Comparativo de Ferramentas de Detecção de Esteganografia Windows e Linux

Guilherme Henrique C, DrKelton A.P Costa
{guicapelli@hotmail.com, kelton.costa@gmail.com}

Curso de Tecnologia em Redes de Computadores - Faculdade de Tecnologia de Bauru (FATEC)
Rua Manoel Bento da Cruz, nº 30 Quadra 3 - Centro - 17.015-171 - Bauru, SP – Brasil

Abstract. *With the advent of the Internet, information systems have become essential in companies, given the amount of important data increase the need to keep this information safe, but every day is created methods for capturing information in order to capture and transmit confidential information, one of the most effective methods for transmitting information is steganography, which consists of hiding information and messages in images, the present work aims at comparing existing programs in the market for steganography analysis, It is concluded that steganography together with encryption makes it almost impossible to detect.*

Resumo. Com o Advento da internet, os sistemas de informações passaram a ser essencial nas empresas, tendo em vista a quantidade de dados importantes, aumentam a necessidade de manter essas informações seguras, porém cada dia que passa criam-se métodos para a captura de informações a fim de capturar e transmitir informações sigilosas, um dos métodos mais eficazes para transmissão de informações é a esteganografia que consiste em ocultar informações e mensagens em imagens, o presente trabalho visa comparar os programas existentes no mercado para análise de esteganografia, conclui-se que a esteganografia juntamente com uma criptografia torna-se quase impossível a detecção

1. Introdução

No mundo atual, a informação obtida ou gerada pelas empresas é essencial como meio para a competitividade no mercado, porém cada dia que se passa criam-se métodos com o intuito de tomar posse de informações valiosas, as empresas buscam meios de se defender de ataques constantes para que ela não seja prejudicada no mercado em que atua, uma técnica eficaz para transmitir informação de forma oculta é a esteganografia.

De acordo com a Associação Nacional de Peritos Criminais Federais APCF (2004), tal método utiliza textos, imagens, sons e vídeos para esconder informações de forma que as mesmas passem despercebidas aos olhos humanos, acredita-se que grandes atentados terroristas como os de 11 de setembro de 2001, tenham sido estruturados e delineados utilizando esteganografia como principal meio de conversação.

Para isto, é primordial que haja um sistema que possa utilizar algumas técnicas de Esteganálise, que é métodos ou algoritmos utilizados para análise de esteganografia, para a identificação de possíveis imagens que contenha arquivos embutidos.

O presente trabalho propõe um comparativo de programas para detecção de imagens esteganográficas nas plataformas Windows e Linux, buscando analisar e poder dizer quais a vantagem de se usar um programa no Windows ou no Linux, porem o arquivo oculto dentro da imagem deve estar em um formato conhecido (caso o texto não esteja em um formato conhecido, ou seja, esteja criptografado de forma que o sistema não consiga identificar o código (*American Standard code for Information Interchange*, ASCII)), caso contrário o programa não conseguira identificar possível alteração na imagem.

2. História da esteganografia

Na "História de Heródoto" há muitas passagens mostrando o estilo da esteganografia, em uma dessas história, um mensageiro se disfarçou de caçador para mandar uma mensagem à realeza, escondendo-a adentro de uma lebre como o mensageiro estava camuflado, passou despercebido pelos portões do castelo e a majestade pôde receber a mensagem.

Kahn (1996), diz que os egípcios utilizavam desenhos para cobrir as mensagens escondidas, o método de escrita egípcio conhecido como hieróglifo (figura 1) era uma técnica comum para esconder mensagens. Quando um mensageiro egípcio era pego com um hieróglifo que continha algum código, o inimigo não suspeitava e a mensagem podia ser entregue sem problemas ao destinatário.

Petiticolas et al (1999), contava que outro método seria raspar a cabeça dos emissários e tatuar a mensagem a ser comunicada e após o crescimento do cabelo o emissário seria enviado até o seu destino, aonde novamente seria raspada a sua cabeça para revelar a mensagem.

Nenhuma pessoa desconfiaria aonde se encontrava a mensagem estava, exceto se soubesse precisamente onde buscar. Nesta ocorrência o segredo com a localização da mensagem precisaria ser mantido.

Na Segunda Guerra Mundial, as práticas esteganográficas se baseavam em tintas invisíveis, de uma forma geral, as tintas invisíveis são químicas que se misturadas a outras químicas, tornam o resultado visível.

Rocha (2003), falava que as primeiras tintas eram simples fluídos orgânicos que não exigiam nenhuma técnica exclusiva para serem reveladas. Somente no aquecer do papel o bilhete surgia, um exemplo são as tintas fundamentadas em fluídos de suco de limão.

Jascones, Tavares (2003), outro método que começou a ser utilizado na Segunda Guerra Mundial foram os micropontos, devido ao aumento da qualidade das câmeras, lentes e filmes. Por meio deste método uma mensagem secreta poderia ser fotografada e reduzida ao tamanho de um ponto, e podendo este ser um ponto final de sentença ou o ponto de uma letra i de outra mensagem qualquer

Figura 1 EXEMPLO DE HIERÓGLIFOS
Fonte 1 http://www.infoescola.com/civilizacao-egipcia/hieroglifos

2.1 Esteganografia na China

Conforme Jasper (2009), na China antiga, mensagens eram escritas sobre seda fina e o pequeno retalho era recoberto por cera. Para transportar a mensagem oculta, um mensageiro era obrigado a engolir a bolinha, ir até o destinatário e entregá-la após expeli-la.

Segundo Kipper (2004), esse método é similar ao usado por Histaeu, onde a mensagem era escrita no corpo de um mensageiro e ele era usado como meio de transporte (figura 3)

Outra técnica na história chinesa foi a utilização dos "Bolos da Lua" (Figura 2) durante a dinastia Yuan, quando a China estava sob o Império Mongol. Os líderes da rebelião contra o império mongol decidiram se utilizar do festival da Lua para coordenar seu ataque, aproveitando-se da tradição do bolo da lua. Os rebeldes inseriram mensagens dentro dos bolos e as levaram, sem levantar suspeitas, a todos que precisavam ter conhecimento de seus planos.

Segundo Kipper (2004), os rebeldes conseguiram sucesso em seu ataque e arrasaram o governo, que se seguiu da dinastia Ming Pedaços do bolo da lua, é distribuído ainda hoje no festival da lua, o episódio chinês relembra a queda do império mongol.

Figura 2 BOLO DA LUA
Fonte 2 3 http://chinaminhavida.com/2010/09/21/moon-cake-bolo-da-lua/

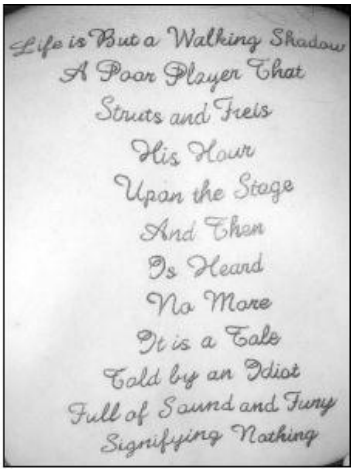


Figura 3 EXEMPLO DE MENSAGEM TATUADA NO CORPO
Fonte 3 http://escafandro.blogtv.uol.com.br/2008/07/21/tatuagem-literaria-suas-frasespreferidas-perto-do-coracao

2.2 Tabuletas de Demarato

De acordo com Kipper (2004), aos gregos são creditados os primeiros fatos históricos do uso da esteganografia, documentados durante o conflito entre a Grécia e a Pérsia, no século V A.C. por Heródoto.

Xerxes, o tirano rei da Pérsia, iniciou a levantar uma nova capital para o seu império, Persepólis. Para tornar interessante a cidade, começaram a chegar vários presentes de todo o império, com a exceção de duas cidades-estados, Atenas e Esparta.

Segundo Singh (2008), determinado a combater tal insolência, Xerxes começou a reunir um grande exército, para lançar um ataque surpresa sobre as cidades estado. Em 480 a.C. ele estava pronto para lançar o ataque.

Apesar disso, os preparatórios tinham sido observados por Demarato, um grego que fora expulso de sua terra natal, apesar de seu exílio, ainda sentia lealdade para com a Grécia e decidiu despachar uma mensagem advertindo os espartanos do plano de Xerxes. O problema era com mandar a mensagem sem-levantar suspeita.

Sobre isso Singh (2008), mencionou o algoritmo explicado por Heródoto a ameaça de ser descoberto era grande, existia exclusivamente uma maneira pela qual a mensagem poderia passar isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo o que Xerxes desejava fazer, posteriormente a mensagem foi coberta novamente com cera.

Deste modo, as tabuletas pareceriam estar em branco e não acarretariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de entender o segredo, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e expôs aos outros que se eles raspassem a cera localizariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os outros gregos.

Como resultado do aviso, os gregos começaram a se armar e em 23 de setembro de 480 A.C. conseguiram preparar uma armadilha para os Persas, na baía de Salamina, onde conseguiram aplicar uma derrota humilhante às formidáveis forças persas.

2.3. Esteganografia como Ciência

De Acordo com a APCF (2004) descreve que a ciência é algo que leva o homem a grandes conquistas, guerras e aniquilamento, com o advento da internet a troca de dados se intensificou de forma mais veloz em pouco tempo, se tornando o meio de comunicação mais utilizado.

Para não serem encontrados, os chamados piratas de computador, ou *hackers*, passaram a reinventar suas técnicas nas trocas de conhecimento. Hoje, um dos métodos mais eficazes se chama: esteganografia.

Tal método utiliza textos, imagens, sons e vídeos para esconder informações de forma que as mesmas passem despercebidas aos olhos humanos. Acredita-se que grandes atentados terroristas como os de 11 de setembro de 2001, tenham sido estruturados e delineados utilizando esteganografia como principal meio de conversação.

Para Tavares, Bandeira e Madeiro (2012): esteganografia e uma técnica de segurança da informação que tem a função de ocultar dados em um objeto de cobertura.

Para diversos tipos de aplicações, sobretudo militares, comunicações seguras são de suma importância, uma vez que o objeto de cobertura oculte a informação, ele passa a ser denominado estego-objeto.

Segundo Chandramouli (2002): esteganálise é uma divisão relativamente nova da investigação. Enquanto estenografia (que é um pouco diferente watermarking) lida com procedimentos de ocultação de dados, o desígnio da Esteganálise é Identificar e / ou estimar informações potencialmente camuflado dos documentos ressaltados com pouco ou nenhum conhecimento sobre a esteganografia código e / ou dos seus parâmetros.

É correto dizer que esteganálise é uma arte e uma ciência. O artifício de esteganálise cumpre um papel admirável na escolha de propriedades ou características de um bilhete stego típico pode apresentar-se ao mesmo tempo a ciência auxílio na forma fiável a avaliar as características escolhidas para a presença da informação oculta.

Segundo Wayner (2009), abrigar os dados de caráter que não pode ser descoberto é um procedimento idêntico, contudo muitas ocasiões distintas muitas vezes chamadas esteganografia. Há muitos modelos históricos de TI, incluindo compartimentos escondidos, sistemas mecânicos, como micropontos, ou transmissões explosão, que tornam a carta difícil de achar.

Diferentes técnicas, tais como a codificação a mensagem nas primeiras letras dos termos disfarçarem o conteúdo e fazer parecer que outra coisa. Todos estes têm sido empregados novamente.

A informação digital oferece oportunidades admiráveis para não só esconder informações, mas também para desenvolver uma estrutura teórica geral para camuflar as informações.

É possível descrever os algoritmos gerais e fazer algumas afirmações sobre o quão difícil consistir em para alguma pessoa que não sabe a chave para encontrar os dados. Determinados algoritmos oferecer um bom modelo de sua força.

Conforme Stallings (2008), os métodos de esteganografia ocultam a existência de uma mensagem. Uma configuração simples de esteganografia, mas que é lenta de se arquitetar é aquela que um arranjo de palavras e letras dentro de um texto visivelmente inofensivo soletra a mensagem real.

Para Gil et al (2008), a esteganografia aplicada a imagens busca modificar-se os bits de pixels menos expressivos, nos bits da mensagem que se almeja ocultar.

Logicamente, esse método arrasta uma perda na qualidade da imagem original. No entanto, dependendo do código utilizado, a imagem contendo a mensagem secreta e a imagem original não exibem diferenças que possam ser identificadas a olho nu pelo ser humano.

Segundo Kawaguchi e Eason (s/d), esteganografia é uma técnica para ocultar documentos secretos em alguns outros dados, sem deixar qualquer aparente evidência de adulteração de dados. Todas as técnicas tradicionais têm steganographic-esconder informações capacidade limitada. Eles podem esconder apenas 10% (ou menos) dos valores de dados do navio. Isto é porque o princípio de tais técnicas foram quer para substituir uma parte especial dos componentes da imagem Embarcação de frequência, ou para substituir todos os bits menos significativos de um valor múltiplo imagem com a informação secreta.

A esteganografia usa uma imagem como dos dados dos barcos, e incorporar informações confidenciais nos pixeis do barco. Esta técnica faz uso das características do aparelho de visão humana em que um humano não pode perceber qualquer formato informações num padrão binário muito complexo. Podemos substituir todas as regiões "ruído-como" nos pixeis do navio imagem com dados secretos sem deteriorar a qualidade da imagem.

Para Provos e Honeyman (2001): esteganografia é a arte e a ciência de ocultar o acontecimento desde que a conversação está acontecendo. Sistemas gráficos estegano podem camuflar mensagens dentro de imagens ou outros objetos digitais.

2.4. Codificação de Huffman

Hayashida (s/d) descreve que o método de codificação de Huffman permite a representação em binário de seus tipos a partir de sua possibilidade de ocorrência.

A ideia geral é que o codificador deve dar como saída, representações mais curtas para símbolos mais prováveis e mais compridas para símbolos menos prováveis. Uma consideração importante é a velocidade do codificador, pois pode haver um grande overhead se for requerida uma compressão ótima. Pode-se sacrificar um pouco do desempenho da compressão para reduzir o overhead.

Tabela 1 CODIFICAÇÃO DE HUFFMAN
Fonte 4 http://www.linux.ime.usp.br/-cef/mac499-01/monografias/ulisses/#_5.1_Código

SIMBOLOS	REPRESENTAÇÕES	PROBABILIDADE
T	00	0,3
E	10	0,2
S	010	0,2
N	110	0,1
A	111	0,1
O	0110	0,05
L	0111	0,05

A figura 4 abaixo, é baseada na Tabela 1 que poderá ser usada para a decodificação. Para decifrar um símbolo, a árvore é corrida transversalmente, começando da origem até a última folha. O caminho percorrido corresponde a uma representação na tabela acima.

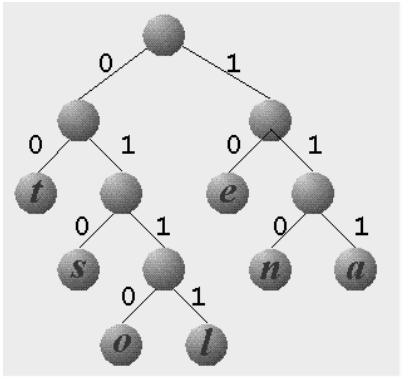


Figura 4 Arvore Binaria
Fonte 5 http://www.linux.ime.usp.br/~cef/mac499-01/monografias/ulisses/#_5.1_Código

O algoritmo de Huffman constrói a árvore de decodificação de baixo para cima. Como exemplo, conhecendo as possibilidades dos símbolos, inicialmente o algoritmo constrói um nó para todo símbolo.

Após os dois nós com menor perspectiva tornam-se irmãos na árvore, criando-se para isso um nó pai que tenha como probabilidade a soma dos seus dois filhos. A intervenção de combinação é repetida, escolhendo-se novamente os dois nós com menor probabilismo e ignorando-se os nós que já são filhos.

2.5. Johannes Trithemius

Segundo Perteson (1990) o Religioso Johannes Trithemius foi responsável pela concepção de diferentes métodos cripto-esteganográficos, vários deles usados nos três volumes de seu principal livro, Steganographia, que foi explanado erroneamente por muitos séculos como um livro diabólico, logo que a mensagem original do livro, que eram criptografadas nos nomes dos querubins citados, não eram conhecidas.

Uma das invenções mais criativas de Johannes é a cifra "Ave Maria". TKOTZ [2007b] explica e exemplifica o algoritmo da seguinte forma, "Este método é composto por 14 alfabetos nos quais cada letra corresponde uma palavra ou grupo de palavras. O resultado da encriptação acaba sendo um texto (mais ou menos) coerente, em Latim, como se fosse uma oração ou glorificação religiosa".

A seguir um dos principais alfabetos "Ave-Maria de Johannes Trithemius".

- A: no céu
- B: para todo o sempre
- C: um mundo sem fim
- D: numa infinidade
- E: perpetuamente
- F: por toda a eternidade
- G: durável
- H: incessantemente
- I-J: irrevogavelmente
- K: eternamente
- L: na sua glória
- M: na sua luz

- N: no paraíso
- O: hoje
- P: na sua divindade
- Q: em Deus
- R: na sua felicidade
- S: no seu reino
- T: na sua majestade
- U-V-W: na sua beatitude
- X: na sua magnificência
- Y: ao trono

"Na sua majestade um mundo sem fim, um mundo sem fim Uma infinidade, perpetuamente, Perpetuamente, no seu reino, na sua majestade perpetuamente, durável no céu, no paraíso hoje, durável na sua felicidade, no céu por toda a eternidade, irrevogavelmente no céu. "

Figura 5 Mensagem esteganografia pelo algoritmo "Ave Maria"
Fonte 6 Adaptada http://www.esotericarchives.com/tritheim/stegano.htm

A mensagem da figura 5 tem significado de "TCC DE ESTEGANOGRAFIA". Apesar de ser uma cifra poderosa, é o período indispensável para o envio de grandes mensagens, o que impede de transmitir de uma mensagem muito extensa.

3. Método LSB (*Least significant bit* (Ultimo Bit Menos Significativo))

De acordo com Tavares, Bandeira e Madeiro (2012), o código LSB evidência pouca segurança quando são aplicadas, as técnicas de Esteganálise em sua forma de ocultação incide em uma mudança conduzida dos bits menos significativos, pelos bits dos dados a serem escondidos, de maneira sequencial.

Em contraponto os métodos de esteganografia são as artes de Esteganálise, que são métodos desenvolvidos com a intenção de identificar dados camuflados, o teste qui-quadrado é um apontador de anormalidades estatísticas, esse teste consiste em determinar o valor de X^2 pela equação.

$$X^2 = \sum_{i=1}^{N} \frac{\left(ei - E(ei)\right)^2}{E(ei)}$$

Equação 1 FORMULA DO QUI-QUADRADO
Fonte 7 Adaptado Tavares, j. r. c. Lima. J. B. Madeiro. F.(2012)

Na equação 1
ei – Representa o Número de ocorrências de evento i
E(ei) – Representa o Valor esperado
N – Representa a quantidade de eventos considerados na analise

Um exemplo simples de um evento pode ser a aparição de um valor de LSB igual a Zero, enquanto seu bit vizinho tenha o valor Um.

Resultados de X^2 próximos a zero indicam que anormalidades não foram detectadas, valores muito alto pode indicar o uso de esteganografia.

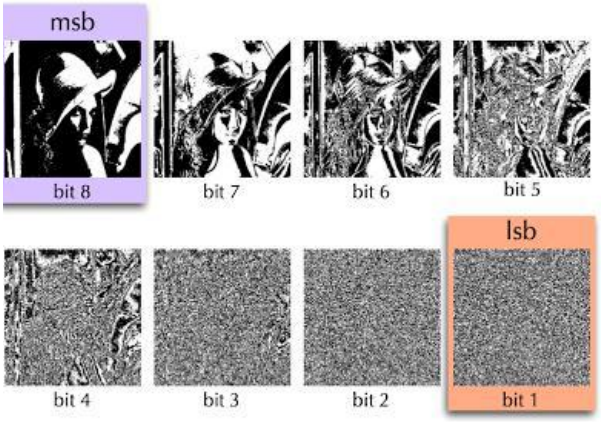


Figura 6 Exemplo de Ataque LSB
FONTE 8 watermarkero.blogspot.com.br/2009/03/el-metodo-lsb.html

3.1. Método *Bit-Plane* (Plano de Bit Complexidade Segmentação)

Conforme Kawaguchi e Eason (s/d): A prática de esteganografia, que tem como objetivo ocultar a informação de grande importância, a substituição das regiões em complexos cada bit-plano de uma cor da Imagem com padrões binários aleatórios é invisível ao olho humano.

Pode-se usar essa qualidade para o nosso refúgio de informação (Agrupamento) tática. A metodologia prática é como se adota. Em nosso procedimento que apelidamos de uma imagem de condutora "um recipiente" ou imagem "dummy". É uma imagem colorida em qualquer tipo de formato, que esconde os conhecimentos secretos em arquivos em qualquer formato.

No segmento de cada arquivo segredo para ser incorporado em uma série de blocos tendo 8 bytes de dados de cada. Estes blocos são considerados como padrões de 8 × 8 imagens. Chamamos esses blocos os blocos secretos.

Bit-plane é por ocasiões serem usadas frequentemente como um sinônimo de Bitmap. No entanto, tecnicamente, o primeiro se menciona à localização das informações na memória e o último aos dados em si.

Uma habilidade do uso de bit plane é definir se algum bit plane é um ruído ocasional ou contém informações importantes.

Um método para calcular isso é confrontar cada pixel (X, Y) a três pixels adjacentes (X-1, Y), (X, Y-1) e (X-1, Y-1). Se o pixel for o mesmo que, pelo menos, dois dos três pixels adjacentes, não é ruído, o bit plane de ruído terá de 49% a 51% dos pixels sendo ruídos.

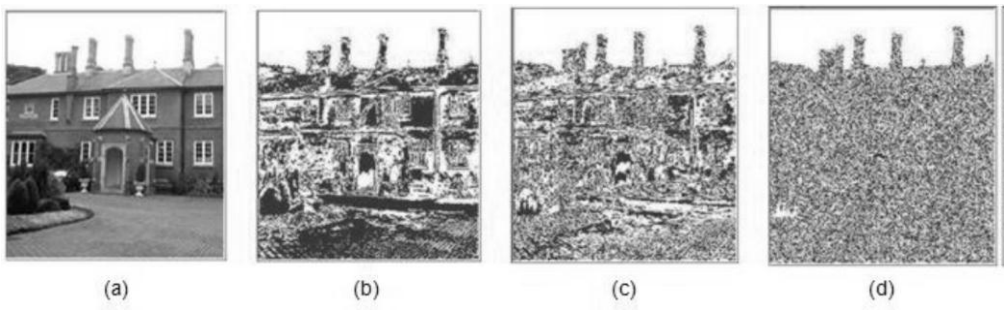


Figura 7 imagem com ataque Bit-plane

Fonte 9 www.gta.ufrj.br/grad/09_1/versao-final/stegano/tecnicas.html

3.2. Ataque Aural

De acordo com Rocha (2003), "Determinados ataques retiram as partes expressivas da imagem como um meio de facilitar aos olhos humanos a busca por irregularidades na imagem". Desta forma a aleatoriedade dos bits menos significativos pode revelar a existência de uma mensagem ocultada, considerando que uma imagem produzida por câmeras, *scanner* ou outros meios digitalizadores sempre deixam marcas de grande estrutura nos bits menos significativos.

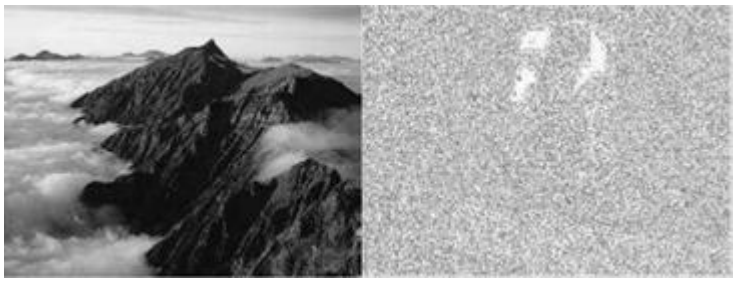


Figura 8 Exemplo de Ataque Aural
Fonte 10 http://rafaeloliveirav/wordpress.com/2009/04/21/esteganografia-e-esteganalise---a-arte-da-informacao-escondida-esteganalise-tipos-de-ataques/ adaptado

Como se pode analisar na Figura 8, percebe-se que há uma alteração no bit menos significativos, após serem retirados os bits mais significativos da imagem pelo Ataque Aural, podendo sinalizar que nesta imagem foi utilizado a esteganografia.

3.3. Ataque Estrutural

Para Rocha (2003), "O formato do arquivo de dados frequentemente se altera de tal modo que outra mensagem é inserida".

Para este modelo pode-se utilizar um compactador de arquivos. Através deste meio se for comparado à imagem original com a estego-imagem nota-se que ambos são visualmente iguais e têm o mesmo tamanho. Somente olhando as imagens, não se pode notar qualquer diferença, e consequentemente não se pode adivinhar mensagens ou informações ocultas neles. Mas quando se aplica a compressão de arquivos, o fato de que alguma coisa está oculta torna-se transparente. Especialmente quando se utiliza dados aleatórios (ou uma mensagem codificada, com dados aleatórios iguais). Assim, a redundância é eliminada tornando o algoritmo de compressão ineficaz.

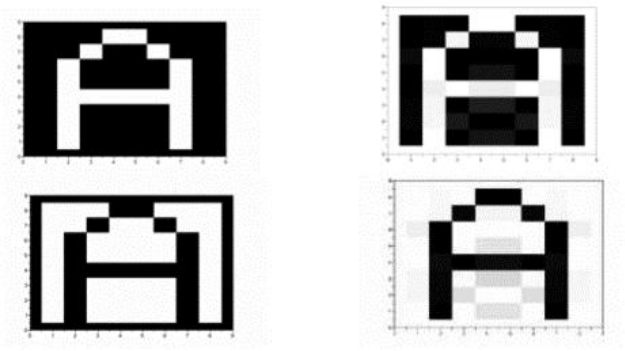


Figura 9 Exemplo de Ataque Aural
FONTE 11 https://www.gta.ufrj.br/grad/15_1/esteg_ofusc/esteganalise.html

Para os ataques estruturais figura 8, a forma mais fácil de identificar mensagens ocultas é o emprego de princípios capazes de considerar padrões estruturais.

Esse tipo de ataque, muitas vezes é impossível compreender a altercação entre a imagem original e a estego-imagem, todavia usando, por exemplo, o método da compressão, apesar de ambas possuírem aproximadamente o mesmo peso, após a compressão, percebe-se a altercação entre elas, devido ao fato desta técnica extinguir os bits semelhantes, ou seja, a redundância e com isso altera a estrutura do arquivo, fazendo com que se torne claro o que estava oculto.

4. Materiais e Métodos

Para esteganografia reversa, foram analizados programas de Esteganálise existentes, utilizando 3 programas para a plataforma Windows, Hide and Reveal, Jphswin, StegoSuite e 3 programas para a Plataforma Linux, OpenStego, OutGuess, StegHide, buscando poder dizer quais são as diferenças entre eles e qual tem um tempo de resposta menor, além de outras informações importantes relacionadas aos sistemas analisados.

Para a Comparação dos programas foram criadas duas máquinas virtuais Windows e Linux contento a mesma Configuração, 4 Giga de memória Ram, 500 Giga de Hard Disk Sistema Operacional Windows 7 32 Bits, Sistema Operacional Ubuntu 16.04 32 bits.

- Hide and Reveal versão 3.0
- Jphswin versão 0.5
- StegoSuite executado no Java 8
- OpenStego versão 0.7.1
- OutGuess
- StegHide Versão 0.5.1

O programa usado para a realização dos testes da sua maior parte, encontra-se nos primeiros anos é recente, outros softwares são totalmente baseados e executados em Java.

Além da parte de comparações também foi feito a utilização de levantamento bibliográficos para a elaboração deste projeto.

4.1 Resultados Obtidos

Os Testes foram realizados através de imagens de “Crisantemo” e “Deserto” obtidas através da internet, foi também criado um Arquivo para a elaboração da Esteganografia e este arquivo foi escondido na imagem do “Crisantemo”, e a Imagem do “Deserto Utilizada nos programas do Windows”

Tabela 2 Comparativo de Ferramentas de Detecção de Esteganografia
Fonte 12 Elaborado pelo Autor

Comparativo de Ferramentas de Detecção de Esteganografia Windows e Linux							
Nome do programa	Tipo de imagem	Licença	Plataforma	Tempo de detecção	Criptografia	Encontrou arquivo	LIMITE TAMANHO
Hide and reveal	Tif, png, bmp	Gratuito	Windows	21,0 segundos	_____	NÃO	NÃO
Jphswin	JPEG	Gratuito	Windows	5 segundos	_____	NÃO	Não
StegoSuite	BMP, GIF, JPG	Gratuito	Windows, Linux	3,30 segundos	AES	Sim	Não
Openstego	JPEG, PNG	Gratuito	Linux	2,81 Segundos	AES – 128	SIM	NÃO
Outguess	JPEG, PPM e PNM	Gratuito	Linux	2,68 Segundos	_____	Sim	Não
Steghide	JPEG, BMP, WAV e AU	Gratuito	Linux	6,08 segundos	AES	Sim	Não

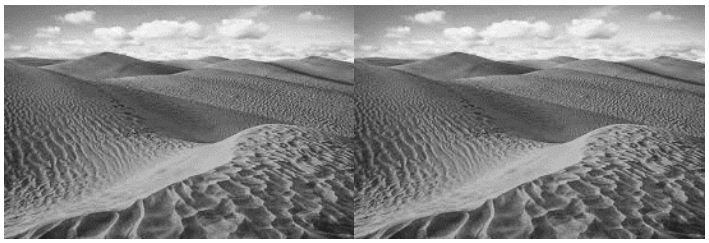


Figura 10 Imagem de Teste do Deserto do SAARA
Fonte 12 Google imagens

Figura 10 Imagem de Deserto do SAARA Obtida no google imagens, para realização dos testes de detecção de esteganografia imagem da Esquerda “Sem Esteganografia” Imagem da Direita “Com Esteganografia”.

Figura 11 imagem de Teste de Crisântemo
Fonte 13 Google Imagens

Figura 11 imagem de Crisântemo obtida no google imagens, para realização dos testes de detecção de esteganografia imagem da Esquerda "Sem Esteganografia" Imagem da Direita "Com Esteganografia".

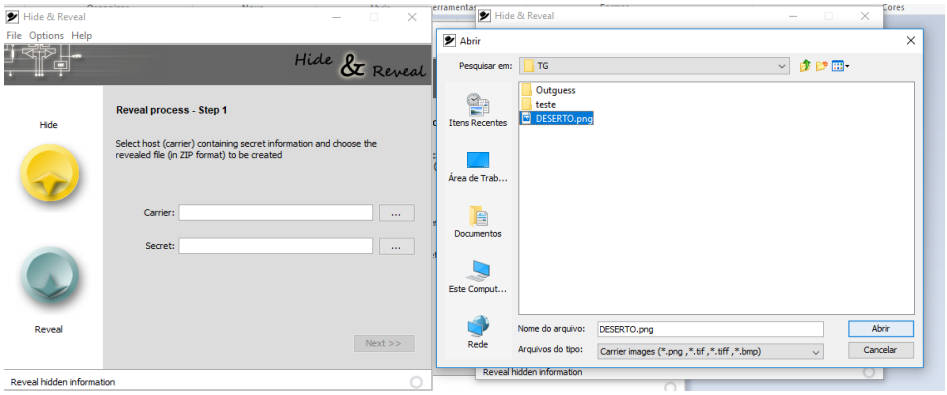


Figura 12 Tela inicial do Hide and Reveal **Figura 13 Selecionando a imagem no Hide and Reveal**
Fonte 14 Hide and Reveal

Figura 12- Tela Inicial do programa Hide and Reveal do Sistema Operacional Windows onde é possível buscar a imagem suspeita de conter esteganografia.

Figura 13 – Imagem onde percebe-se a seleção da imagem suspeita de conter Esteganografia.

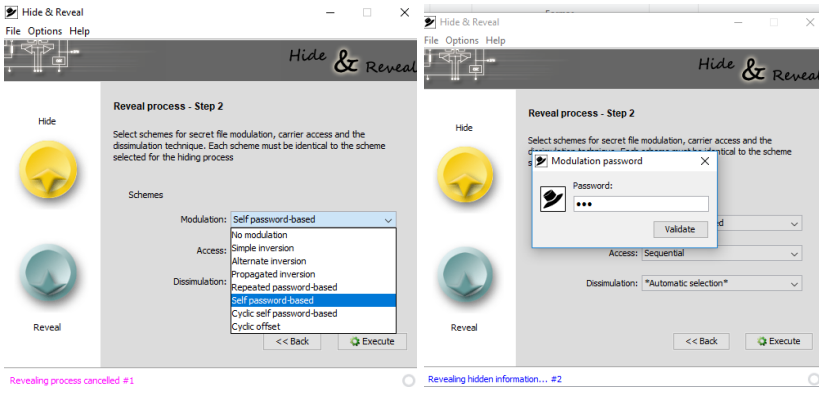


Figura 14 Selecionando a modulação **Figura 15 Inserindo a Senha no Hide and Reveal Da Senha no Hide and Reveal**
Fonte 15 Hide and Reveal

Figura 14 – Imagem aonde permite-se escolher uma modulação para a Senha, para o teste foi escolhido a Modulação Self Modulation Based.

Figura 15 – Colocando a Senha no Hide and Reveal para a Detecção da Esteganografia.

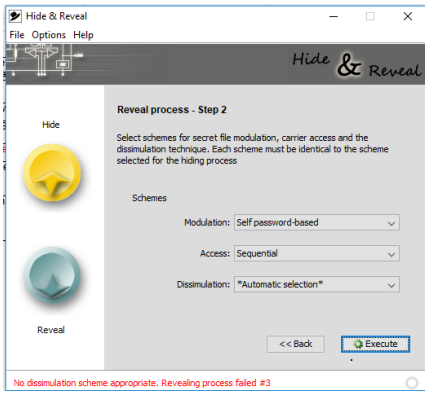
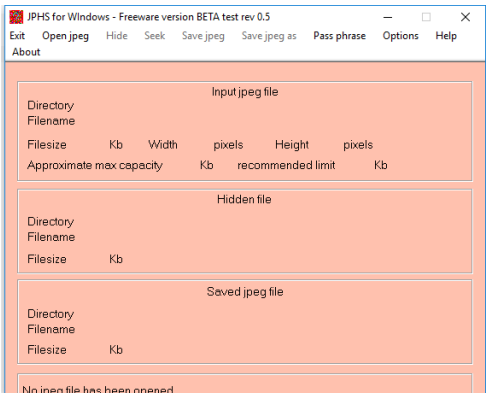


Figura 16 Teste no Hide and Reveal Concluído
Fonte 16 Hide and Reveal

Figura 16 - Imagem do Programa Hide and Reveal Concluído onde mostra a mensagem de falha no processo de detecção.



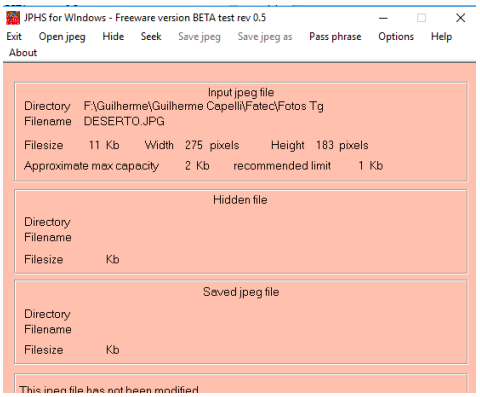


Figura 17 Tela Inicial do Jphswin **Figura 18 Selecionando a Imagem no Jphswin**
Fonte 17 Jphswin

Figura 17 - Tela Inicial do programa Jphswin do Sistema Operacional Windows onde é possível buscar a imagem suspeita de conter esteganografia.

Figura 18 – Imagem do Programa Jphswin realizado a seleção da Imagem através da opção Open jpeg.

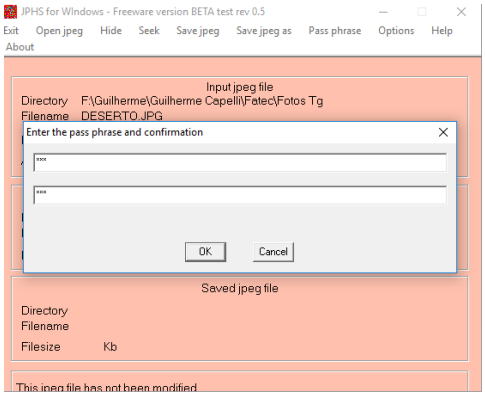
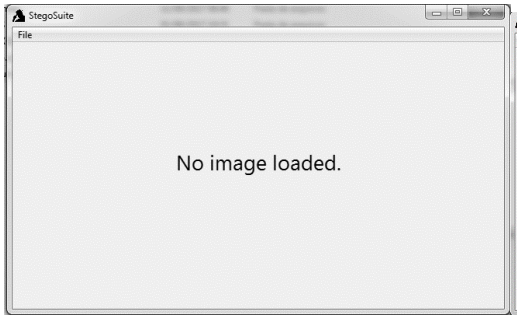


Figura 19 Colocando a Senha no Jphswin
Fonte 18 Jphswin

Figura 19 - Colocando a Senha da Imagem no Programa Jphswin através da opção Seek e realizando a Detecção.



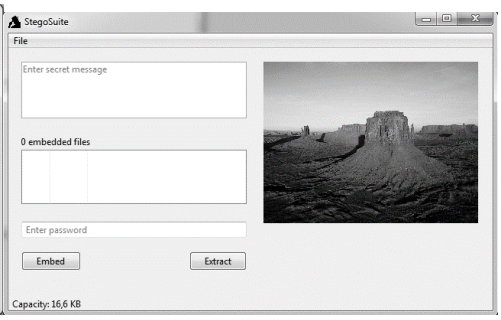


Figura 20 tela Inicial do StegoSuite **Figura 21 Imagem Selecionada no StegoSuite**
Fonte 19 StegoSuite

Figura 20 – Tela inicial do programa StegoSuite do Sistema operacional Windows Realizado o Teste com a imagem Deserto.

Figura 21 – Imagem Selecionada no programa StegoSuite através da opção File do Programa.

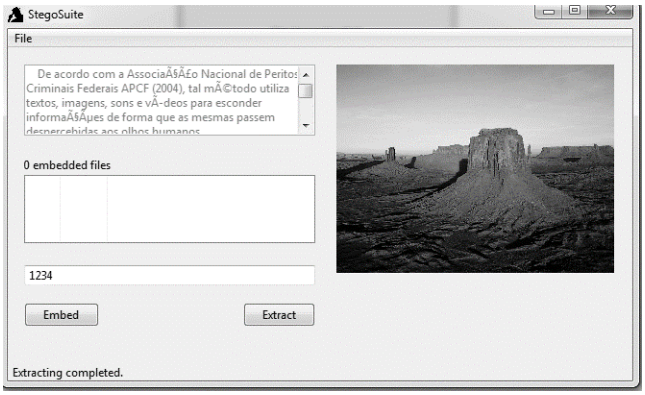
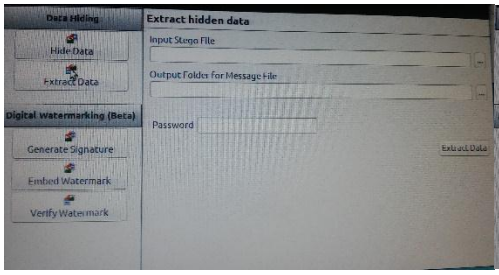


Figura 22 Imagem Selecionada no StegoSuite
Fonte 20 StegoSuite

Figura 22- Imagem de Teste concluída aonde podemos perceber a mensagem que estava oculta dentro da imagem do Deserto do SAARA e a senha padrão utilizada para ocultar.



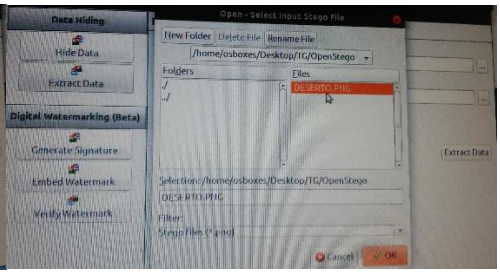
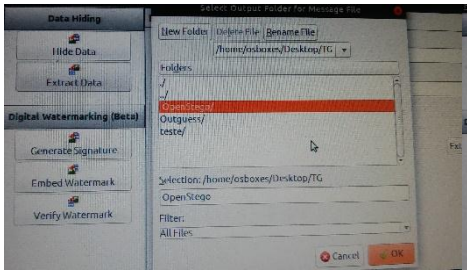


Figura 23 Tela Inicial do OpenStego **Figura 24 Selecionando a Figura no OpenStego**
Fonte 21 OpenStego

Figura 23 – Tela Inicial do programa OpenStego do Sistema Operacional Linux.
Figura 24 – Selecionando a Imagem esteganografada no programa OpenStego



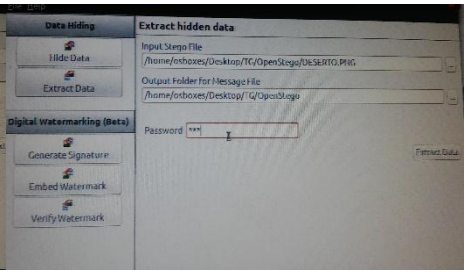


Figura 25 Selecionando a Pasta para Salvar a Mensagem no OpenStego **Figura 26 Colocando a Senha no OpenStego**

Fonte 22 OpenStego

Figura 25 – Selecionando a Pasta para Salvar a mensagem oculta na imagem.
Figura 26 - Colocando a Senha no OpenStego.

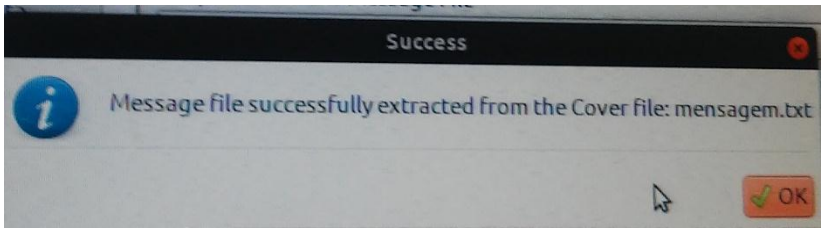


Figura 27 Teste Concluído no Programa OpenStego
Fonte 23 OpenStego

Figura 27 – Teste realizado através do Programa OpenStego no qual apresenta-se uma mensagem oculta.

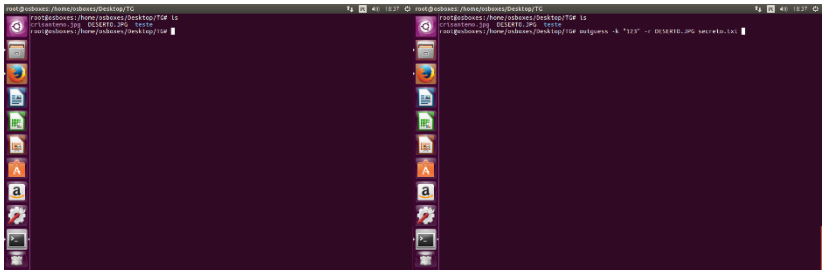


Figura 28- imagem do Linux Figura 29- Aplicando o Comando do Outguess Mostrando a imagem a ser testada

Fonte 24 - OutGuess

Figura 28 – Imagem do Terminal do Ubuntu onde através do Comando “ls -la” mostra todos as imagems salvas na Pasta do Teste

Figura 29 – Imagem do Terminal do Ubuntu aonde é aplicado o Comando “outguess -k “senha” -r DESERTO.JPG secreto.txt” para a verificar se a imagem Deserto contem alguma mensagem Oculta.

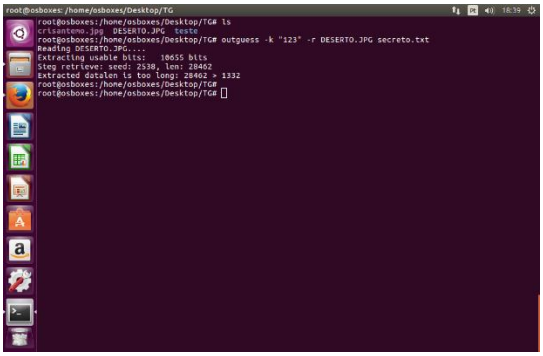


Figura 30 Teste Concluído no Programa OutGuess
Fonte 25 OutGuess

Figura 30 – Teste Realizado através do programa Outguess aonde mostra-se os dados estatístico da mensagem oculta na Tela do Terminal

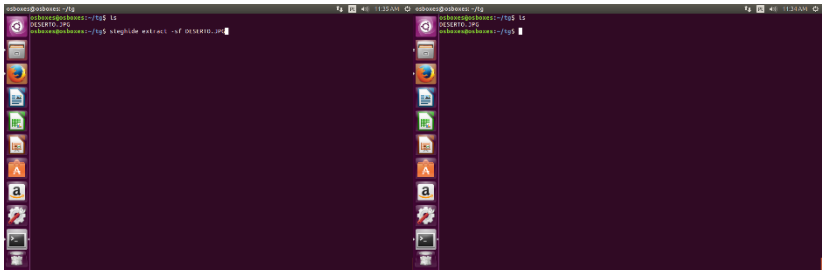


Figura 31- tela inicial do steghide figura 32 aplicando o comando no steghide

Fonte 26 - Steghide

Figura 31- Imagem do Terminal mostrando a Figura a Ser Testada no StegHide.

Figura 32 - Aplicando o Comando “steghide extract -sf DESERTO.JPG” no steghide para Detecção da mensagem.

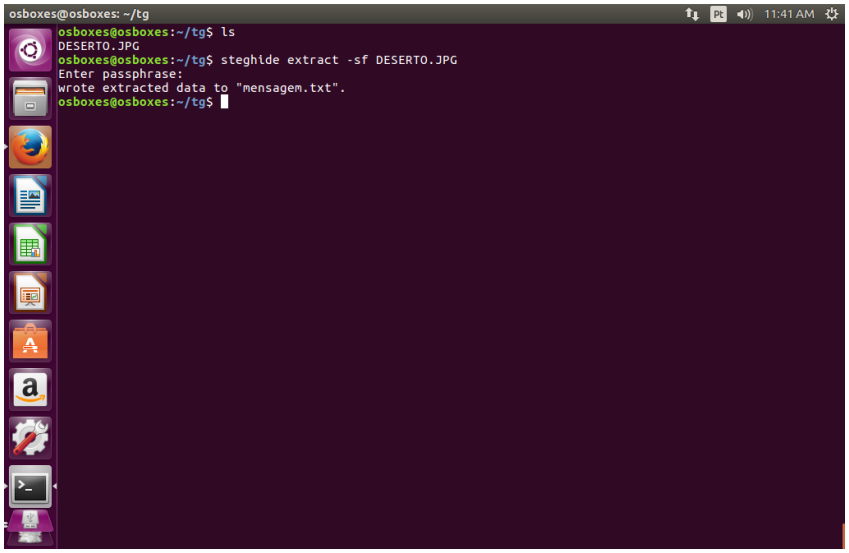


Figura 33 - aplicando a senha da imagem no programa StegHide
Fonte 27 – steghide

Figura 33 – Imagem do Terminal do Ubuntu aonde pede-se a senha de acesso a imagem esteganografada para teste se possui alguma mensagem.

Os Sistemas operacionais Windows e Linux apresentam diversos programas para análise de esteganografia, o programa que apresentou um resultado em menor tempo no Sistema Linux foi o programa “OUTGUESS” cujo não apresenta limite no tamanho da imagem a ser analisada e aceita os formatos de imagem e vídeo “JPEG, PPM e PNM”, com tempo de resposta de 2,68 segundos, outro programa com um excelente resultado no Sistema Operacional Windows foi o “STEGOSUITE” no qual utiliza da criptografia AES , não possuindo limites no tamanho de imagens e Aceitando os Seguintes formatos” BMP, GIF, JPG”.

5. Conclusão

Foi pesquisada a Esteganografia através do algoritmo simétrico LSB e a aplicação em imagens digitais e o método de inserção no último bit significativo (LSB), O principal método para conter dados em uma imagem.

A Esteganografia em conjunto com uma Criptografia torna-se bastante segura, sendo praticamente impossível violar qualquer mensagem que esteja camuflada.

Como a esteganografia é possível ocultar qualquer tipo de formato de arquivo, não apenas texto, pois o que realmente importa é a informação binária que representa este arquivo. Pode-se, por exemplo, ocultar uma imagem dentro de outra.

Conclui-se que o Trabalho atendeu as expectativas proporcionando uma opção de programa a ser usado no Linux ou Windows.

Como trabalho futuro pretende-se realizar testes com mais Softwares existentes para análise de imagens e verificar a performance desses *softwares* com áudios e vídeos.

Referências

Associação nacional de peritos Criminais Federais – APCF (2004) “I Conferencia Internacional de Pericias em Crimes Cibernéticos”. Brasília https://angelacmesecurity.org/ãdriano/papers/anais-iccyber-dpf-2004.pdf, Outubro 2016

Chandramouli R. 2002 “A Mathematical Approach To Steganalysis” http://www.Nist.Gov/dads/HTML/datastructur.Html Outubro 2016

Gil, F. De. O. et al (2008) “SEA- Sistema Esteganográfico de Arquivos”. Porto Alegre, sbseg2008.inf.ufrgs.br/resources/slides/WTICG_ST3/apr_st03_04_wticg.pdf, Outubro 2016

Hayashida, U. “Código de Huffman” São Paulo, Monografia. https://www.linux.ime.usp.br/~cef/mac499-01/monografias/Ulisses/#_5.1__Código, Novembro 2016

Jascone, F, Tavares, L (2003) “Prototipo de Software para ocultar Texto Criptografado em imagens Digitais”. Blumenau http://www.inf.furb.br/~pericas/orientaçoes/Esteganografia2003.pdf, novembro 2016

Jasper N (2009) “Esteganografia: integridade, confidencialidade e autenticidade”. São Paulo. Fevereiro 2017

Kawaguchi, E, Eason. R, “O Principle and applications of BPCS – Steganography” https://www.datahide.com/bpcse/articles/ref-6.spie98.pdf, Outubro 2016

Kahn, D. (1996) “the history of steganography. In: proceedings of the first international” http://dl.acm.org/citation.cfm?id=728895, Outubro. 2016

Kipper, G. (2004) “Investigator's Guide to Steganography. Auerbach Publications.
LEAL, S. Certinews Criptografia Quântica”. https://www.certisign.com.br/certinews/edicoes/certnews_06/sleal.htm> Março 2017

Perteson, J, H. (1990) “Steganographia (Secret Writing)” http://www.esotericarchives.com/tritheim/stegano.htm > Setembro 2017

Petitcolas, F. A. Et Al (1999) “Information hiding - a survey In Proceedings of IEEE. Special issue on Protection on multimedia” Fevereiro 2017

Provos. N, Honeyman. P,(€2001) “Hide and Seek: An Introduction to Steganography”, http://niels.xtdnet.nl/papers/practical.pdf, Outubro. 2017

Rocha. A. R. (2003) “Camaleão: Um Software para Segurança Digital Utilizando Esteganografia”, Outubro 2016

Stallingns, W. “Criptografia e Segurança de Redes: Princípios e Praticas”. 4 ed. São Paulo: Pearson, 2008. Outubro 2016

Singh, S. (2008) “O Livro dos Códigos -A Ciência do Sigilo: do Antigo Egito à Criptografia Quântica” Rio de Janeiro Outubro 2016

Tavares, j. r. c. Bandeira. J. L. Madeiro. F.(2012) “LSB Word-Hunt: Um Método de Esteganografia para Imagens Digitais Utilizando Chave Simétrica” www.sbmac.org.br/cmacs/cmac-ne/2012/trabalhos/PDF/190.pdf Outubro. 2016

Universidade Federal do Paraná (2013) “Código ASCII”, Paraná http://www.ufpa.br/dicas/progra/arq-asc.htm Março 2017

Wayner, P (2009) “Disappearing Cryptography – escondendo Informações: Esteganografia e marca de água”. 2 Edição. Outubro. 2016