a segunda foi a etapa prática de aplicação de técnicas de esteganografia e análise dos resultados.

Na primeira etapa foi elaborado o referencial teórico, que consistiu em levantar informações e aspectos históricos para mostrar as definições sobre esteganografia e suas técnicas utilizadas atualmente dentro da perícia computacional. Estudos relacionados a área de segurança da informação, segurança digital e pericia computacional, também foram abordadas no decorrer do trabalho.

Na segunda etapa, a parte prática, teve como intuito a instalação das ferramentas Stegdetect, baseado na plataforma FDTK, distribuição Linux, Hide and Reveal e SilentEye, baseados em Windows.

As aplicações foram realizadas em um notebook particular Acer Aspire M, plataforma Windows 8.1 de 64 bits, processador Intel Core i-5 3317U CPU @ 1.70GHz e memória RAM de 4 GB. E para as aplicações em plataforma Linux, foi utilizado uma máquina virtual (VMware) em plataforma FDTK.

Depois de instalados, os testes foram realizados, inserindo uma mensagem, mensagem essa criada aleatoriamente, onde fosse curta porem tivesse sentido: “Este é o TCC apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração.” em imagens nos formatos JPG e BMP de dimensões 256, 512 e 1024 pixels, para que fosse possível comparar os resultados encontrados e apresenta-los como qual a melhor técnica e ferramenta a ser utilizada não só por sua eficiência, mas também pela integridade do arquivo após sua modificação, onde a melhor será aquela que atenda todos ou quase todos os requisitos.

Foram escolhidas imagens coloridas para que fosse possível identificar mais facilmente distorções visuais nas imagens, após as modificações, imagens estas que foram retiradas da internet em tamanhos e formatos predefinidos, de acordo com o que cada ferramenta suporta.

A distribuição dos testes seguiram as definições conforme pode-se ver na Figura 21, onde as ferramentas Stegdetect e SilentEye suportam imagens no formato JPG e a ferramenta Hide And Reveal que suporta imagens BMP. Foram

utilizadas 3 imagens de diferentes dimensões para cada ferramenta, de maneira que uma quantidade maior de resultados fossem gerados, ampliando a possibilidade de resultados diferentes.

Figura 21 – Disposição dos testes de acordo com a ferramenta e respectiva imagem.

Software	Formato da Imagem		Tamanho da Imagem (pixels)		
	JPG	BMP	256	512	1024
Stegdetect	X		X	X	X
Hide And Reveal		X	X	X	X
SilentEye	X		X	X	X

Fonte: Elaborado pelo autor.

Os softwares mencionados foram escolhidos por serem gratuitos, e por se tratarem de duas plataformas distintas, a fim de descobrir em qual delas o processo realizado foi mais eficiente, e também analisar mais de uma técnica e mais de um tipo de imagem.

Após finalizar as inserções, as imagens originais e modificadas foram dispostas para que fosse possível compará-las e, assim, verificar se no arquivo final houve alguma alteração perceptível a olho nu. Posteriormente, um quadro comparativo foi elaborado apresentando os resultados das inserções, apontando qual ferramenta foi capaz de gerar uma imagem segura e íntegra, com o mínimo de alterações possíveis.

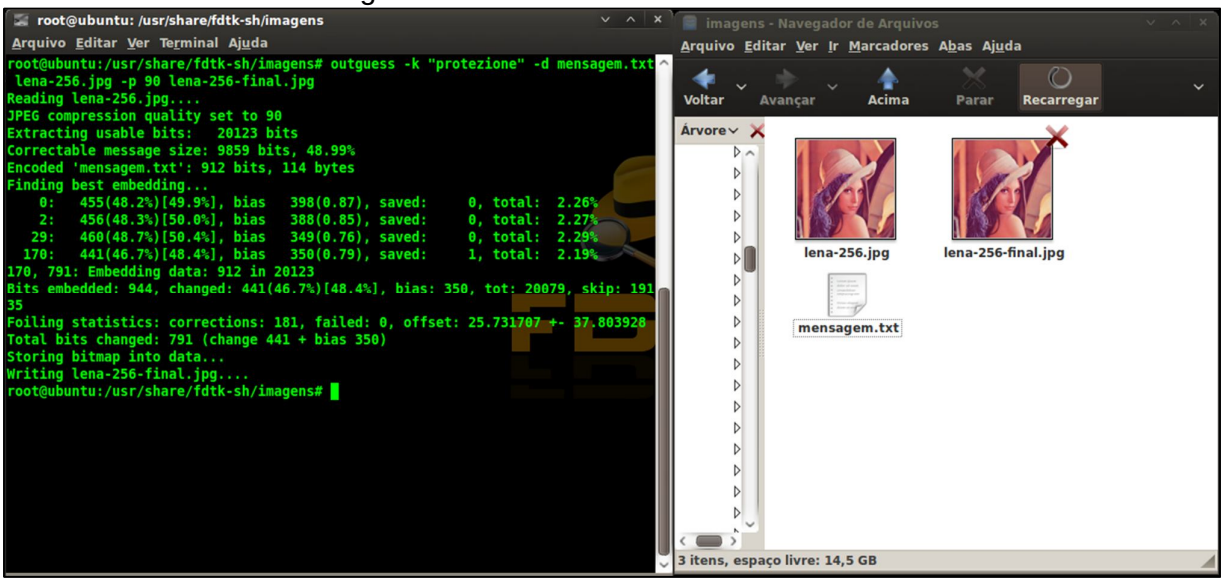
6 RESULTADOS FINAIS

As três ferramentas foram utilizadas com o intuito de aplicar técnicas de esteganografia de maneira que fosse possível analisar qual ferramenta trabalha de maneira mais eficiente, analisando sua qualidade visual, bem como o tamanho do arquivo após a modificação.

Para obter uma precisão maior nos resultados, foram testados três arquivos de diferentes tamanhos e com a extensão de acordo com a suportada pela ferramenta, e para uma melhor interpretação, os resultados foram tabulados com perguntas-chave. As imagens originais e modificadas foram colocadas em paralelas, como pode ser observado adiante, de forma que fosse possível visualizar os resultados.

A Figura 22 consiste na inserção da mensagem “Este é o TCC apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração.”, num arquivo no formato “txt” de tamanho 109 bytes, em uma imagem JPG 256 x 256, utilizando a ferramenta Stegdetect.

Figura 22 – Inserção da mensagem em uma imagem JPG de 256 x 256 utilizando a ferramenta Stegdetect.

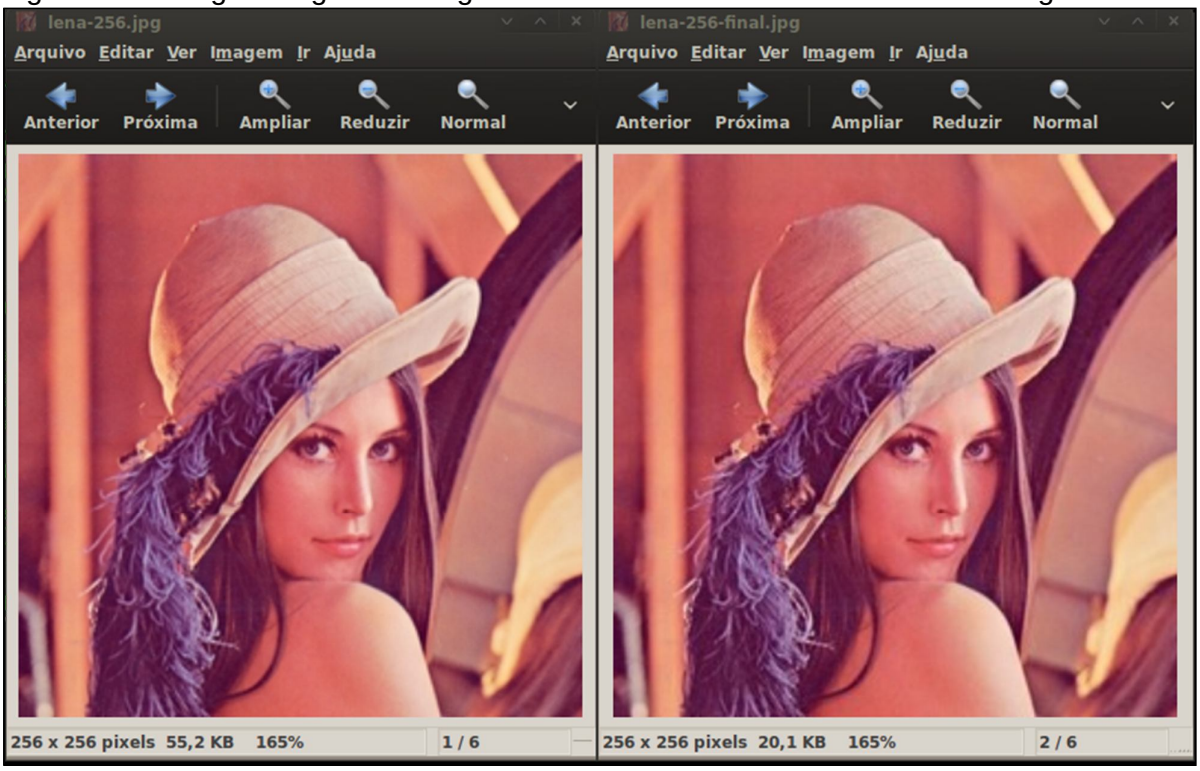


Fonte: Stegdetect, 2014.

Ainda de acordo com a Figura 22, pode-se ver a imagem original (à esquerda) e a imagem gerada após a inserção da mensagem (à direita), a qual teve uma redução de 63,6% no tamanho do arquivo, passando de 55,2 Kb para 20,1 Kb. Já de acordo com a Figura 23, é possível ver as imagens original e modificada,

respectivamente. A imagem modificada não teve grande alteração visual pois de acordo com o padrão oferecido pela ferramenta, o nível de qualidade da imagem foi mantida em 90%.

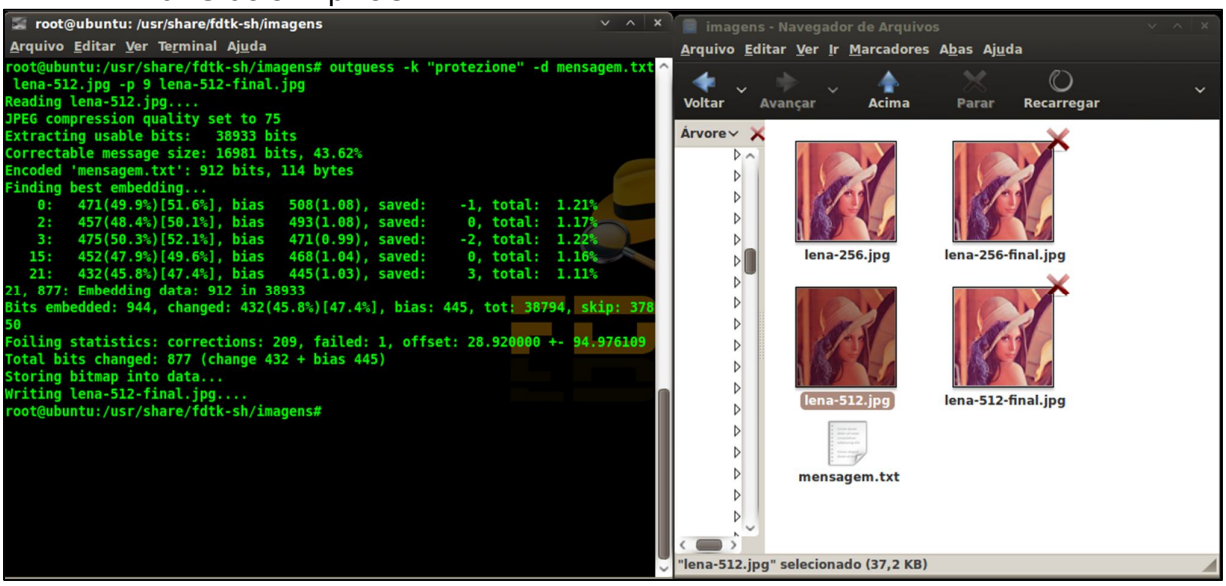
Figura 23 – Imagem original e imagem modificada utilizando a ferramenta Stegdetect



Fonte: Stegdetect, 2014.

A Figura 24 representa a inserção da mesma mensagem, utilizando a ferramenta Stegdetect em uma imagem no formato JPG de tamanho 512 x 512. Ao final da inserção, foi gerada uma imagem final (à direita na segunda linha) a qual manteve-se no mesmo tamanho da imagem original (à esquerda), 37,2 Kb, e conforme pode-se ver na Figura 25, não houve falhas aparentes na imagem pela qualidade da mesma ter sido mantida em 90% durante o processo de inserção.

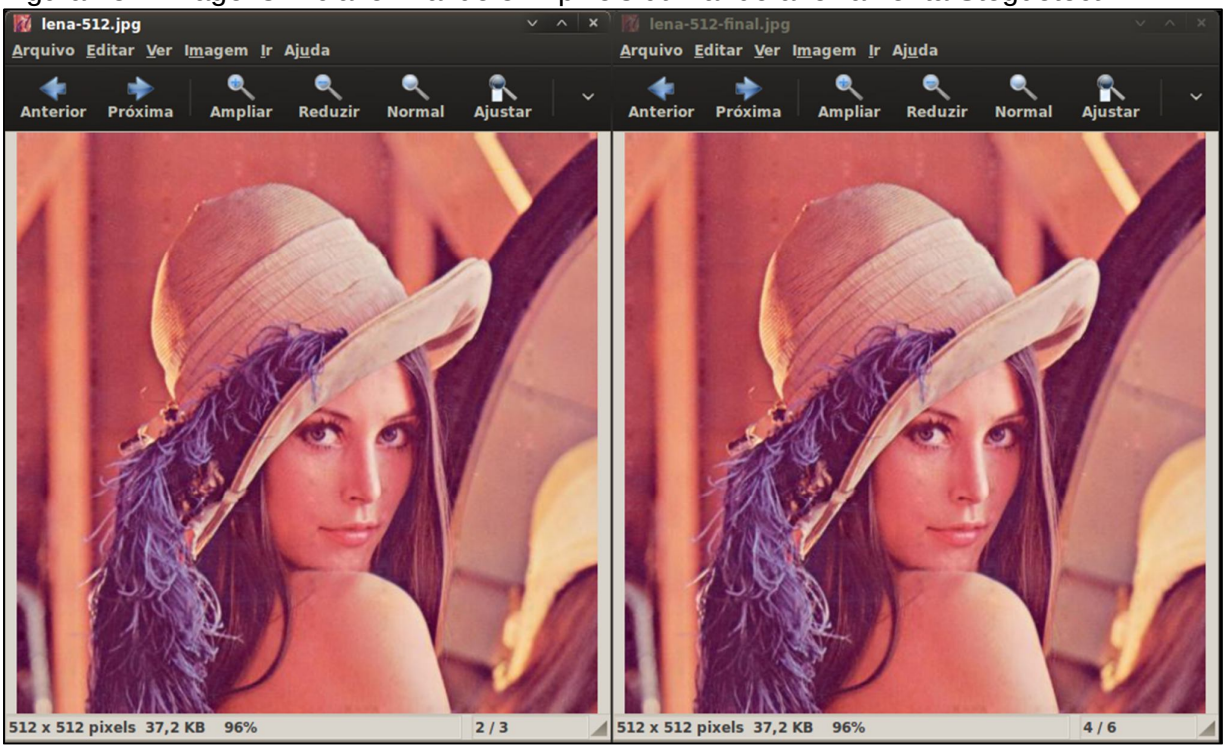
Figura 24 – Inserção da mensagem utilizando a ferramenta Stegdetect em uma imagem JPG de 512 pixels.



Fonte: Stegdetect, 2014.

Conforme pode ser visto na Figura 25, as imagens original (à esquerda) e final (à direita), não sofreu distorções perceptíveis a olho nu na imagem.

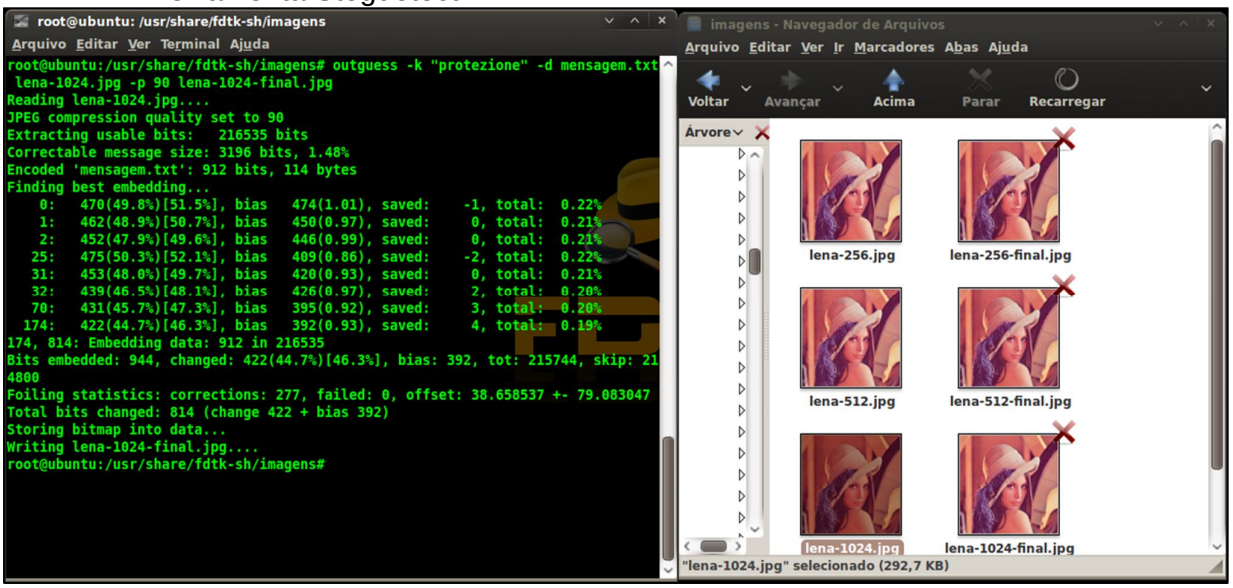
Figura 25 – Imagens inicial e final de 512 pixels utilizando a ferramenta Stegdetect.



Fonte: Stegdetect, 2014.

Na Figura 26, pode-se ver a inserção da mensagem em uma imagem JPG de dimensões 1024 x 1024 pixels utilizando a ferramenta Stegdetect.

Figura 26 – Inserção da mensagem em uma imagem de 1024 pixels utilizando a ferramenta Stegdetect.

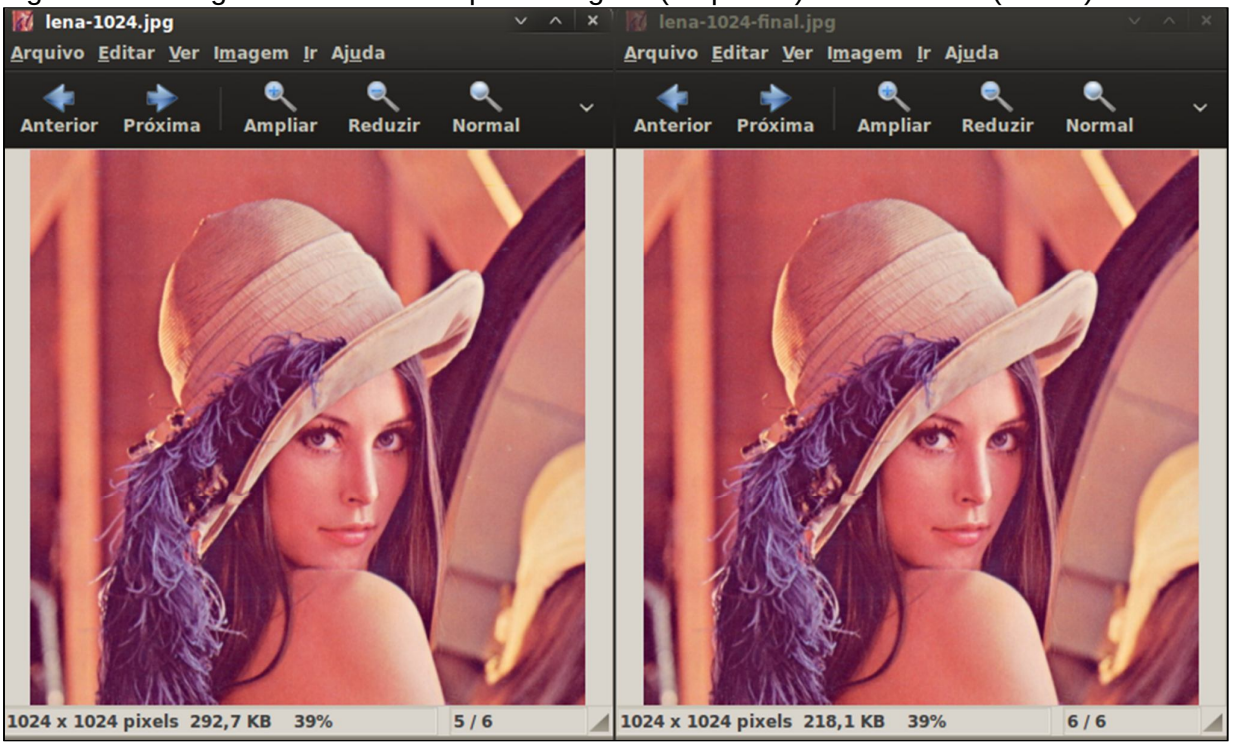


Fonte: Stegdetect, 2014.

Ao final da inserção, um novo arquivo foi gerado, sendo que este sofreu uma perda de 25,5% no tamanho do arquivo, passando de 292,7 Kb para 218,1 Kb.

Já na Figura 27, é possível ver as imagens original (à esquerda) e modificada (à direita), que de acordo com o padrão da ferramenta, teve sua qualidade foi mantida em 90%, e proporcionou que a imagem final não sofresse alterações perceptíveis a olho nu após a inserção da mensagem.

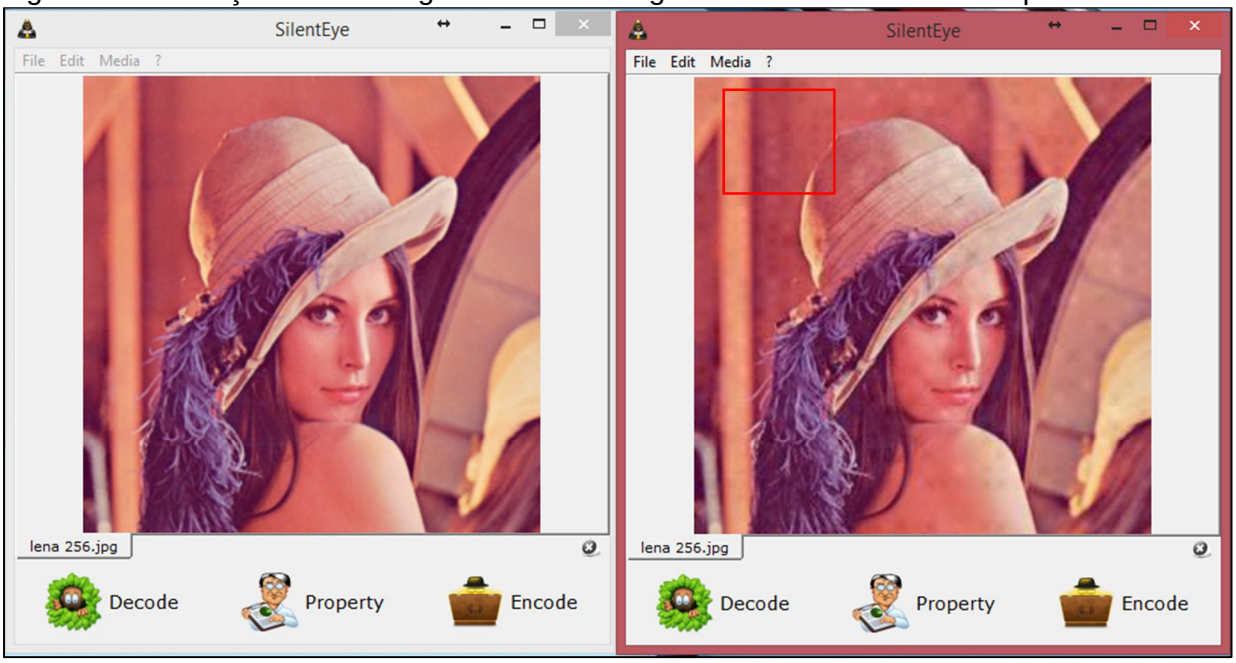
Figura 27 – Imagens JPG de 1024 pixels original (esquerda) e modificada (direita).



Fonte: Stegdetect, 2014.

A Figura 28 consiste na utilização da ferramenta SilentEye para inserir a mesma mensagem utilizada na ferramenta anterior – “Este é o TCC apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração.” – contida num arquivo “txt” de 109 bytes, em uma imagem no formato JPG de 256 pixels mantendo em 75% a qualidade da imagem, de acordo com o padrão apresentado pela ferramenta.

Figura 28 – Inserção da mensagem em uma imagem JPG de dimensão 256 pixels.

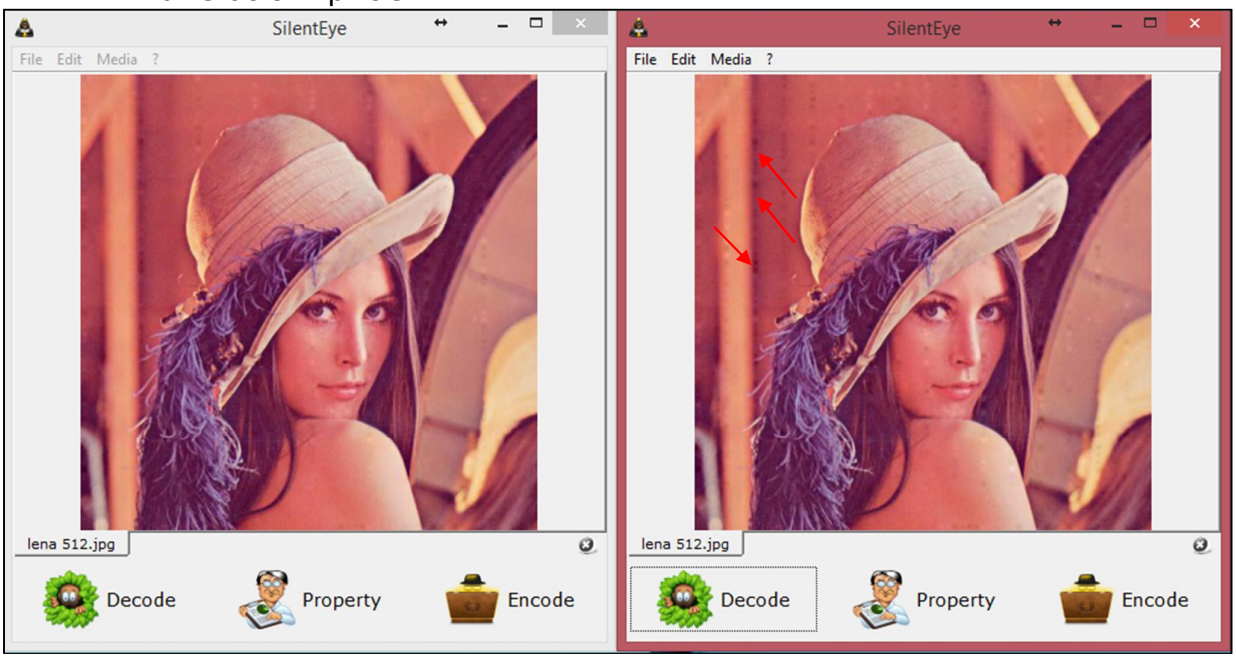


Fonte: SilentEye, 2014.

É possível identificar que na imagem modificada (à direita), existem falhas visíveis, como por exemplo o destaque em vermelho na imagem, esta que também sofreu uma perda de 77,9% no tamanho do arquivo, assumindo o valor de 12,2 Kb, diferentemente da imagem original, que possuía 55,1 Kb.

Na Figura 29, é possível ver a imagem original (à esquerda) e a imagem após a inserção da mensagem (à direita). Neste processo foi utilizada uma imagem no formato JPG de 512 pixels e qualidade mantida em 75%, de acordo com o padrão oferecido pela ferramenta. Após a inserção da mensagem, um novo arquivo foi gerado, onde este arquivo sofreu um aumento de 0,53% no seu tamanho, passando de 37,1 Kb para 37,3 Kb.

Figura 29 – Utilizando a ferramenta SilentEye para inserir a mensagem em uma imagem JPG de 512 pixels.

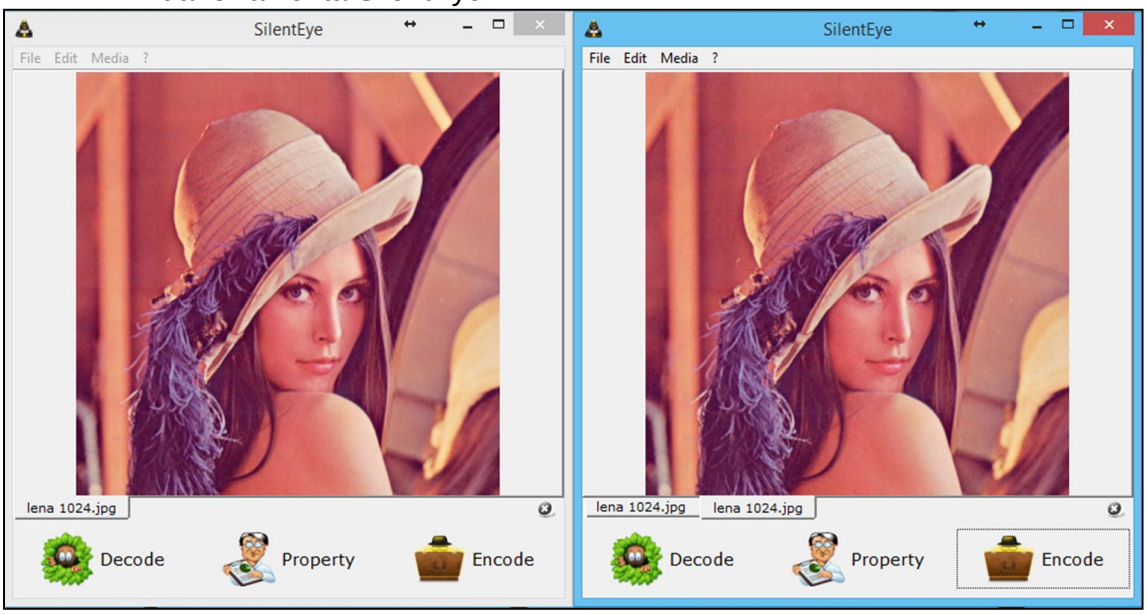


Fonte: SilentEye, 2014.

Na imagem final gerada pela ferramenta, é possível identificar que pontos mais escuros estão destacados na imagem, estes que não são perceptíveis na imagem original.

Já na Figura 30, ainda trabalhando com a ferramenta SilentEye, foi utilizada uma imagem no formato JPG de 1024 pixels para inserir o arquivo contendo a mensagem. Durante o processo, a qualidade da imagem também foi mantida em 75% (de acordo com o apresentado pela ferramenta). Por se tratar de uma imagem de alta qualidade, não foi possível identificar alterações visíveis a olho nu na imagem final, porém, a mesma teve uma redução de 60,7% no tamanho do arquivo, passando de 292 Kb para 115 Kb.

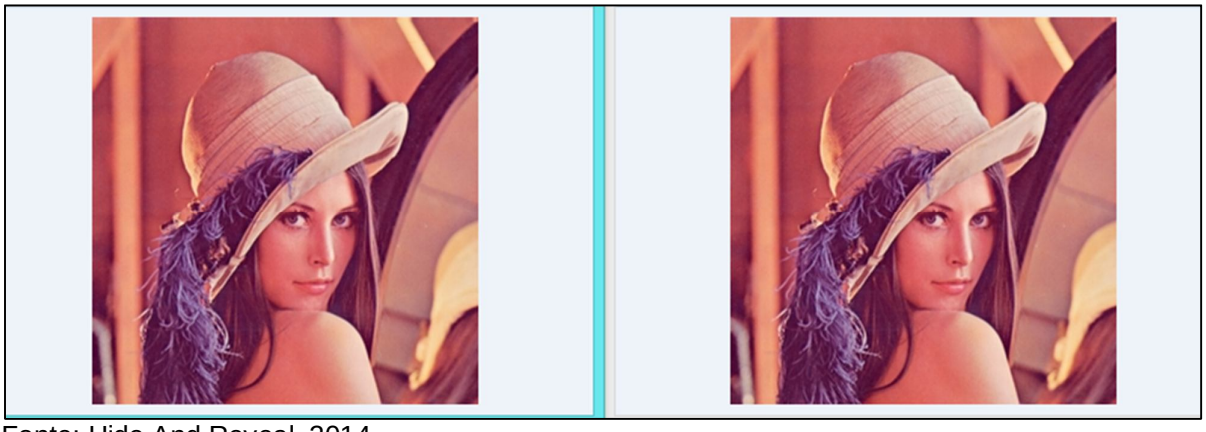
Figura 30 – Inserção da mensagem na imagem no formato JPG de 1024 pixels, através da ferramenta SilentEye.



Fonte: SilentEye, 2014.

Na Figura 31, o teste foi realizado em uma imagem de formato BMP e 256 pixels, utilizando a ferramenta Hide And Reveal. Foi utilizada a mesma mensagem – “Este é o TCC apresentado ao Centro de Ciências Exatas e Sociais Aplicadas da Universidade do Sagrado Coração.” – em um arquivo txt de 109 bytes.

Figura 31 – Imagem BMP de 256 pixels original (à esquerda) e modificada (à direita) utilizando a ferramenta Hide And Reveal.



Fonte: Hide And Reveal, 2014.

Após a inserção da mensagem, foi gerado um novo arquivo onde não é possível identificar falhas visíveis na imagem final, porém, houve um aumento de 248% no arquivo, passando de 55,1 Kb para 192 Kb.

Já na Figura 32, foi utilizada uma imagem no formato BMP de 512 pixels, inserindo o arquivo de 109 bits contendo a mensagem através da ferramenta Hide And Reveal. Ao final da inserção, uma nova imagem foi gerada com a mensagem embutida.

Figura 32 – Imagem BMP de 512 pixels original (à esquerda) e imagem final (à direita) utilizando a ferramenta Hide And Reveal.

Fonte: Hide And Reveal, 2014.

A imagem final sofreu um aumento de 1.530% no tamanho do arquivo, passando de 47,1 Kb para 768 Kb. Neste processo, não foi possível identificar falhas perceptíveis na imagem final.

Na Figura 33, uma imagem no formato BMP de 1024 pixels foi utilizada para inserir o arquivo “txt” contendo a mensagem. Ao término do processo de inserção, um novo arquivo de imagem foi gerado com a mensagem inserida.

Figura 33 – Imagem BMP de 1024 pixels original (à esquerda) e final (à direita) utilizando a ferramenta Hide And Reveal.

Fonte: Hide And Reveal, 2014.

Neste processo, também não foi possível identificar falhas visíveis na imagem final, porém a mesma sofreu uma alteração de tamanho do arquivo em 927%, passando de 292 Kb para 3 Mb, fazendo com que este não fosse o melhor método de aplicação esteganográfica em uma imagem.

6.1 ANÁLISE COMPARATIVA DOS RESULTADOS

Após dispor as imagens geradas de modo que fosse possível identificar falhas visuais, tabelas foram criadas para realizar comparações entre os arquivos originais e os finais.

A Figura 34 apresenta a comparação entre os arquivos originais e os finais criados após a inserção da mensagem, utilizando imagens de 256 pixels. Das três ferramentas utilizadas, duas delas geraram um arquivo com tamanho inferior ao original, porém, conforme discutido anteriormente, na ferramenta Stegdetect não houve alterações visíveis na imagem, já na ferramenta SilentEye, puderam ser vistas distorções na imagem final. Já na ferramenta Hide And Reveal, não houve alterações perceptíveis na imagem final, mas o tamanho do arquivo sofreu uma grande alteração. Sendo assim, neste comparativo, a ferramenta que apresentou melhor resultado foi a Stegdetect.

Figura 34 - Comparação entre imagens de resolução 256 x 256.

FERRAMENTA	ORIGINAL	GERADA	%
Stegdetect	55,1	20,1	-63,52
SilentEye	55,1	12,2	-77,86
Hide And Reveal	55,1	192	248,46

Fonte: Elaborado pelo autor.

Já a Figura 35, contempla o tamanho dos arquivos antes e depois das inserções utilizando as ferramentas abordada, em imagens JPG e BMP de 512 pixels. Nestes testes, assim como no realizado com as imagens de 256 pixels, a ferramenta Stegdetect e SilentEye apresentaram um arquivo menor ao final, mas novamente o arquivo gerado pela segunda ferramenta teve distorções visuais na imagem, diferentemente das outras, entretanto, novamente a ferramenta Hide And Reveal gerou um arquivo com um tamanho maior que a original, fazendo com que mais uma vez a ferramenta Stegdetect fosse escolhida como a ideal para essa inserção.

Figura 35 – Comparação entre imagens de resolução 512 x 512.

FERRAMENTA	ORIGINAL	GERADA	%
Stegdetect	37,1	37,2	0,27
SilentEye	37,1	37,3	0,54
Hide And Reveal	47,1	768	1530,57

Fonte: Elaborado pelo autor.

A Figura 36 apresenta a comparação entre os arquivos originais e finais através das ferramentas definidas, em imagens nos formatos JPG e BMP de 1024 pixels, e como pode ser observado, as ferramentas atuaram da mesma forma como nos dois últimos testes, onde a ferramenta SilentEye apresentou uma alteração considerável no tamanho do arquivo final, além de pequenas distorções visuais na imagem. Já na ferramenta Stegdetect, o arquivo sofreu pouca alteração no tamanho e nenhuma redução na qualidade da imagem, como pode ser vista na Figura 27, assim como na ferramenta Hide And Reveal, que por sua vez gerou um arquivo num tamanho superior ao original, sendo assim, a ferramenta Stegdetect também foi escolhida como a ideal.

Figura 36 - Comparação entre imagens de resolução 1024 x 1024.

FERRAMENTA	ORIGINAL	GERADA	%
Stegdetect	292	218,1	-25,31
SilentEye	292	115	-60,62
Hide And Reveal	292	3072	952,05

Fonte: Elaborado pelo autor.

Na Figura 37, os resultados foram separados pelo formato da imagem e pela ferramenta que foi utilizada, de maneira que fosse possível comparar a funcionalidade da mesma individualmente e analisar em qual das imagens o resultado foi mais satisfatório. De acordo com a ferramenta Stegdetect, nenhuma das imagens modificadas sofreram alteração visual perceptível, e os níveis de tamanho de arquivo não sofreram grandes mudanças. De tal forma, pode-se considerar que o melhor resultado obtido foi com a imagem de 512 pixels, esta que teve a menor taxa de alteração no tamanho do arquivo e sem alterações na qualidade do mesmo.

Figura 37 – Ferramenta Stegdetect: Comparação entre resoluções diferentes em imagem do tipo JPG.

256 x 256			512 x 512			1024 x 1024		
ORIGINAL	GERADA	%	ORIGINAL	GERADA	%	ORIGINAL	GERADA	%
55,1	20,1	-63,52	37,1	37,2	0,27	292	218,1	-25,31

Fonte: Elaborado pelo autor.

A Figura 38 apresenta os resultados gerados pela ferramenta SilentEye, esta que proporcionou os piores resultados, já que a qualidade das imagens foram afetadas e houveram variações no tamanho dos arquivos finais. Esses resultados podem chamar a atenção de investigadores ou mesmo curiosos. Por fim, nesta ferramenta, a inserção que apresentou melhor resultado, utilizando a imagem de 1024 pixels, sendo que esta não sofreu redução na qualidade visual.

Figura 38 – Ferramenta SilentEye: Comparação entre resoluções diferentes em imagem do tipo JPG.

256 x 256			512 x 512			1024 x 1024		
ORIGINAL	GERADA	%	ORIGINAL	GERADA	%	ORIGINAL	GERADA	%
55,1	12,2	-77,86	37,1	37,3	0,54	292	115	-60,62

Fonte: Elaborado pelo autor.

Já a Figura 39, mostra os resultados gerados pela ferramenta Hide And Reveal, onde os testes foram realizados utilizando imagens no formato BMP. Ao final dos testes, as imagens finais não sofreram nenhuma alteração visual, porém, os arquivos tiveram um aumento significativo de tamanho, o que também poderia ser motivo de chamar a atenção de investigadores ou curiosos. Todavia, o melhor resultado apresentado por esta ferramenta, foi utilizando a imagem de 256 pixels, já que ela obteve o menor índice de aumento no tamanho do arquivo.

Figura 39 – Ferramenta Hide And Reveal: Comparação entre resoluções diferentes em imagem do tipo BMP.

256 x 256			512 x 512			1024 x 1024		
ORIGINAL	GERADA	%	ORIGINAL	GERADA	%	ORIGINAL	GERADA	%
55,1	192	248,46	47,1	768	1530,57	292	3072	952,05

Fonte: Elaborado pelo autor.

Na Figura 40, os resultados foram divididos pelas ferramentas que trabalham com imagens no formato JPG, onde é possível identificar que a ferramenta Stegdetect apresentou melhores resultados, já que não houveram alterações visuais perceptíveis e o tamanho dos arquivos tiveram uma pequena redução.

Figura 40 – Comparação por ferramenta e imagem do tipo JPG

FERRAMENTA	256 x 256			512 x 512			1024 x 1024		
	ORIGINAL Tamanho	GERADA Tamanho	%	ORIGINAL Tamanho	GERADA Tamanho	%	ORIGINAL Tamanho	GERADA Tamanho	%
Stegdetect	55,1	20,1	-63,521	37,1	37,2	0,27	292	218,1	-25,31
SilentEye	55,1	12,2	-77,86	37,1	37,3	0,54	292	115	-60,6164384

Fonte: Elaborado pelo autor.

Já na Figura 41, os resultados gerados foram dispostos independentes do formato e tamanho da imagem, de forma que seja possível ver qual das ferramentas proporcionou o melhor resultado. Como já definido nas outras demonstrações, a ferramenta Stegdetect foi a que apresentou os melhores resultados, tanto por manter a qualidade das imagens quanto por não gerar alterações consideráveis no tamanho dos arquivos.

Figura 41 – Comparação por ferramenta e resolução de imagem

FERRAMENTA	256 x 256			512 x 512			1024 x 1024		
	ORIGINAL	GERADA		ORIGINAL	GERADA		ORIGINAL	GERADA	
	Tamanho	Tamanho	%	Tamanho	Tamanho	%	Tamanho	Tamanho	%
Stegdetect	55,1	20,1	-63,521	37,1	37,2	0,27	292	218,1	-25,31
SilentEye	55,1	12,2	-77,86	37,1	37,3	0,54	292	115	-60,62
Hide And Reveal	55,1	192	248,457	47,1	768	1530,57	292	3072	952,05

Fonte: Elaborado pelo autor.

7 CONSIDERAÇÕES FINAIS

As ferramentas escolhidas se destacam por serem gratuitas e por trabalharem em duas plataformas diferentes, ampliando a possibilidade de diferenciar os resultados finais.

Nos testes realizados na ferramenta Stegdetect, o trabalho foi mais complexo, por utilizar a mesma em uma máquina virtual instalada na plataforma Windows. Por se tratar de uma ferramenta baseada em Linux, é necessário um conhecimento um pouco mais profundo em linhas de comando. Das três imagens geradas ao final das inserções pela ferramenta Stegdetect, nenhuma delas sofreu alguma alteração perceptível a olho nu, bem como os tamanhos dos arquivos, que por sua vez não sofreram grandes alterações.

Já a ferramenta SilentEye, é uma ferramenta que trabalha em plataforma Windows e possui uma interface mais amigável ao usuário, tornando seu uso mais fácil. Já os resultados finais gerados por esta ferramenta, não foram satisfatórios, pois os três arquivo finais sofreram alterações visíveis nas imagens, entretanto os tamanhos dos arquivos sofreram um aumento menos significativo. Pelos defeitos visuais apresentados, esta ferramenta não é considerada com boa opção de uso.

A ferramenta Hide And Revel também trabalha em plataforma Windows e possui uma interface amigável ao usuário. Nos testes realizados utilizando-a, os arquivos gerados ao final das inserções não tiveram modificações visíveis a olho nu, por outro lado, os tamanhos dos arquivos finais tiveram um aumento exorbitante, o que pode ser um motivo para chamar a atenção de analistas de segurança, ou até mesmo curiosos e/ou interessados no assunto.

De acordo com os resultados gerados, pode-se julgar a ferramenta Stegdetect como a mais indicada para se ocultar uma informação em uma imagem, pois gerou um arquivo sem falhas, e capaz de ser transmitido sem chamar a atenção. Já a ferramenta SilentEye não é a mais indicada por prejudicar a qualidade final das imagens, tornando-as alvos de desconfiança e de possíveis análises durante sua transmissão. A ferramenta Hide And Reveal apresentou bons resultados, mas deixou a desejar na discrição dos tamanhos dos arquivos, que também podem ser alvos de desconfiança e observação.

REFERÊNCIAS

ACCESSDATA GROUP, Forensic Toolkit® 5. **Accessdata**, c2014. Disponível em: <http://www.accessdata.com/solutions/digital-forensics/ftk>. Acessado em: 31 ago 2014.

BASSETTI, N., Caine Computer Forensics Linux Live Distro. **Caine-live.net**, c20[--]. Disponível em: <http://www.caine-live.net>. Acessado em 31 ago 2014.

CAPURRO, R.; HJORLAND, B., O Conceito de informação[1]. **Ufmg**, 2007. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/viewFile/54/47>. Acessado em: 10 Set 2014.

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. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-08062009-143448/pt-br.php>. Acessado em: 04 maio 2014.

CARVALHO, D. F.; GOULARTE, R. Esteganografia Digital: Uma abordagem baseada em vídeos. **Stoa.usp**, [20--]. Disponível em: <http://stoa.usp.br/diegofdc/files/-1/1305/StegoVideoDiegoRudinei_final.pdf>. Acessado em: 04 maio 2014.

CARVALHO, G. M. Assinatura Digital. **Assinatura-digital.info**, [20--]. Disponível em: <http://assinatura-digital.info/>. Acessado em: 05 abr. 2014.

Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. Criptografia. **cartilha.cert**, c2012. Disponível em: <http://cartilha.cert.br/criptografia/>. Acessado em: 05 abr. 2014.

CHIRIGATI, F. S.; KIKUCHI, R. S. A.; GOMES, T. L. Esteganografia. **Gta.ufrj**, c2006. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html>. Acessado em: 09 abr. 2014.

CHOREIN, A., SilentEye Steganography is yours. **Silenteye.org**, c2010. Disponível em: <http://www.silenteye.org/changes.html?i1s3>. Acessado em: 20 abr 2014.

COTTIN, N., Hide and Reveal. **Hidereveal.org**, c2013. Disponível em: <http://hidereveal.ncottin.net/>. Acessado em: 20 abr 2014.

CRIME Digital – Cibercrime. **SaferNet Brasil**, c2008. Disponível em: <http://www.safernet.org.br/site/prevencao/cartilha/safer-dicas/crime>. Acessado em: 31 mar 2014.

GALVAO, JR. Diferenças entre chaves simétrica e assimétrica para criptografia. **wordpress.com**, c2007. Disponível em: <http://pedrogalvaojunior.wordpress.com/2007/11/16/diferencas-entre-chaves-simetrica-e-assimetrica-para-criptografia/>. Acessado em: 05 abr. 2014.

GAZZARRINI, R. O que é assinatura digital? **Techmundo**, c2012. Disponível em: <http://www.tecmundo.com.br/web/941-o-que-e-assinatura-digital-.htm>. Acessado em: 05 abr. 2014.

GONÇALVES, M. et al., **Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas**, 2012. In: Revista Científica Eletrônica de Ciências Sociais Aplicadas da EDUVALE. Disponível em: <http://www.eduvalesl.edu.br/site/edicao/edicao-74.pdf>. Acessado em: 06 maio 2014.

GONZALES, P., Um Códice Ocultista de 500 Anos Desvelado. **Vopus.org**, c2005. Disponível em: <http://www.vopus.org/pt/gnose/dimensao-desconhecida/esteganografia-de-trithemius--codice-desvelado.html>. Acessado em: 25 ago. 2014.

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://jeiks.net/wp-content/uploads/2013/11/cap2-esteganografia.pdf>. Acessado em: 09 abr. 2014.

KOLLING, G. S. **Segurança da Informação**. [20--]. Disponível em: <http://seguranca-da-informacao.info/>. Acessado em: 10 mar 2014.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerenciais**. São Paulo: Pearson, 2007. v. 7.

MARTINS, E.; O que é cracker²? **Tecmundo**, 2012. Disponível em: <http://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm>. Acessado em: 16 out 2014.

VISÃO geral sobre os protocolos de autenticação. **Microsoft**, 2005. Disponível em: <http://technet.microsoft.com/pt-br/library/cc739177(v=ws.10).aspx>. Acessado em: 05 abr. 2014.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem, c2012. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. Acessado em: 05 abr. 2014.

PEREIRA, A. P.; O que é hash³? **Tecmundo**, 2009. Disponível em: <http://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm>. Acessado em: 16 out 2014.

PEREIRA, M. R. T. **Esteganografia: Análise de Técnicas Aplicadas a Segurança da Informação**, 2013. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Universidade do Sagrado Coração, Bauru, 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. Disponível em: <http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_petri_esteganografia.pdf>. Acessado em: 09 abr. 2014.

PISA, P. O que é criptografia? **Techtudo**, c2013. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html>. Acessado em: 05 abr. 2014.

PROVOS, N., Steganography Detection with Stegdetect. **Outguess.org**, c2004. Disponível em: <http://www.outguess.org/detection.php>. Acessado em: 20 abr 2014.

REPRODUÇÃO/GOOGLE. Certificados de Autenticação. **Techmundo**, c2012. Disponível em: <http://www.tecmundo.com.br/web/941-o-que-e-assinatura-digital-.htm>. Acessado em: 05 abr. 2014.

SILVA, A. A. G. **A Perícia Forense no Brasil**, 2010. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2010.

SOUZA, R. J. C. Segurança de Redes de Computadores. **Ricardojcsouza**, [30--]. Disponível em: <http://www.ricardojcsouza.com.br/download/seguranca_redes_4.pdf>. Acessado em: 10 abr. 2014.

TAIT, T. F. C. Evolução da Internet: do início secreto à explosão mundial. **Dim.uem**, c2007. Disponível em: <http://www.din.uem.br/~tait/evolucao-internet.pdf>. Acessado em: 31 mar 2014.

TOLENTINO, L. C.; SILVA, W. MELLO, P. A. M. S., **Perícia Forense Computacional**, 2011. In: Revista Tecnologias em Projeção. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/view/168/149>. Acessado em: 08 maio 2014.

TRINTA, F. A. M.; MACEDO, R. C. de. Um Estudo sobre Criptografia e Assinatura Digital. **Di.ufpe**, 1998. Disponível em: < http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acessado em: 05 abr. 2014.

Técnicas de Esteganografia: um comparativo entre as ferramentas Stegdetect, Hide And Reveal e SilentEye

Murilo José Marqui Botura, Elvio Gilberto da Silva, Patrick Pedreira Silva, Henrique Pachioni Martins

Centro de Ciências Exatas e Sociais Aplicadas – Universidade do Sagrado Coração (USC)
Bauru – SP – Brasil

Resumo. *A constante evolução tecnológica faz com que cada vez mais a informação esteja vulnerável, sendo assim, torna-se necessário o investimento em melhorias nas técnicas de segurança da informação. Este artigo consiste em apresentar a análise de três ferramentas esteganográficas onde o intuito foi inserir uma mensagem em imagens no formato JPG e BMP, de maneira que se fosse possível identificar qual das ferramentas apresentou o melhor resultado baseando-se na qualidade da imagem após sua modificação, bem como alterações consideráveis no tamanho dos arquivos.*

Abstract. *The constant evolution of technology makes the information more and more vulnerable, therefore, it is necessary to invest in techniques that improve information security. This article presents the analysis of three steganography tools where the goal was to insert a message into images in JPG and BMP format in a way that was possible to identify which of the tools had the best result based on the quality of the image as well as significant changes in the size of the files.*

1. Introdução

A constante evolução tecnológica faz com que a comunicação e a troca de informações se torne cada vez mais pratica e acessível a todos os públicos. A internet pode ser vista como um dos meios de comunicação mais utilizados atualmente, capaz de proporcionar lazer e praticidade aos usuários, entretanto, o seu uso de forma ilegal pode causar problemas envolvendo questões de segurança digital. Usuários que utilizam da internet como um meio de realizar crimes, se aproveitam de pequenas falhas em sistemas para invadir e roubar informações sigilosas. O termo cibercrimes é dado para estas práticas criminosas, que se tornam uma causa preocupante para empresas, usuários domésticos e até mesmo os governos. (CRIME..., c2008).

Um dos meios de transferir uma informação de forma segura é a criptografia, esta que consiste em converter a mensagem em códigos para que seja transmitida de forma segura, e ao ser recebida pelo destinatário, ela será decodificada para que o destinatário possa interpretá-la. Ainda que seja uma forma segura de transmissão de dados, é uma técnica capaz de chamar a atenção de curiosos, já que é possível desconfiar que em um

código criptografado pode conter alguma informação importante. (GALVAO, JUNIOR, C2007).

Segundo Pereira (2013), diferentemente da criptografia, a técnica de esteganografia tem como intuito transmitir uma mensagem de forma que possa passar despercebida a olho nu por outros usuários, para isso, utilizam-se textos, imagens, vídeos ou áudio para ocultar dados ou informações.

Com base nesse contexto, o presente trabalho tem como intuito contribuir com interessados na area de segurança digital, apresentando um referencial teorico abordando o tema esteganografia, além de técnicas de inserção, analise e detecção de informações em imagens e, ao final, estabelecer um comparative entre as ferramentas de esteganografia, que possam ser úteis para futuros trabalhos, e também para uso em perícias digitais.

2. Revisão da Literatura

2.1 Sistemas de Informação

Segundo Capurro e Hjorland (2007), podemos definir a informação como um conjunto organizado de dados, capaz de constituir uma mensagem sobre um fenômeno ou evento. O conceito de informação no sentido de conhecimento, caracteriza a sociedade como uma sociedade da informação, tendo em vista que a informação é uma condição básica para o desenvolvimento econômico.

Um sistema de informação pode ser definido como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações, de maneira que seja possível auxiliar na coordenação e controle de uma organização. (LAUDON; LAUDON, 2007).

2.2 Segurança da Informação

Existem várias maneiras de transmitirmos informações e atualmente, a internet vem tomando frente de revisas, jornais, televisão, dentre outros meios de comunicação, devido a sua acessibilidade.

Segundo Kolling ([20--]), quando se fala sobre segurança da informação, nos referimos a segurança daquilo que estamos transmitindo pela internet, ou por qualquer outro meio de comunicação. Tendo a internet como uma das principais vias de acesso as informações, é preciso respeitar três características básicas de segurança: confidencialidade, integridade e disponibilidade.

2.3 Criptografia

A palavra criptografia tem por significado “escrita secreta”, que tem como função converter uma mensagem em códigos, em um conjunto de informações ilegíveis e impossível de ser decifrado. O conceito visa que apensa quem tenha a chave para decriptação, consiga converter o código em mensagem legível novamente, de forma que a mensagem seja transmitida de forma segura e impedindo que usuários que não possuam essa chave de decodificação tenham acesso à mensagem. (PEREIRA, 2013).

Dois tipos de técnicas criptográficas podem ser citadas, a criptografia de chave simétrica, ou a criptografia assimétrica.

2.3.1 Criptografia de Chave Simétrica

A técnica de criptografia por chave simétrica, é a técnica mais antiga conhecida. Esta utiliza a mesma chave tanto para criptografar quanto para descriptografar uma mensagem, fazendo com que o processo seja realizado mais rapidamente. O texto original passa por um algoritmo de cifragem passando a partir daí a ser um texto cifrado, este que é transmitido ao usuário final, que por sua vez utiliza o mesmo algoritmo com a mesma chave para decifrar o texto, tornando-o compreensível novamente. (OLIVEIRA,2007).

Ainda de acordo com o autor citado anteriormente, sua simplicidade torna essa técnica mais vantajosa, por apresentar maior facilidade e rapidez na execução do processo, por outro lado, a principal desvantagem desta técnica, é utilizar da mesma chave para os dois processo, criptografar e descriptografar uma mensagem.

2.3.2 Criptografia de Chave Assimétrica

A criptografia por chave assimétrica é o método mais seguro de criptografia, já que é utilizado um par de chaves privadas no processo, uma chave para criptografar (chave pública) e uma chave privada para descriptografar. Um texto convencional passa pelo algoritmo de cifragem que possui uma chave pública, gerando a partir daí um texto cifrado, que por sua vez é repassado ao usuário final, que utiliza o algoritmo de decifragem com uma chave privada, tornando a mensagem compreensível novamente. (TRINTA; MACEDO, 1998).

A desvantagem de utilizar essa técnica, é que se trata de um algoritmo mais complexo e de difícil interpretação, causando uma perda na agilidade do processo. (OLIVEIRA, 2007).

2.4 Esteganografia

De acordo com Petri (2004), a esteganografia é a arte de ocultar informações utilizando técnicas onde o objetivo é se comunicar de forma secreta, proporcionando sigilo no momento da transmissão, de forma que a sua presença não seja percebida.

Uma das técnicas mais utilizadas, é a alteração do bit menos significativo de um pixel contido em uma imagem colorida, este que será substituído pelo bit da mensagem a ser oculta. (CHIRIGATI; KIKUCHI; GOMES, c2006).

Um exemplo de técnica esteganográfica que ainda é utilizada até hoje, é a marca d'agua, que é de grande interesse comercial para produtoras e editoras, visando a diminuição dos casos de pirataria, garantindo sua marca e qualidade original no produto. (PEREIRA, 2013).

Nem sempre a técnica de esteganografia é utilizada para fins legais, muitos se aproveitam dessa opção para planejar crimes cuja finalidade é auto lucrativa. Para tanto métodos de esteganografia em textos, imagens, sons e vídeos podem ser utilizados.

2.4.1 Esteganografia em Textos

É uma técnica efetiva, desde que as duas partes, emissor e receptor, tenham conhecimento sobre a técnica, já que é necessário que um texto tenha sentido para que o mesmo não chame a atenção. A técnica consiste em cifradores nulos, onde em uma mensagem, apenas algumas letras são utilizadas para formar a verdadeira mensagem a ser

transmitida, e o restante das letras podem ser desconsideradas. (JULIO; BRAZIL; ALBUQUERQUE, 2013).

2.4.2 Esteganografia em Imagens

Ainda segundo os autores citados anteriormente, a técnica **LSB** (Last Significant Bit) é uma das técnicas mais utilizada, que baseia-se na modificação dos bits menos significativos da imagem, onde em uma implementação simples, os pixels substituem o plano LSB por completo com a informação inserida. Já em um esquema mais complexo, os locais de inclusão são adaptativamente selecionados, e dependendo das características da visão humana, uma peque distorção é aceitável, desde que não chame a atenção das pessoas.

2.4.3 Esteganografia em Áudio

Uma das técnicas utilizadas neste método, é o de inserir uma informação através de um eco. Para que a informação seja oculta de forma eficaz, variam-se três parâmetros de sinais de eco: a amplitude, taxa de deterioração e o atraso. Esses parâmetros são configurados de forma que fiquem abaixo do limite sensorial do ouvido humano, de forma que não seja possível distinguir entre o som original e o eco, que pode ser considerado como uma ressonância. (PETRI, 2004).

2.4.4 Esteganografia em Vídeo

Tendo em vista que um vídeo digital é composto por um conjunto de inúmeras imagens que quando exibidas em uma taxa de 24 a 30 quadros por segundo, dão a impressão de movimento. Sendo assim, para que seja possível inserir uma informação oculta em um vídeo, é necessário manipular as imagens ali contidas. Isso só é possível pelo fato de que a visão humana não tem a capacidade de percepção de pequenas alterações nas imagens realizadas por meio da introdução de bits relativos a mensagem que será oculta. A mesma técnica LSB é utilizada. (CARVALHO, 2008).

2.5 Esteganálise

Segundo Petri (2004), a Esteganálise refere-se a estudos e pesquisas com o intuito de descobrir informações que foram ocultadas de alguma forma, seja em texto, imagem, áudio ou vídeo. As técnicas esteganográficas possuem falhas como em qualquer outro sistema, e podem ser descobertas por qualquer usuário que tenha interesse em avaliar e examinar detalhadamente algum objeto em busca de informações ali ocultas.

Ainda segundo o autor supracitado, não há métodos de ataques a esteganografia que sejam universais ou mesmo que correspondam a todos os softwares com esta finalidade. Em um ataque passivo, a intenção é de apenas identificar a presença ou ausência de uma informação no arquivo, já no ativo, além de interceptar a mensagem também é possível manipular os dados.

Quando há a suspeita de que existe uma informação oculta em um arquivo, é preciso realizar uma série de testes e analises de hipóteses a fim de descobrir uma maneira de extrair as informações ali contidas. Quando se sabe qual software foi utilizado para inserir a mensagem, o esteganalista consegue obter uma melhor análise do processo. (CHIRIGATI; KIKUCHI; GOMES, 2006 citado por PEREIRA, 2013).

2.6 Pericia Forense

Segundo Silva (2010), a perícia pode ser considerada como uma pesquisa onde são exigidos conhecimentos técnicos e/ou científicos, a fim de que o perito esteja capacitado para interpretar e decifrar algum crime. Já a perícia forense, consiste em aplicar métodos científicos para que seja possível identificar, analisar e solucionar um caso por meio das evidencias deixadas pelo autor.

2.6.1 Pericia Forense Computacional

A perícia forense computacional é um método criado para investigar e combater cibercrimes, onde se utiliza de técnicas especificas para coletar, preservar, analisar e apresentar informações suspeitas contidas em computadores que foram utilizados na elaboração e execução de algum crime, e a partir daí buscar evidencias deixadas pelos criminosos com o intuito de solucionar o caso. (GONÇALVES et al., 2012).

3. Softwares de Perícia Forense Digital

Para realizar um trabalho efetivo entre coletar, analisar e evidenciar dados e informações, os peritos dependem de ferramentas precisa e eficientes, de forma que possam colaborar com investigações criminais. No presente trabalho, foram utilizadas as ferramentas: Stegdetect, Hide And Reveal e SilentEye.

3.1 Stegdetect

É uma ferramenta de código livre, capaz de detectar e inserir informações através da esteganografia em imagens no formato **JPG**. A ferramenta utiliza analise de descriminante limiar para comparar a imagem original com a modificada. Um cálculo é realizado para apresentar as diferenças existentes nas imagens. (PROVOS, c2004).

A ferramenta pode ser encontrada no sistema operacional FDTK, versão 3.0, baseado em plataforma Linux, possuindo cerca de 100 ferramentas que podem ser utilizadas em uma investigação criminal. (NEUKAMP; BOTELHO, c2014).

3.2 Hide And Reveal

Segundo Cottin (c2013), é uma ferramenta desenvolvida em Java. O Hide And Reveal é um aplicativo de código livre, que usa a técnica de esteganografia para camuflar informações em uma imagem de formato BMP. A ferramenta possui uma interface agradável ao usuário e de fácil utilização, com as opções de inserir ou revelar uma mensagem em uma imagem.

3.3 SilentEye

A ferramenta SilentEye é uma aplicação multiplataforma com uma interface de fácil utilização. Capaz de ocultar informações em imagens no formato JPG utilizando a técnica LSB. (CHOREIN, c2010).

4. Metodologia

O presente trabalho foi dividido em duas etapas, onde a primeira etapa consistiu no levantamento do referencial teorico, consistido pelas informações e aspectos históricos sobre o tema abordado. Já a segunda etapa foi a parte pratica, com o intuito de instalar as ferramentas já citadas anteriormente e início das inserções da mensagem contida em

um arquivo “txt” de 109 bytes em imagens nos formatos JPG e BMP de dimensões 256, 512 e 1024 pixels, imagens estas que foram retiradas da web, de forma que fosse possível ampliar a quantidade de resultados gerados, permitindo uma melhor analise ao final das inserções.

5. Resultados Finais e Considerações Finais

Após finalizar as inserções, os resultados gerados foram dispostos lado a lado a fim de analisar se houve alguma alteração visível a olho nu nas imagens.

Utilizando a ferramenta Stegdetect, os resultados gerados pelas três imagens no formato JPG foram mais satisfatórios, considerando que as imagens não sofreram alterações visíveis e o tamanho dos arquivos não sofreram alterações consideráveis, mantendo a qualidade e discrição das imagens.

Na ferramenta SilentEye, utilizando as três imagens no formato JPG, os resultados não foram satisfatórios, tendo em vista que as imagens finais tiveram distorções perceptíveis e os tamanhos dos arquivos também sofreram um aumento considerável.

Em relação à ferramenta Hide And Reveal, nos testes que foram realizados nas três imagens no formato BMP, os resultados, em termos, foram satisfatórios, pois nenhuma das imagens geradas ao final, tiveram sua qualidade diminuída, todavia, o tamanho dos arquivos sofreram um grande aumento.

Tendo em vista os resultados gerados, ficou definido que a melhor ferramenta esteganográfica utilizada para inserir uma mensagem, foi a Stegdetect, esta que teve bons resultados tanto na qualidade das imagens, quanto ao tamanho dos arquivos.

Referências

CAPURRO, R.; HJORLAND, B., O Conceito de informação[1]. **Ufmg**, 2007. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/viewFile/54/47>. Acessado em: 10 Set 2014.

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. Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-08062009-143448/pt-br.php>. Acessado em: 04 maio 2014.

Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. Criptografia. **cartilha.cert**, c2012. Disponível em: <http://cartilha.cert.br/criptografia/>. Acessado em: 05 abr. 2014.

CHIRIGATI, F. S.; KIKUCHI, R. S. A.; GOMES, T. L. Esteganografia. **Gta.ufrj**, c2006. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html>. Acessado em: 09 abr. 2014.

CHOREIN, A., SilentEye Steganography is yours. **Silenteye.org**, c2010. Disponível em: <http://www.silenteye.org/changes.html?i1s3>. Acessado em: 20 abr 2014.

COTTIN, N., Hide and Reveal. **Hidereveal.org**, c2013. Disponível em: <http://hidereveal.ncottin.net/>. Acessado em: 20 abr 2014.

CRIME Digital – Cibercrime. **SaferNet Brasil**, c2008. Disponível em: <http://www.safernet.org.br/site/prevencao/cartilha/safer-dicas/crime>. Acessado em: 31 mar 2014.

GALVAO, JR. Diferenças entre chaves simétrica e assimétrica para criptografia. **wordpress.com**, c2007. Disponível em: <http://pedrogalvaojunior.wordpress.com/2007/11/16/diferencas-entre-chaves-simetrica-e-assimetrica-para-criptografia/>. Acessado em: 05 abr. 2014.

GONÇALVES, M. et al., **Perícia Forense Computacional: Metodologias, Técnicas e Ferramentas**, 2012. In: Revista Científica Eletrônica de Ciências Sociais Aplicadas da EDUVALE. Disponível em: <http://www.eduvalesl.edu.br/site/edicao/edicao-74.pdf>. Acessado em: 06 maio 2014.

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://jeiks.net/wp-content/uploads/2013/11/cap2-esteganografia.pdf>. Acessado em: 09 abr. 2014.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informação Gerenciais**. São Paulo: Pearson, 2007. v. 7.

PEREIRA, M. R. T. **Esteganografia: Análise de Técnicas Aplicadas a Segurança da Informação**, 2013. Trabalho de Conclusão de Curso (Bacharel em Ciência da Computação) – Universidade do Sagrado Coração, Bauru, 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. Disponível em: <http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_petri_esteganografia.pdf>. Acessado em: 09 abr. 2014.